ASDMを使用したASAでの特定のトラフィックの接続タイムアウトの設定

内容

はじめに

このドキュメントでは、HTTP、HTTPS、FTP、またはその他のプロトコルなどの特定のアプリケーションプロトコル用のASAおよびASDMでの接続タイムアウトの設定について説明します。接続タイムアウトは、アイドル状態の接続をファイアウォールまたはネットワークデバイスが終了してリソースを解放し、セキュリティを強化するまでの非アクティブ期間です。最初の質問は、「この設定の要件は何か」です。アプリケーションに適切なTCPキープアライブ設定がある場合、ファイアウォールでの接続タイムアウトの設定は不要なことがよくあります。ただし、アプリケーションに適切なキープアライブ設定またはタイムアウト設定がない場合、リソースの管理、セキュリティの強化、ネットワークパフォーマンスの向上、コンプライアンスの確保、およびユーザエクスペリエンスの最適化を行うには、ファイアウォールでの接続タイムアウトの設定が不可欠です。

要件

次の項目に関する知識があることが推奨されます。

- Access Control List (ACL; アクセス コントロール リスト)
- サービス ポリシー

- 接続タイムアウト

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。

- ASA 9.17(1)
- ASDM 7.17(1)

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、クリアな（デフォルト）設定で作業を開始しています。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。

デフォルト

 注：デフォルトタイムアウト

デフォルトの初期タイムアウトは30秒です。

デフォルトのhalf-closedアイドルタイムアウトは10分です。

デフォルトのdcd max_retries値は5です。

デフォルトのdcd retry_interval値は15秒です。

デフォルトのtcpアイドルタイムアウトは1時間です。

デフォルトのudpアイドルタイムアウトは2分です。

デフォルトのicmpアイドルタイムアウトは2秒です。

デフォルトのsipアイドルタイムアウトは30分です。

デフォルトのsip_mediaアイドルタイムアウトは2分です。

デフォルトのespおよびhaのアイドルタイムアウトは30秒です。

他のすべてのプロトコルでは、デフォルトのアイドルタイムアウトは2分です。

タイムアウトを決して行わない場合は、0:0:0と入力します。

接続タイムアウトの設定

ASDM

特定のトラフィックに接続テーブルがある場合、そのトラフィックには特定のアイドルタイムア

ウトがあります。たとえば、この記事では、DNSトラフィックの接続タイムアウトを変更します。

このトラフィックのネットワークダイアグラムを考慮すると、特定のトラフィックに対して接続タイムアウトを設定するオプションは多数あります。

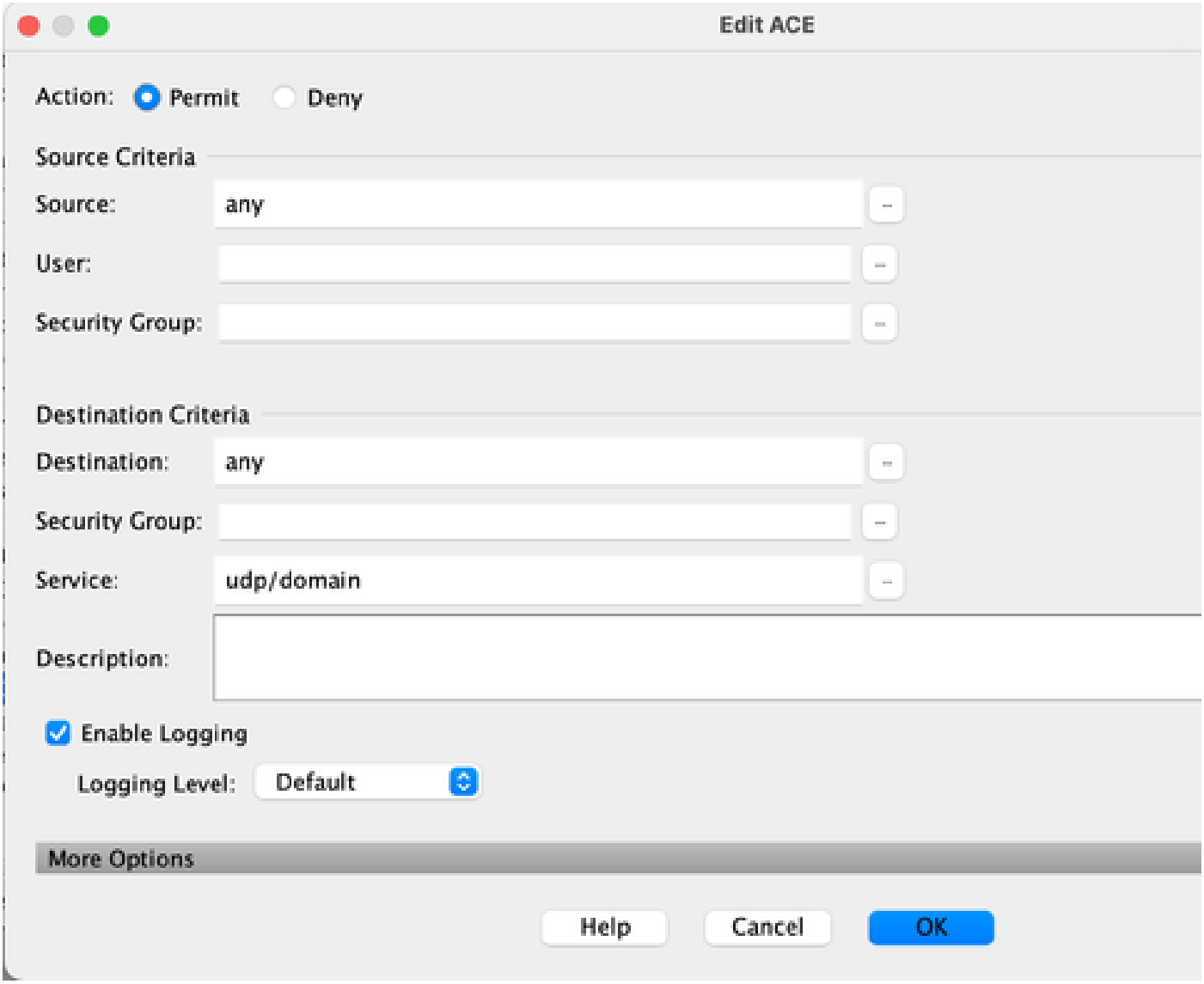
Client ----- [Interface: MNG] Firewall [Interface: OUT] ----- Server

インターフェイスにACLを割り当てる可能性があります。

手順1:ACLの作成

送信元、宛先、またはサービスを割り当てることができます

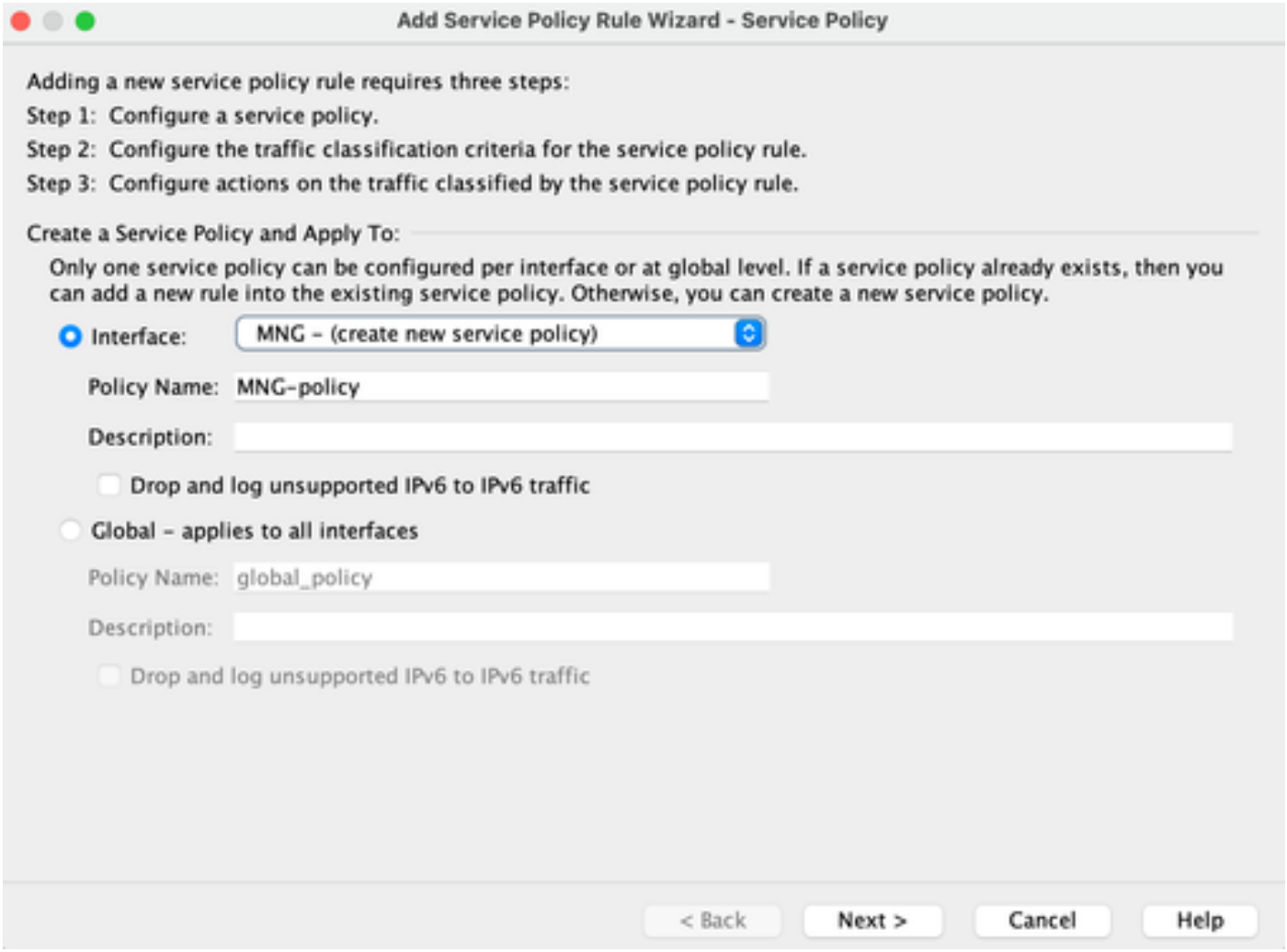
ASDM > Configuration > Firewall > Advanced > ACL Manager



ステップ2:サービスポリシールールを作成します。

ACLがすでに存在する場合は、最後の手順を省略できます。また、サービスポリシーのパラメータ（送信元、宛先、またはサービス）の1つをインターフェイスに割り当てることもできます。

ASDM > Configuration > Firewall > Service Policy rules

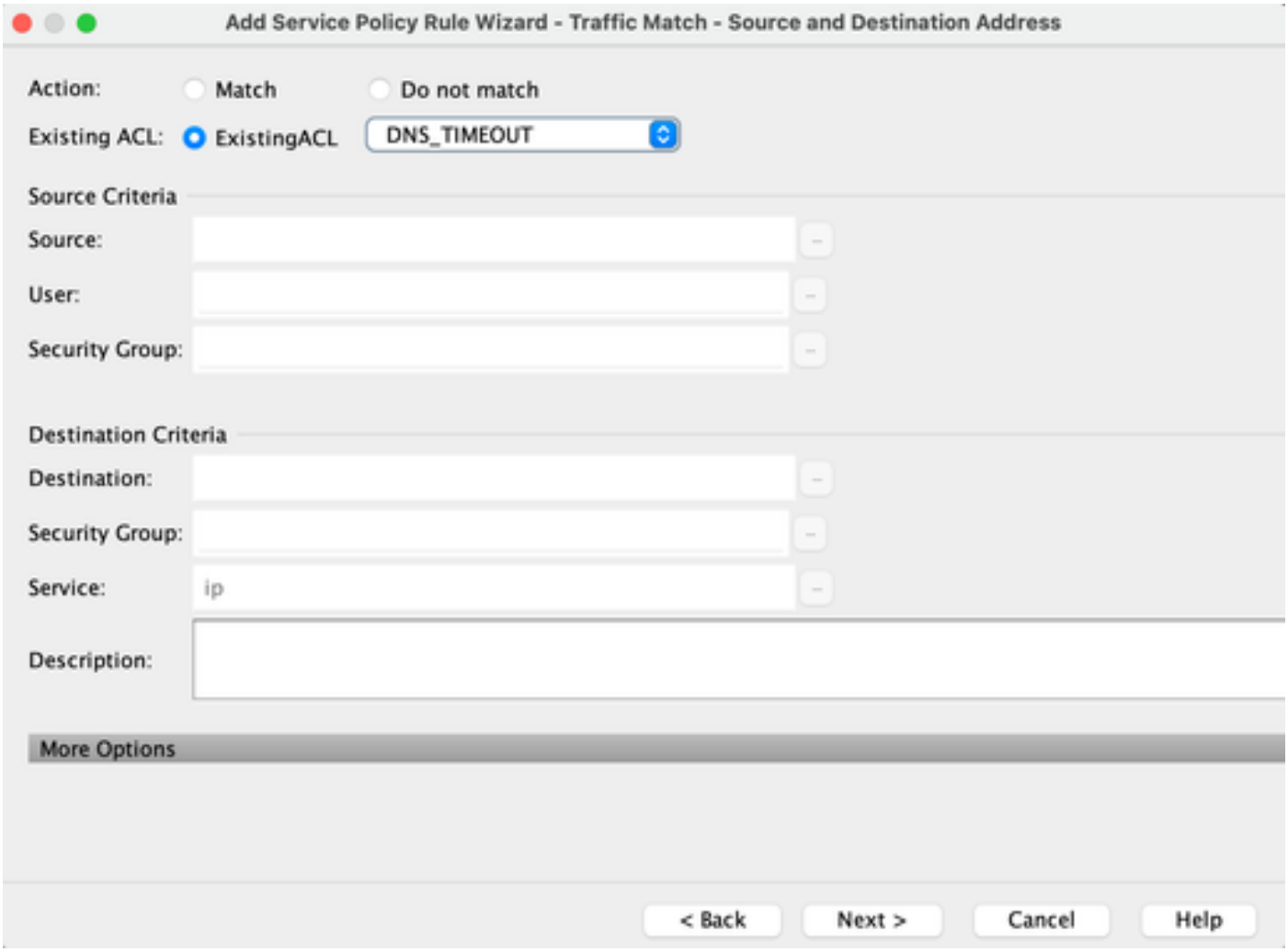


ステップ3:トラフィッククラスを作成します。

送信元IPアドレスと宛先IPアドレス（ACLを使用）を選択できます。

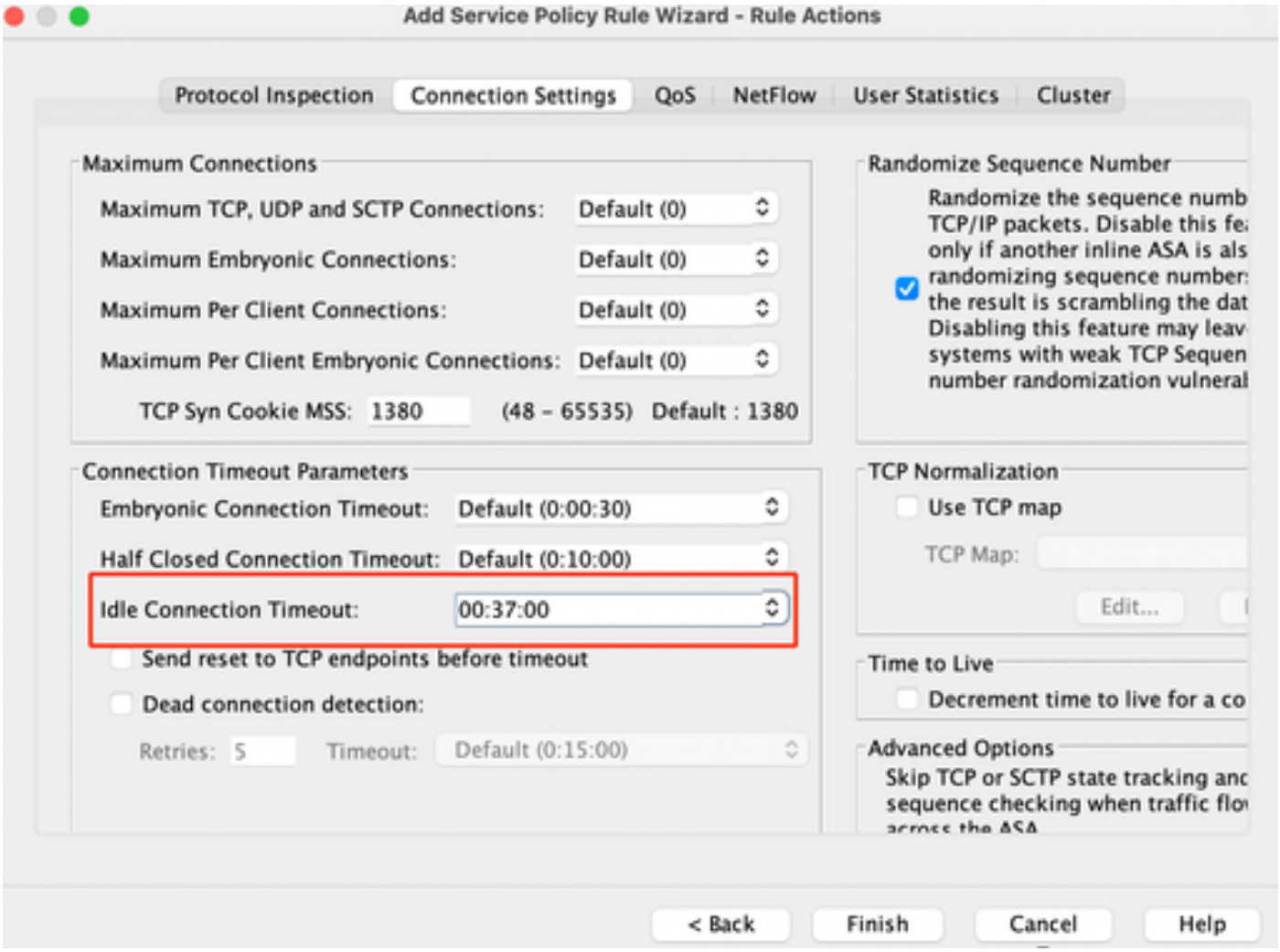
手順4:ACLの割り当て

この手順では、既存のACLを割り当てるか、一致条件（送信元、宛先、またはサービス）を選択します



ステップ5:アイドルタイムアウトパラメータを設定します

有効な形式HH:MM:SSに基づいて、アイドルタイムアウトを設定します。



その特定のトラフィックの接続をクリアします。

#clear conn address:IPアドレスまたはIPアドレスの範囲を入力します #clear conn protocol:SCP/TCP/UDP接続のみをクリアするには、このキーワードを入力します

ASAのCLI

CLIを使用して、次のすべての設定を行うことができます。

ACL： access-list DNS_TIMEOUT extended permit udp any any eq domainコマンド Class-map: クラスマップMNGクラス match access-list DNS_TIMEOUTコマンド Policy-map:

```
ポリシーマップMNGポリシー
クラスMNGクラス
set connection timeout idle 0:37:00

インターフェイスにポリシーマップを適用します。

service-policy MNG-policyインターフェイスMNG
```

確認

ヒント：このコマンドを実行すると、DNSトラフィックの接続タイムアウトを確認できます。

ASA CLI >イネーブルモード> show conn long

例：show conn long address 192.168.1.1

```
UDP MNG: 192.168.1.1/53 (192.168.1.1/53) OUT: 10.10.10.30/63327 (10.10.10.30/63327), flags - , idle 17s, uptime 17s, timeout 2m0s, bytes 36

UDP MNG: 192.168.1.1/53 (192.168.1.1/53) OUT: 10.10.10.30/62558 (10.10.10.30/62558), flags - , idle 40 s, uptime 40 s, timeout 2m0 s, bytes 36
```

設定後、アイドルタイムアウトの設定を確認できます。

例：show conn long address 192.168.1.1

```
UDP MNG: 192.168.1.1/53 (192.168.1.1/53) OUT: 10.10.10.30/63044 (10.10.10.30/63044), flags - , idle 8s, uptime 8s, timeout 37m0s, bytes 37

UDP MNG: 192.168.1.1/53 (192.168.1.1/53) OUT: 10.10.10.30/63589 (10.10.10.30/63589), flags - , idle 5s, uptime 5s, timeout 37m0s, bytes 41
```

参考資料

[接続設定とは]

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。