クライアントレス SSL VPN のトラブルシューティング

（注） **シスコは、ASA バージョン 9.17(1) で有効なクライアントレス SSL VPN の非推奨機能を発表しました。**9.17(1) より前のリリースでは、限定的なサポートが継続されます。より堅牢で新しいソリューション（たとえば、リモート Duo ネットワークゲートウェイ、AnyConnect、リモートブラウザの分離機能など）への移行オプションに関する詳細なガイダンスを提供します。

Application Access 使用時の hosts ファイル エラーからの回復

Application Access の実行の妨げになる hosts ファイル エラーを回避するために、Application Access を使用し終えたら、Application Access ウィンドウを必ず閉じるようにします。ウィンドウを閉じるには、[Close] アイコンをクリックします。

Application Access が正しく終了しなかった場合は、`hosts` ファイルは、クライアントレス SSL VPN 用にカスタマイズされた状態のままになっています。ユーザーが次に Application Access を起動するときに、クライアントレス SSL VPN は hosts.webvpn ファイルを検索することで、Application Access の状態をチェックします。hosts.webvpn ファイルが検出されると、「`Backup HOSTS File Found`」というエラー メッセージが表示され、Application Access が一時的にオフに切り替わります。

Application Access が異常終了した場合は、リモート アクセス クライアント/サーバー アプリケーションが不安定な状態になります。クライアントレス SSL VPN を使用せずにこれらのアプリケーションを起動しようとすると、正しく動作しない場合があります。通常の接続先のホ

ストが使用できなくなる場合があります。一般にこのような状況は、自宅からリモートでアプリケーションを実行し、Application Access ウィンドウを終了せずにコンピュータをシャットダウンし、その後職場でそのアプリケーションを実行しようとした場合に発生します。

Application Access ウィンドウを正しく閉じないと、次のエラーが発生する可能性があります。

- 次に Application Access を起動しようとしたときに、Application Access がオフに切り替わっている可能性があり、「`Backup HOSTS File Found`」エラー メッセージが表示される。
- アプリケーションをローカルで実行している場合でも、アプリケーション自体がオフに切り替わっているか、または動作しない。

このようなエラーは、Application Access ウィンドウを不適切な方法で終了したことが原因です。次に例を示します。

- Application Access の使用中に、ブラウザがクラッシュした。
- Application Access の使用中に、停電またはシステム シャットダウンが発生した。
- 作業中に Application Access ウィンドウを最小化し、このウィンドウがアクティブな状態（ただし最小化されている）でコンピュータをシャットダウンした。

Hosts ファイルの概要

ローカル システム上の hosts ファイルには、IP アドレスとホスト名がマッピングされています。Application Access を起動すると、クライアントレス SSL VPN は hosts ファイルを修正し、クライアントレス SSL VPN 固有のエントリを追加します。Application Access ウィンドウを正しく閉じて Application Access を終了すると、hosts ファイルは元の状態に戻ります。

Application Access の起動前	hosts ファイルは元の状態です。
Application Access の起動時	• クライアントレス SSL VPN は hosts ファイルを hosts.webvpn にコピーして、バックアップを作成します。 • 次に、クライアントレス SSL VPN は hosts ファイルを編集し、クライアントレス SSL VPN 固有の情報を挿入します。
Application Access の終了時	• クライアントレス SSL VPN はバックアップ ファイルを `hosts` ファイルにコピーして、hosts ファイルを元の状態に戻します。 • クライアントレス SSL VPN は、hosts.webvpn を削除します。
Application Access の終了後	hosts ファイルは元の状態です。

（注） Microsoft 社のアンチスパイウェア ソフトウェアは、ポート転送 Java アプレットによる hosts ファイルの変更をブロックします。アンチスパイウェア ソフトウェアの使用時に hosts ファイルの変更を許可する方法の詳細については、www.microsoft.com を参照してください。

クライアントレス SSL VPN による hosts ファイルの自動再設定

リモートアクセス サーバーに接続できる場合は、hosts ファイルを再設定し、Application Access やアプリケーションを再度イネーブルにするために、次の手順を実行します。

手順

ステップ 1 クライアントレス SSL VPN を起動してログインします。

[Applications Access] リンクをクリックします。

ステップ 2 次のいずれかのオプションを選択します。

- [Restore from backup]：クライアントレス SSL VPN は強制的に正しくシャットダウンされます。クライアントレス SSL VPN は hosts.webvpn backup ファイルを `hosts` ファイルにコピーし、hosts ファイルを元の状態に戻してから、hosts.webvpn を削除します。その後、Application Access を再起動する必要があります。
- [Do nothing]：Application Access は起動しません。リモートアクセスのホームページが再び表示されます。
- [Delete backup]：クライアントレス SSL VPN は hosts.webvpn ファイルを削除し、hosts ファイルをクライアントレス SSL VPN 用にカスタマイズされた状態にしておきます。元の `hosts` ファイル設定は失われます。Application Access は、クライアントレス SSL VPN 用にカスタマイズされた hosts ファイルを新しいオリジナルとして使用して起動します。このオプションは、hosts ファイル設定が失われても問題がない場合にだけ選択してください。

Application Access が不適切にシャットダウンされた後に、ユーザーまたはユーザーが使用するプログラムによって hosts ファイルが編集された可能性がある場合は、他の 2 つのオプションのどちらかを選択するか、または hosts ファイルを手動で編集します

手動による hosts ファイルの再設定

現在の場所からリモートアクセス サーバーに接続できない場合や、カスタマイズした hosts ファイルの編集内容を失いたくない場合は、次の手順に従って、hosts ファイルを再設定し、Application Access とアプリケーションを再度イネーブルにします。

手順

ステップ 1 hosts ファイルを見つけて編集します。最も一般的な場所は、c:\windows\sysem32\drivers\etc\hosts です。

ステップ 2 `# added by WebVpnPortForward` という文字列が含まれている行があるかどうかをチェックします。この文字列を含む行がある場合、hosts ファイルはクライアントレス SSL VPN 用にカスタマイズされています。hosts ファイルがクライアントレス SSL VPN 用にカスタマイズされている場合、次の例のようになっています。

```
server1 # added by WebVpnPortForward
server1.example.com invalid.cisco.com # added by WebVpnPortForward
server2 # added by WebVpnPortForward
server2.example.com invalid.cisco.com # added by WebVpnPortForward
server3 # added by WebVpnPortForward
server3.example.com invalid.cisco.com # added by WebVpnPortForward

# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to hostnames. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding hostname.
# The IP address and the hostname should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     cisco.example.com          # source server
#       38.25.63.10     x.example.com              # x client host

123.0.0.1       localhost
```

ステップ 3 `# added by WebVpnPortForward` という文字列が含まれている行を削除します

ステップ 4 ファイルを保存して、閉じます。

ステップ 5 クライアントレス SSL VPN を起動してログインします。

ステップ 6 [Application Access] リンクをクリックします。

WebVPN 条件付きデバッグ

リモート アクセス VPN 上で複数のセッションを実行すると、ログのサイズを考慮するとトラブルシューティングが困難になることがあります。**debug webvpn condition** コマンドを使用して、デバッグ プロセスをより正確に絞り込むためのフィルタを設定できます。

debug webvpn condition { **group** *name* | **p-ipaddress** *ip_address* [{ **subnet** *subnet_mask*| **prefix** *length*}] | **reset** | **user** *name*}

それぞれの説明は次のとおりです。

- **group** *name* は、グループ ポリシー（トンネル グループまたは接続プロファイルではない）でフィルタ処理を行います。
- **p-ipaddress** *ip_address* [{**subnet** *subnet_mask* | **prefix** *length*}] は、クライアントのパブリック IP アドレスでフィルタ処理を行います。サブネット マスク（IPv4）またはプレフィックス（IPv6）はオプションです。
- **reset** すべてのフィルタをリセットします。**no debug webvpn condition** コマンドを使用して、特定のフィルタをオフにできます。
- **user** *name* は、ユーザー名でフィルタ処理を行います。

複数の条件を設定すると、条件が結合（AND で連結）され、すべての条件が満たされた場合にのみデバッグが表示されます。

条件フィルタを設定したら、基本の **debug webvpn** コマンドを使用してデバッグをオンにします。条件を設定するだけではデバッグは有効になりません。デバッグの現在の状態を表示するには、**show debug** および **show webvpn debug-condition** コマンドを使用します。

ASA VPN で複数のセッションが実行されている場合、単一のユーザー セッションをトラブルシューティングすることが煩わしくなります。条件付きデバッグを使用すると、フィルタ条件のセットに基づいて特定のセッションのログを検証できます。条件付きデバッグをサポートするモジュールは、SAML、WebVPN 要求および応答、Anyconnect です。

（注） IPv4 および IPv6 サブネットの「any, any」のサポートが提供されます。

次に、ユーザー jdoe で条件付きデバッグを有効にする例を示します。

```
asa3(config)# debug webvpn condition user jdoe

asa3(config)# show webvpn debug-condition
INFO: Webvpn conditional debug is turned ON
INFO: User name filters:
INFO: jdoe
```

```
asa3(config)# debug webvpn
INFO: debug webvpn  enabled at level 1.

asa3(config)# show debug
debug webvpn  enabled at level 1
INFO: Webvpn conditional debug is turned ON
INFO: User name filters:
INFO: jdoe
```

データのキャプチャ

CLI **capture** コマンドを使用すると、クライアントレス SSL VPN セッションでは正しく表示されない Web サイトに関する情報を記録できます。このデータは、シスコ カスタマー サポート エンジニアによる問題のトラブルシューティングに役立ちます。

前提条件

クライアントレス SSL VPN キャプチャをイネーブルにすると、セキュリティ アプライアンスのパフォーマンスに影響します。トラブルシューティングに必要なキャプチャ ファイルを生成したら、キャプチャを必ずオフに切り替えます。

キャプチャ ファイルの作成

手順

ステップ 1 クライアントレス SSL VPN 用のキャプチャ ユーティリティを開始して、user2 のトラフィックをファイルにキャプチャする hr という名前のキャプチャを作成します。

capture capture_name type webvpn user webvpn_username

capture_name は、キャプチャに割り当てる名前です。これはキャプチャ ファイルの名前の先頭にも付加されます。

webvpn_user は、キャプチャの対象となるユーザー名です。

例：

```
hostname# capture hr type webvpn user user2
WebVPN capture started.
   capture name   hr
   user name      user2
hostname# no capture hr
```

ステップ 2 （任意） ユーザーがログインしてクライアントレス SSL VPN セッションを開始したら、キャプチャ ユーティリティによるパケットの取得を停止します。キャプチャ ユーティリティが *capture_name.zip* ファイルを作成します。このファイルはパスワード **koleso** で暗号化されます。

no capture capture_name

ステップ 3 .zip ファイルをシスコに送信するか、Cisco TAC サービス リクエストに添付します。

ステップ 4 パスワード *koleso* を使用してファイルの内容を解凍します。

ブラウザによるキャプチャ データの表示

手順

ステップ 1 クライアントレス SSL VPN のキャプチャ ユーティリティを開始します。

capture capture_name type webvpn user webvpn_username

- *capture_name* は、キャプチャに割り当てる名前です。これはキャプチャ ファイルの名前の先頭にも付加されます。
- *webvpn_user* は、キャプチャの対象となるユーザー名です。

ステップ 2 （任意） ユーザーがログインしてクライアントレス SSL VPN セッションを開始したら、キャプチャ ユーティリティによるパケットの取得を停止します。

no capture capture_name

ステップ 3 ブラウザを開いて、hr という名前のキャプチャをスニファ形式で表示します。

https://**asdm_enabled_interface_of_the_security_appliance**:*port*/**admin/capture/***capture_name*/pcap

例：

```
https://192.0.2.1:60000/admin/capture/hr/pcap
```

クライアントレス SSL VPN セッション クッキーの保護

Flash アプリケーションや Java アプレットなどの組み込みオブジェクト、および外部アプリケーションは、通常は既存のセッションのクッキーに依存してサーバーと連携しています。これらの組み込みオブジェクトは、初期化時にいくつかの Javascript を使用してブラウザからクッキーを取得します。クライアントレス SSL VPN セッション クッキーに httponly フラグを追加すると、セッション クッキーがブラウザのみで認識され、クライアント側のスクリプトでは認識されなくなり、セッションの共有は不可能になります。

始める前に

- VPN セッションのクッキー設定は、アクティブなクライアントレス SSL VPN セッションがない場合にだけ変更してください。

- クライアントレス SSL VPN セッションのステータスを確認するには、show vpn-sessiondb webvpn コマンドを使用します。
- vpn-sessiondb logoff webvpn コマンドを使用して、すべてのクライアントレス SSL VPN セッションからログアウトします。
- 次のクライアントレス SSL VPN 機能は、http-only-cookie コマンドがイネーブルの場合に動作しません。
  - Java プラグイン
  - Java リライタ
  - ポートフォワーディング。
  - ファイルブラウザ
  - デスクトップ アプリケーション（Microsoft Office アプリケーションなど）を必要とする Sharepoint 機能
  - AnyConnect Web 起動
  - Citrix Receiver、XenDesktop、および Xenon
  - その他の非ブラウザ ベース アプリケーションおよびブラウザプラグインベースのアプリケーション

クライアントレス SSL VPN セッション Cookie が JavaScript などのクライアント側のスクリプトを介してサードパーティからアクセスされないようにするには、次の手順を実行します。

手順

クライアントレス SSL VPN セッションのクッキーで httponly フラグを有効にします。

http-only-cookie

例：

```
hostname(config)# webvpn
hostname(config-webvpn)# http-only-cookie
```

（注） このコマンドは、Cisco TAC から使用を推奨された場合のみ使用してください。このコマンドをイネーブルにすると、「ガイドライン」に記載されているクライアントレス SSL VPN 機能が警告なしで動作しなくなるため、セキュリティ上のリスクが発生します。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。