# ASA 8.X： ASA 8.X：L2L VPN トンネルの再構築による実行するユーザ アプリケーションの許可

## 目次



## 概要

このドキュメントでは、Persistent IPSec Tunneled Flows 機能、および VPN トンネルが中断しても TCP フローを維持する方法について説明します。

## 前提条件

### 要件

このドキュメントの読者は、VPN の動作方法について基本的に理解している必要があります。詳細は、次のドキュメントを参照してください。

- L2L VPN の設定例
- ASA での L2L VPN

### 使用するコンポーネント

このドキュメントの情報は、Cisco 適応型セキュリティ アプライアンス ( ASA ) バージョン 8.2 以降に基づいています。

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、クリアな ( デフォルト ) 設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

## 表記法

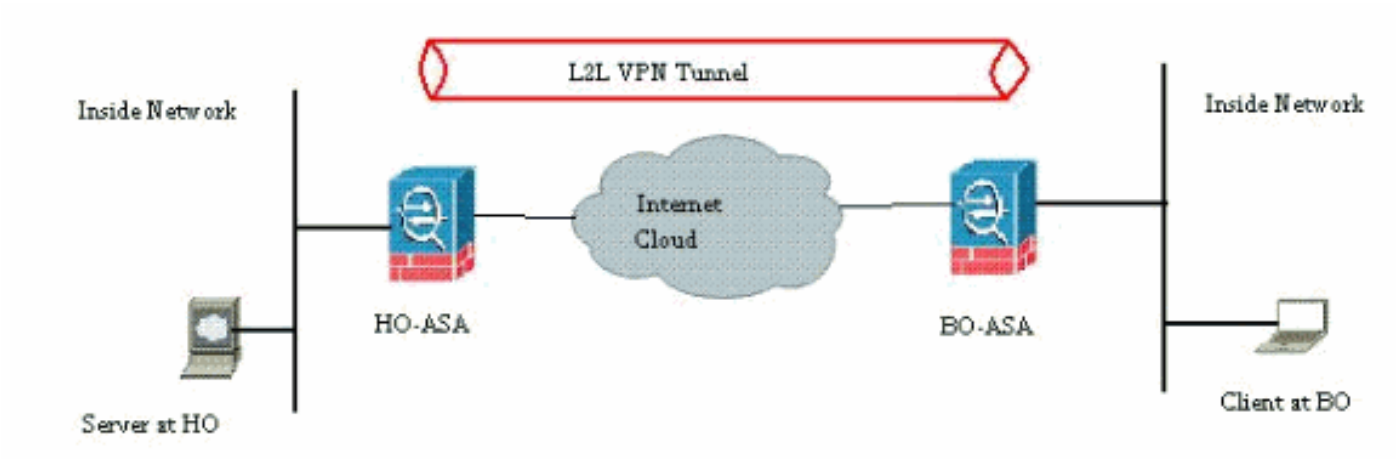
ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

# 設定

ネットワーク図で示すように、ブランチ オフィス ( BO ) を本社オフィス ( HO ) にサイト間 VPN で接続します。 ブランチ オフィスのエンド ユーザが、本社オフィスにあるサーバから大きいファイルをダウンロードしようとしているとします。 ダウンロードには数時間かかります。 VPN が正常に動作している限り、ファイル転送も正常に動作します。 ただし VPN が中断するとファイル転送はハングし、ユーザは、トンネルが確立した後でファイル転送要求を最初からやり直す必要があります。

## 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。




この問題が発生するのは、ASA の動作方法に関する組み込み機能のためです。 ASA は ASA を通過するすべての接続を監視し、アプリケーション検査機能に従って状態テーブルでエントリを維持します。 VPN を通過する暗号化済みトラフィックの詳細は、セキュリティ アソシエーション ( SA ) データベースの形式で維持されます。 このドキュメントのシナリオでは、2 つのトラフィック フローが維持されます。 1 つは、VPN ゲートウェイ間の暗号化済みトラフィックであり、もう 1 つは、本社オフィスのサーバとブランチ オフィスのエンドユーザとの間のトラフィック フローです。 VPN を終了すると、この特定 SA のフロー詳細は削除されます。 ただし、この TCP 接続用に ASA によって維持されていた状態テーブル エントリは、アクティビティがないために古くなり、これがダウンロードを妨害します。 つまり、ユーザ アプリケーションが終了している間でも、ASA はこの特定フローの TCP 接続を維持します。 しかし TCP アイドル タイマーが切れると、TCP 接続は離れて最終的にタイムアウトになります。

この問題は、Persistent IPSec Tunneled Flows と呼ばれる機能の導入によって解決しました。 新

しいコマンドが Cisco ASA に統合され、VPN トンネルの再ネゴシエート時に状態テーブルの情報は維持さるようになりました。 そのコマンドは次のとおりです。

```
sysopt connection preserve-vpn-flows
```

デフォルトでは、このコマンドはディセーブルです。 これを有効にすると、L2L VPN が中断から回復してトンネルが再確立したとき、Cisco ASA は TCP 状態テーブル情報を維持します。

このシナリオでは、トンネルの両端でこのコマンドを有効にする必要があります。 片側がシスコ以外のデバイスである場合は、Cisco ASA でこのコマンドを有効にするだけで十分です。 トンネルがすでにアクティブであるときにこのコマンドを有効にした場合は、このコマンドを有効にするためにトンネルをクリアして再確立する必要があります。 トンネルのクリアと再確立について詳しくは、『古いまたは既存のセキュリティ アソシエーション（トンネル）をクリアする』を参照してください。

## この機能の互換性の詳細

この機能は、Cisco ASA ソフトウェア バージョン 8.0.4 以降で導入されています。 これは、次のタイプの VPN のみでサポートされます。

- LAN-to-LAN トンネル
- Network Extension Mode（NEM）のリモート アクセス トンネル

この機能は、次のタイプの VPN でサポートされません。

- クライアント モードの IPSec リモート アクセス トンネル
- AnyConnect トンネルまたは SSL VPN トンネル

この機能は次のプラットフォームで存在しません。

- ソフトウェア バージョン 6.0 の Cisco PIX
- Cisco VPN コンセントレータ
- Cisco IOS® プラットフォーム

この機能を有効にしても、ASA の内部 CPU 処理にさらに負荷がかかることはありません。トンネルが動作しているときにデバイスに含まれるものと同じ TCP 接続が維持されるためです。

**注:** このコマンドは TCP 接続のみに適用可能です。 UDP トラフィックにはまったく影響しません。 UDP 接続は、設定されているタイムアウト期間に従ってタイムアウトします。

## 設定

**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。

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。

このドキュメントでは次の設定を使用しています。

- CiscoASA

次の例では、VPN トンネルの片端で Cisco ASA ファイアウォールの設定出力を実行しています。

## CiscoASA

```
ASA Version 8.2(1)
!
hostname CiscoASA
domain-name example.com
enable password <removed>
passwd <removed>
names
!
interface Ethernet0/0
 speed 100
 duplex full
 nameif outside
 security-level 0
 ip address 209.165.201.2 255.255.255.248
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 10.224.9.5 255.255.255.0
!
interface Ethernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
!
interface Management0/0
 nameif management
 security-level 100
 ip address 10.224.14.10 255.255.255.0
!
boot system disk0:/asa822-k8.bin
ftp mode passive
 !---Output Suppressed ! access-list test extended
permit ip 10.224.228.0 255.255.255.128 any access-list
test extended permit ip 10.224.52.0 255.255.255.128 any
access-list 100 extended permit ip 10.224.228.0
255.255.255.128 any access-list 100 extended permit ip
10.224.52.0 255.255.255.128 any access-list
inside_access_out extended permit ip any 10.224.228.0
255.255.255.1 ! !---Output Suppressed global (outside) 1
interface nat (inside) 0 access-list test nat (inside) 1
10.224.10.0 255.255.255.0 ! !---Output Suppressed route
inside 10.0.0.0 255.0.0.0 10.224.9.1 1 route outside
0.0.0.0 255.255.255.255 209.165.201.1 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 sip-provisional-media 0:02:00
uauth 0:05:00 absolute timeout tcp-proxy-reassembly
0:01:00 dynamic-access-policy-record DfltAccessPolicy !
!---Output Suppressed http server idle-timeout 40 http
10.224.3.0 255.255.255.0 management http 0.0.0.0 0.0.0.0
inside ! snmp-server enable traps snmp authentication
linkup linkdown coldstart ! !--- To preserve and resume
stateful (TCP) tunneled IPsec LAN-to-LAN traffic within
the timeout period after the tunnel drops and recovers.
sysopt connection preserve-vpn-flows service
resetoutside ! crypto ipsec transform-set ESP-AES-256-
MD5 esp-aes-256 esp-md5-hmac crypto ipsec transform-set
```

```
testSET esp-3des esp-md5-hmac crypto map map1 5 match
address 100 crypto map map1 5 set peer 209.165.200.10
crypto map map1 5 set transform-set testSET crypto map
map1 interface outside crypto isakmp enable outside
crypto isakmp policy 5 authentication pre-share
encryption 3des hash sha group 2 lifetime 86400 crypto
isakmp policy 10 authentication pre-share encryption des
hash sha group 2 lifetime 86400 !---Output Suppressed !
telnet timeout 5 ssh timeout 5 console timeout 0 threat-
detection basic-threat threat-detection statistics
access-list ! !---Output Suppressed ! tunnel-group
209.165.200.10 type ipsec-l2l tunnel-group
209.165.200.10 ipsec-attributes pre-shared-key * !---
Output Suppressed 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 rsh inspect rtsp inspect esmtp
inspect sqlnet inspect skinny inspect sunrpc inspect
xdmcp inspect sip inspect netbios inspect tftp !
service-policy global_policy global prompt hostname
state Cryptochecksum:5c228e7131c169f913ac8198ecf8427e :
end
```

## この機能の有効化

デフォルトで、この機能は無効になっています。 ASA の CLI で次のコマンドを使用すると有効になります。

```
CiscoASA(config)#sysopt connection preserve-vpn-flows
```

これを表示するには、次のコマンドを使用します。

```
CiscoASA(config)#show run all sysopt no sysopt connection timewait sysopt connection tcpmss 1380
sysopt connection tcpmss minimum 0 sysopt connection permit-vpn sysopt connection reclassify-vpn
sysopt connection preserve-vpn-flows no sysopt nodnsalias inbound no sysopt nodnsalias outbound
no sysopt radius ignore-secret no sysopt noproxyarp outside
```

ASDM を使用しているときは、次のパスによってこの機能を有効にできます。

[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Advanced] > [IPsec] > [System Options]

[Preserve stateful VPN flows when the tunnel drops for Network Extension Mode (NEM)] オプションをオンにしてください。

## 確認

ここでは、設定が正常に動作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 asp table vpn-context detail**：高速セキュリティ パスの VPN コンテキストの内容を表示します。この情報は、問題のトラブルシューティングに役立つ場合があります。 Persistent IPSec Tunneled Flows 機能が有効なときのコマンド **show asp table vpn-context** からの出力例を次に示します。 特定の **PRESERVE** フラグが含まれることに注意してください。

```
CiscoASA(config)#show asp table vpn-context VPN CTX=0x0005FF54, Ptr=0x6DE62DA0,
DECR+ESP+PRESERVE, UP, pk=0000000000, rk=0000000000, gc=0 VPN CTX=0x0005B234,
Ptr=0x6DE635E0, ENCR+ESP+PRESERVE, UP, pk=0000000000, rk=0000000000, gc=0
```

# トラブルシューティング

このセクションでは、トンネルのフラッピングを回避するための回避策を提示します。 回避策の賛否両論についても詳述します。

## IKE ライフタイム値のゼロへの設定

IKE ライフタイム値をゼロに維持すると、VPN トンネルを無期限に機能させて、再ネゴシエートしないようにすることができます。 SA に関する情報は、ライフタイムが切れるまで VPN ピアによって維持されます。 値をゼロとして割り当てると、この IKE セッションを永続的に持続させることができます。 これにより、トンネルの鍵の再作成中に、断続的なフローの切断の問題を回避できます。 次のコマンドを使用して実行できます。

```
CiscoASA(config)#crypto isakmp policy 50 lifetime 0
```

ただしこれには、VPN トンネルのセキュリティ レベルが低下するという短所があります。 指定間隔内で IKE セッションの鍵を再作成することにより、暗号鍵が毎回変更されて、侵入者が情報をデコードすることが難しくなり、VPN トンネルのセキュリティが強化されます。

**注:** IKE ライフタイムを無効にしても、トンネルで鍵の再作成がまったく行われないということではありません。 IPSec SA は指定間隔で鍵を再作成します。これをゼロに設定することはできないためです。 IPSec SA で許可される最小ライフタイム値は 120 秒であり、最大値は 214783647 秒です。 詳細については、『IPSec SA ライフタイム』を参照してください。

## トンネルが中断されたときのエラー メッセージ

この機能を設定で使用しないと、VPN トンネルが中断されたとき、Cisco ASA は次の口グ メッセージを返します。

```
%ASA-6-302014: Teardown TCP connection 57983 for outside:XX.XX.XX.XX/80 to
inside:10.0.0.100/1135 duration 0:00:36 bytes 53947 Tunnel has been torn down
```

**トンネルが解体されたこと**が理由であることがわかります。

**注:** このメッセージを確認するには、レベル 6 の口ギングを有効にする必要があります。

## この機能と reclassify-vpn オプションの違い

トンネルがバウンスするときは、preserve-vpn-flow オプションを使用します。 これによって前の TCP フローが開いたままになるので、トンネルが回復したとき、同じフローを使用できるようになります。

コマンド **sysopt connection reclassify-vpn** を使用すると、トンネリング トラフィックに関連する以前のフローがクリアされ、そのフローはトンネルを通過するように分類されます。 TCP フローがすでに作成されて VPN が関連していない状況では、reclassify-vpn オプションを使用します。 これにより、VPN が確立した後でトラフィックがトンネルを流れない状況が生まれます。 詳細については、『sysopt reclassify-vpn』を参照してください。

## 関連情報

- ASA でのサイト間 VPN ( L2L )
- Cisco ASA のマニュアル ページ：
- テクニカルサポートとドキュメント - Cisco Systems