AAA Double Authentication Secured by Absolute Timeout

AAA Double Authentication Secured by Absolute Timeout 機能により、ユーザ単位のセッション タイムアウトを使用して保護することで、二重の認証メカニズムが確保されます。この機能は、サービスプロバイダーにより認可されたネットワークへの接続を最適化し、不要なセッションが接続されないようにすることで、ネットワークへのアクセス全体のセキュリティを高めます。

AAA Double Authentication Secured by Absolute Timeout の前提条件

- Cisco RADIUS サーバまたは TACACS+ サーバにアクセスできる必要があります。また、RADIUS または TACACS+ の設定方法を十分に理解していることが必要です。
- 認証、許可、アカウンティング（AAA）の設定方法および AAA 自動二重認証の有効化方法を十分理解していることが必要です。

AAA Double Authentication Secured by Absolute Timeout の制約事項

- AAA Double Authentication Secured by Absolute Timeout 機能は、PPP 接続専用です。自動二重認証は、X.25 やシリアル ライン インターネット プロトコル（SLIP）などの他のプロトコルとともに使用することはできません。
- TACACS+ サーバが使用されている場合、パフォーマンスにわずかに影響することがあります。ただし、RADIUS サーバが使用されている場合は、パフォーマンスへの影響はありません。

AAA Double Authentication Secured by AbsoluteTimeout に関する情報

AAA 二重認証

ホストのユーザ名とパスワードを使用して最初の認証を渡すために、AAA 二重認証メカニズムを使用します。2 回目の認証は、チャレンジ ハンドシェイク認証プロトコル（CHAP）またはパスワード認証プロトコル（PAP）認証の後で行われますが、このときはログインユーザ名とそのパスワードが使用されます。最初の認証では、PPP セッション タイムアウトがローカルまたはリモートで設定されていれば、PPP セッション タイムアウトがバーチャル アクセス インターフェイスに適用されます。

AAA Double Authentication Secured by Absolute Timeout 機能により、ユーザ単位のセッション タイムアウトを使用して保護することで、二重の認証メカニズムが確保されます。ユーザ単位のセッション タイムアウトは、一般的な絶対タイムアウト値よりも優先されるほか、カスタマイズすることが可能です。このメカニズムの動作原理は、二重認証のユーザ単位のアクセス コントロール リスト（ACL）と同じです。

AAA Double Authentication Secured by Absolute Timeout の適用方法

AAA Double Authentication Secured by Absolute Timeout の適用

絶対タイムアウトを適用するために、リンク コントロール プロトコル（LCP）のユーザ単位の属性としてログイン ユーザ プロファイルでセッション タイムアウトを設定する必要があります。AAA 二重認証を有効にするには、**access-profile** コマンドを使用します。このコマンド

は、PPPセッション中にインターフェイスにユーザ単位の認可属性を適用するために使用されます。**access-profile** コマンドを使用する前に、LCP のユーザー単位の属性（セッションタイムアウトなど）を再度認可してから、ネットワーク制御プロトコル（NCP）を再度認可して、ACL やルートなどの他の必要な条件を適用します。「AAA Double Authentication Secured by Absolute Timeout の例」を参照してください。

（注） TACACS+ユーザ プロファイルのタイムアウト設定は、RADIUS ユーザ プロファイルの設定とは異なります。RADIUS プロファイルでは、autocommand の **access-profile** とともに 1 つのセッションタイムアウトだけが設定されています。このタイムアウトは EXEC セッションおよび PPP セッションにそれぞれ適用されます。TACACS+ では、タイムアウトはサービス タイプ「exec」および「ppp」（LCP）下で設定し、EXEC セッションと PPP セッションに適用する必要があります。タイムアウトをサービス タイプ「ppp」下でのみ設定すると、そのタイムアウト値は EXEC 認可で使用できず、EXEC セッションに適用されません。

AAA Double Authentication Secured by Absolute Timeout の設定例

例：RADIUS ユーザ プロファイル

次の出力例は、RADIUS ユーザ プロファイルが適用されていることと、AAA 二重認証が絶対タイムアウトによって保護されていることを示しています。

```
aaapbx2 Password = "password1",
 Service-Type = Framed,
 Framed-Protocol = PPP,
 Session-Timeout = 180,
 Idle-Timeout = 180000,
 cisco-avpair = "ip:inacl#1=permit tcp any any eq telnet"
 cisco-avpair = "ip:inacl#2=permit icmp any any"
broker_default Password = "password1",
 Service-Type = Administrative,
 cisco-avpair = "shell:autocmd=access-profile",
 Session-Timeout = 360,
 cisco-avpair = "ip:inacl#1=permit tcp any any"
 cisco-avpair = "ip:inacl#2=permit icmp any any"
broker_merge Password = "password1",
 Service-Type = Administrative,
 cisco-avpair = "shell:autocmd=access-profile merge",
 Session-Timeout = 360,
 cisco-avpair = "ip:inacl#1=permit tcp any any"
 cisco-avpair = "ip:inacl#2=permit icmp any any"
 cisco-avpair = "ip:route#3=10.4.0.0 255.0.0.0"
 cisco-avpair = "ip:route#4=10.5.0.0 255.0.0.0"
 cisco-avpair = "ip:route#5=10.6.0.0 255.0.0.0"
broker_replace Password = "password1",
 Service-Type = Administrative,
 cisco-avpair = "shell:autocmd=access-profile replace",
 Session-Timeout = 360,
```

```
 cisco-avpair = "ip:inacl#1=permit tcp any any"
 cisco-avpair = "ip:inacl#2=permit icmp any any"
 cisco-avpair = "ip:route#3=10.4.0.0 255.0.0.0"
 cisco-avpair = "ip:route#4=10.5.0.0 255.0.0.0"
 cisco-avpair = "ip:route#5=10.6.0.0 255.0.0.0"
```

例：TACACS ユーザ プロファイル

次の出力例は、TACACS+ ユーザ プロファイルが適用されていることと、AAA 二重認証が絶対タイムアウトによって保護されていることを示しています。

リモート ホスト認証

次に、最初の段階の認証でリモート ホストがローカル ホストによって認証され、リモート ホストの認可プロファイルが提供される例を示します。

```
user = aaapbx2
 chap = cleartext Cisco
 pap = cleartext cisco
 login = cleartext cisco
 service = ppp protocol = lcp
  idletime = 3000
  timeout = 3
 service = ppp protocol = ip
  inacl#1="permit tcp any any eq telnet"
 service = ppp protocol = ipx
```

引数のない access-profile コマンドの使用

引数を何も付けずに **access-profile** コマンドを実行すると、古い設定（ユーザー単位およびインターフェイス単位）で見つかったアクセスリストがすべて削除され、アクセスリストの定義のみが新しいプロファイルに存在する状態になります。

```
user = broker_default
 login = cleartext Cisco
 chap = cleartext "cisco"
 service = exec
  autocmd = "access-profile"
! This is the autocommand that executes when broker_default logs in.
  timeout = 6
 service = ppp protocol = lcp
  timeout = 6
 service = ppp protocol = ip
! Put access lists, static routes, and other requirements that are
! needed here. Read the software specifications for details. If you leave
! this blank, the user will have no access lists (not even the ones that were
! installed prior to the creation of this user profile)!
  inacl#1="permit tcp any any"
  inacl#2="permit icmp host 10.0.0.0 any"
 service = ppp protocol = ipx
! Put access lists, static routes, and other requirements that are
! needed here. Read the software specifications for details. If you leave
! this blank, the user will have no access lists (not even the ones that were
! installed prior to the creation of this user profile)!
```

merge キーワードを指定した access-profile コマンドの使用

access-profile コマンドの **merge** キーワードを使用して、すべての古いアクセスリストを削除すると、属性と値（AV）のペアのアップロードおよびインストールが許可されます。**merge** キーワードを使用すると、カスタムのスタティックルート、Service Advertisement Protocol（SAP）フィルタ、プロファイルに必要になることがある他の要件をアップロードできます。**merge** キーワードは競合する設定のあらゆる要素を未処理のままにするため、注意して設定してください。

```
user = broker_merge
 login = cleartext Cisco
 chap = cleartext "cisco"
 service = exec
  autocmd = "access-profile merge"
! This is the autocommand that executes when broker_merge logs in.
  timeout = 6
 service = ppp protocol = lcp
 timeout = 6
 service = ppp protocol = ip
! Put access lists, static routes, and other requirements that are
! needed here. Read the software specifications for details. If you leave
! this blank, the user will have no access lists (not even the ones that were
! installed prior to the creation of this user profile)!
  route#1="10.4.0.0 255.0.0.0"
  route#2="10.5.0.0 255.0.0.0"
  route#3="10.6.0.0 255.0.0.0"
  inacl#5="permit tcp any any"
  inacl#6="permit icmp host 10.60.0.0 any"
 service = ppp protocol = ipx
! Put access lists, static routes, and other requirements that are
! needed here. Read the software specifications for details. If you leave
! this blank, the user will have no access lists (not even the ones that were
! installed prior to the creation of this user profile)!
```

replace キーワードを指定した access-profile コマンドの使用

access-profile コマンドに **replace** キーワードを指定して実行すると、古い設定がすべて削除され、新しい設定がインストールされます。

（注） **access-profile** コマンドを設定すると、アドレスプールとアドレスと AV のペアについて新しい設定がチェックされます。この時点でアドレスは再ネゴシエートできないため、このコマンドはそのようなアドレスと AV のペアを検出すると正常に動作しません。

```
user = broker_replace
 login = cleartext Cisco
 chap = cleartext "cisco"
 service = exec
  autocmd = "access-profile replace"
! This is the autocommand that executes when broker_replace logs in.
  timeout = 6
 service = ppp protocol = lcp
  timeout = 6
 service = ppp protocol = ip
! Put access lists, static routes, and other requirements that are
! needed here. Read the software specifications for details. If you leave
```

```
! this blank, the user will have no access lists (not even the ones that were
! installed prior to the creation of this user profile)!
  route#1="10.7.0.0 255.0.0.0"
  route#2="10.8.0.0 255.0.0.0"
  route#3="10.9.0.0 255.0.0.0"
  inacl#4="permit tcp any any"
 service = ppp protocol = ipx
! Put access lists, static routes, and other requirements that are
! needed here. Read the software specifications for details. If you leave
! this blank, the user will have no access lists (not even the ones that were
! installed prior to the creation of this user profile)!
```

（注） TACACS+ユーザプロファイルのタイムアウト設定は、RADIUSユーザプロファイルの設定とは異なります。RADIUSプロファイルでは、autocommandの **access-profile** とともに1つのセッションタイムアウトだけが設定されています。このタイムアウトはEXECセッションおよびPPPセッションに適用されます。TACACS+ユーザプロファイルでは、タイムアウトはサービス タイプ「exec」および「ppp」（LCP）下で設定し、EXECセッションとPPPセッションにそれぞれ適用する必要があります。タイムアウトをサービス タイプ「ppp」下でのみ設定すると、そのタイムアウト値はEXEC認可で使用できず、EXECセッションに適用されません。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Master Command List, All Releases』
セキュリティ コマンド	• 『Security Command Reference: Commands A to C』 • 『Security Command Reference: Commands D to L』 • 『Security Command Reference: Commands M to R』 • 『Security Command Reference: Commands S to Z』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

AAA Double Authentication Secured by AbsoluteTimeout の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *1 : AAA Double Authentication Secured by AbsoluteTimeout* の機能情報

機能名	リリース	機能情報
AAA Double Authentication Secured by Absolute Timeout		AAA Double Authentication Secured by Absolute Timeout 機能により、ユーザ単位のセッション タイムアウトを使用して保護することで、二重の認証メカニズムが確保されます。この機能では、サービス プロバイダーによるネットワークへの接続を認可された接続のみに最適化し、不要なセッションが接続されないようにすることで、ネットワークへのアクセス全体のセキュリティを高めます。

AAA Double Authentication Secured by AbsoluteTimeout の機能情報

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。