VPN の監視

VPN 接続グラフの監視

ASA の VPN 接続データをグラフ形式または表形式で表示するには、次の画面を参照してください。

[Monitor IPsec Tunnels]

[Monitoring] > [VPN] > [VPN Connection Graphs] > [IPSec Tunnels]

表示や、エクスポートまたは印刷の準備を行う IPsec トンネル タイプのグラフとテーブルを指定します。

[Monitor Sessions]

[Monitoring] > [VPN] > [VPN Connection Graphs] > [Sessions]

表示や、エクスポートまたは印刷の準備を行う VPN セッション タイプのグラフとテーブルを指定します。

VPN 統計の監視

特定のリモートアクセス、または LAN 間セッションの詳細なパラメータおよび統計情報を表示するには、次の画面を参照してください。パラメータと統計情報は、セッションプロトコルによって異なります。また、統計情報テーブルの内容は、選択した接続のタイプによって異なります。各詳細テーブルには、それぞれのセッションの関連パラメータがすべて表示されます。

[Monitor Session] ウィンドウ

[Monitoring] > [VPN] > [VPN Statistics] > [Sessions]

ASA の VPN セッション統計情報を表示します。このペインの 2 番目のテーブルの内容は、[Filter By] リストの選択によって異なります。

（注） 管理者は、非アクティブ状態のユーザー数をトレースし、統計情報を確認できるようになりました。ライセンス数の上限に達することなく、新規ユーザーがログインできるように、最も長時間非アクティブなセッションはアイドル状態であると見なされます（自動的にログオフされます）。これらの統計情報には、**show vpn-sessiondb** CLI コマンドを使用してアクセスすることもできます（『『Cisco ASA Command Reference Guide』の適切なリリース』を参照してください）。

- [All Remote Access]

  このテーブルの値がリモート アクセス（IPsec ソフトウェアおよびハードウェア クライアント）トラフィックに関連することを示します。

- [Username/Connection Profile]：セッションのユーザー名またはログイン名、および接続プロファイル（トンネル グループ）を示します。クライアントが認証にデジタル証明書を使用している場合、フィールドに証明書の Subject CN または Subject OU が表示されます。

- [Group Policy Connection Profile]：セッションのトンネル グループ ポリシー接続プロファイルが表示されます。

- [Assigned IP Address/Public IP Address]：このセッションのリモート クライアントに割り当てられているプライベート（「割り当てられた」）IP アドレスを示します。これは「内部」または「仮想」IP アドレスとも呼ばれ、クライアントはプライベート ネットワーク上のホストとして表示されます。また、このリモート アクセス セッションのクライアントのパブリック IP アドレスも表示します。パブリック IP アドレスは、「外部」IP アドレスとも呼ばれます。通常、これは ISP によってクライアントに割り当てられます。このアドレスにより、クライアントは、パブリック ネットワーク上のホストとして機能することが可能となります。

（注） [Assigned IP Address] フィールドは、クライアントレス SSL VPN セッションには適用されません。ASA（プロキシ）がすべてのトラフィックの送信元になります。ネットワーク拡張モードにおけるハードウェア クライアント セッションの場合、割り当てられた IP アドレスは、ハードウェア クライアントのプライベート/内部ネットワーク インターフェイスのサブネットです。

- [Ping]：ICMP ping（Packet Internet Groper）パケットを送信して、ネットワークの接続をテストします。具体的には、ASA は選択されたホストに ICMP Echo Request メッセージを送信します。ホストが到達可能な場合は、Echo Reply メッセージが返され、ASA はテストしたホストの名前と共に Success メッセージを表示し、さらに要求を送信してから応答を受信するまでの経過時間も表示します。何らかの理由でシステムに到達できない場合（ホストがダウンしている、ホストで ICMP が実行されていない、ルートが設定されていない、

中間ルータがダウンしている、ネットワークがダウンまたは輻輳しているなど）、ASA では、テストしたホストの名前が記された [Error] 画面が表示されます。

- [Logout By]：ログアウトするセッションのフィルタリングに使う基準を選択します。--All Sessions-- 以外を選択した場合、[Logout By] リストの右側のボックスがアクティブになります。値に Protocol for Logout By を選択した場合、ボックスがリストに変わり、ログアウト フィルタとして使用するプロトコル タイプを選択できます。このリストのデフォルト値は IPsec です。Protocol 以外の値を選択した場合は、このボックスに適切な値を入力する必要があります。

[アクティブ AnyConnect セッションのモニタリング（Monitor Active VPN AnyConnect Sessions）]

[Monitoring] > [VPN] > [VPN Statistics] > [Sessions]

ユーザー名、IP アドレス、アドレスタイプ、またはパブリックアドレスでソートされた AnyConnect クライアント セッションを表示します。

[Monitor VPN Session Details]

[Monitoring] > [VPN] > [VPN Statistics] > [Sessions] > [Details]

選択したセッションのコンフィギュレーション設定、統計情報、およびステート情報を表示します。

- [NAC Result and Posture Token]

ASDM では、ASA にネットワーク アドミッション コントロールが設定されている場合にのみ、このカラムに値が表示されます。

- [Accepted]：ACS は正常にリモート ホストのポスチャを検証しました。
- [Rejected]：ACS はリモート ホストのポスチャの検証に失敗しました。
- [Exempted]：ASA に設定されたポスチャ検証免除リストに従って、リモート ホストはポスチャ検証を免除されています。
- [Non-Responsive]：リモート ホストは EAPoUDP Hello メッセージに応答しませんでした。
- [Hold-off]：ポスチャ検証に成功した後、ASA とリモート ホストの EAPoUDP 通信が途絶えました。
- [N/A]：VPN NAC グループ ポリシーに従い、リモート ホストの NAC はディセーブルにされています。
- [Unknown]：ポスチャ検証が進行中です。

ポスチャ トークンは、Access Control Server で設定可能な情報文字列です。ACS は情報提供のために ASA にポスチャ トークンをダウンロードし、システム モニタリング、レポート、デバッグ、およびロギングを支援します。NAC Result に続く一般的なポスチャ トークンは、Healthy、Checkup、Quarantine、Infected または Unknown です。

[Session Details] ペインの [Details] タブには、次のカラムが表示されます。

- [ID]：セッションにダイナミックに割り当てられた一意の ID。ID は、セッションへの ASA のインデックスとして機能します。このインデックスを使用して、セッションに関する情報を維持および表示します。
- [Type]：セッションのタイプ。IKE、IPsec または NAC。
- [Local Addr., Subnet Mask, Protocol, Port, Remote Addr., Subnet Mask, Protocol, and Port]：実際の（ローカル）ピアの両方に割り当てられているアドレスとポートと外部ルーティングのためにそのピアに割り当てられているアドレスとポート。
- [Encryption]：このセッションで使用しているデータ暗号化アルゴリズム（使用している場合）。
- [Assigned IP Address and Public IP Address]：このセッションのリモート ピアに割り当てられているプライベート IP アドレスを示します。内部または仮想 IP アドレスとも呼ばれ、割り当てられている IP アドレスによって、リモート ピアはプライベート ネットワーク上にあるように見えます。2 番目のフィールドには、このセッションのリモート コンピュータのパブリック IP アドレスが表示されます。外部 IP アドレスとも呼ばれ、通常、パブリック IP アドレスは ISP によってリモート コンピュータに割り当てられます。これによって、リモート コンピュータはパブリック ネットワークのホストとして機能できます。
- [Other]：セッションに関連付けられているその他の属性。

次の属性は、IKE セッション、IPsec セッション、および NAC セッションに適用されます。

- [Revalidation Time Interval]：成功した各ポスチャ検証間に必要とされる間隔（秒数）。
- [Time Until Next Revalidation]：最後のポスチャ検証試行が成功しなかった場合は 0 です。それ以外の場合は、Revalidation Time Interval と、正常に完了した直前のポスチャ確認からの経過秒数との差です。
- [Status Query Time Interval]：成功したポスチャ検証またはステータス クエリーの応答と次のステータス クエリーの応答との間に許容される時間（秒数）。ステータス クエリーは、直前のポスチャ確認以降にホストでポスチャが変化したかどうかを確認するために、ASA がリモート ホストに発行する要求です。
- [EAPoUDP Session Age]：最後に成功したポスチャ検証から経過した秒数。
- [Hold-Off Time Remaining]：最後のポスチャ検証が成功した場合は 0 秒です。それ以外の場合は、次回のポスチャ確認試行までの秒数です。
- [Posture Token]：Access Control Server で設定可能な情報文字列。ACS は情報提供のために ASA にポスチャ トークンをダウンロードし、システム モニタリング、レポート、デバッグ、およびロギングを支援します。一般的なポスチャ トークンは、Healthy、Checkup、Quarantine、Infected、または Unknown です。
- [Redirect URL]：ポスチャ検証またはクライアントレス認証が終わると、ACS はセッション用のアクセス ポリシーを ASA にダウンロードします。Redirect URL は、アクセス ポリシー ペイロードのオプションの一部です。ASA は、リモート ホストのすべての HTTP（ポート 80）要求と HTTPS（ポート 443）要求を Redirect URL（存在する場合）にリダイ

レクトします。アクセス ポリシーに Redirect URL が含まれていない場合、ASA はリモート ホストからの HTTP 要求や HTTPS 要求をリダイレクトしません。

Redirect URL は、IPsec セッションが終了するか、ポスチャ再検証が実行されるまで有効です。ACS は、異なる Redirect URL が含まれるか、Redirect URL が含まれない新しいアクセス ポリシーをダウンロードします。

[More]：このボタンを押して、セッションやトンネル グループを再検証または初期化します。

ACL タブには、セッションに一致した ACE が含まれる ACL が表示されます。

[Monitor Cluster Loads]

[Monitoring] > [VPN] > [VPN Statistics] > [Cluster Loads]

VPN ロードバランシング クラスタ内のサーバー間における現在のトラフィックの負荷分散を表示します。サーバーがクラスタの一部でない場合、このサーバーが VPN ロードバランシング クラスタに参加していない旨を伝える情報メッセージが表示されます。

[Monitor Crypto Statistics]

[Monitoring] > [VPN] > [VPN Statistics] > [Crypto Statistics]

ASA で現在アクティブなユーザーと管理者セッションの暗号統計情報を表示します。テーブルの各行は、1 つの暗号統計情報を表します。

[Monitor Compression Statistics]

[Monitoring] > [VPN] > [VPN Statistics] > [Compression Statistics]

ASA で現在アクティブなユーザーと管理者セッションの圧縮統計情報を表示します。テーブルの各行は、1 つの圧縮統計情報を表します。

[Monitor Encryption Statistics]

[Monitoring] > [VPN] > [VPN Statistics] > [Encryption Statistics]

ASA で現在アクティブなユーザーと管理者セッションが使用しているデータ暗号化アルゴリズムを表示します。テーブルの各行は、1 つの暗号化アルゴリズム タイプを表します。

[Monitor Global IKE/IPsec Statistics]

[Monitoring] > [VPN] > [VPN Statistics] > [Global IKE/IPSec Statistics]

ASA で現在アクティブなユーザーと管理者セッションのグローバル IKE/IPsec 統計情報を表示します。テーブルの各行は、1 つのグローバル統計情報を表します。

[Monitor NAC Session Summary]

アクティブな累積ネットワーク アドミッション コントロール セッションを表示します。

- [Active NAC Sessions]：ポスチャ検証の対象のリモート ピアに関する一般的な統計情報。

- [Cumulative NAC Sessions]：現在ポスチャ検証の対象か、または以前から対象だったリモート ピアに関する一般的な統計情報。
- [Accepted]：ポスチャ検証に成功し、Access Control Server によってアクセス ポリシーが与えられたピアの数。
- [Rejected]：ポスチャ検証に失敗し、Access Control Server によってアクセス ポリシーが与えられなかったピアの数。
- [Exempted]：ASA で設定された [Posture Validation Exception] リストのエントリと一致しているため、ポスチャ検証の対象になっていないピアの数。
- [Non-responsive]：Extensible Authentication Protocol（EAP）over UDP のポスチャ検証要求に応答しないピアの数。CTA が実行されていないピアは、この要求に応答しません。ASA のコンフィギュレーションがクライアントレス ホストをサポートしている場合、Access Control Server は、クライアントレス ホストに関連付けられているアクセス ポリシーをこれらのピアの ASA にダウンロードします。クライアントレス ホストをサポートしていない場合、ASA は NAC デフォルト ポリシーを割り当てます。
- [Hold-off]：ポスチャ検証が成功した後に、ASA が EAPoUDP 通信を失ったピアの数。NAC Hold Timer 属性（[Configuration] > [VPN] > [NAC]）は、このタイプのイベントと次のポスチャ検証試行との間の遅延時間を判定します。
- [N/A]：VPN NAC グループ ポリシーに従って NAC が無効になっているピアの数。
- [Revalidate All]：ピアのポスチャまたは割り当てられているアクセス ポリシー（ダウンロードされた ACL）が変更された場合にクリックします。このボタンをクリックすると、ASA によって管理されるすべての NAC セッションの新しい無条件ポスチャ検証が開始されます。このボタンをクリックするまで各セッションに対して有効だったポスチャ検証と割り当てられているアクセス ポリシーは、新しいポスチャ検証が成功または失敗するまで有効のままとなります。ポスチャ検証から免除されているセッションには、このボタンをクリックしても影響はありません。
- [Initialize All]：ピアのポスチャまたは割り当てられているアクセス ポリシー（ダウンロードされた ACL）が変更され、セッションに割り当てられているリソースをクリアする場合にクリックします。このボタンをクリックすると、ASA によって管理されるすべての NAC セッションのポスチャ検証で使用される、EAPoUDP アソシエーションと割り当てられたアクセス ポリシーがパージされ、新しい無条件のポスチャ検証が開始されます。再検証中には NAC のデフォルトの ACL が有効となるため、セッションを初期化するとユーザー トラフィックに影響する場合があります。ポスチャ検証から免除されているセッションには、このボタンをクリックしても影響はありません。

[Monitor Protocol Statistics]

[Monitoring] > [VPN] > [VPN Statistics] > [Protocol Statistics]

ASA で現在アクティブなユーザーと管理者セッションが使用しているプロトコルを表示します。テーブルの各行は、1 つのプロトコル タイプを表します。

[Monitor VLAN Mapping Sessions]

使用中の各グループ ポリシーの Restrict Access to VLAN パラメータの値で判別された、出力 VLAN に割り当てられているセッション数を表示します。ASA はすべてのトラフィックを指定された VLAN に転送します。

[Monitor SSO Statistics for Clientless SSL VPN Session]

[Monitoring] > [VPN] > [WebVPN] > [SSO Statistics]

ASA に設定されている現在アクティブなシングル サインオン（SSO）サーバーの SSO 統計情報を表示します。

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。