VPN のモニタリング

この章では、VPN モニタリング パラメータと、次に示す統計情報の使用方法について説明します。

- 特定のネットワーク（クライアント）リモート アクセス、サイト間 VPN、クライアントレス SSL VPN、および電子メール プロキシ セッションの VPN 統計情報
- トンネル グループの暗号化統計情報
- トンネル グループのプロトコル統計情報
- グローバル IPsec および IKE の統計情報
- IPsec、IKE、SSL およびその他のプロトコルの暗号統計情報
- クラスタ VPN サーバ負荷の統計情報

VPN 接続グラフ

ASA の VPN 接続データをグラフ形式または表形式で表示します。

IPsec Tunnels

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

このペインを使用して、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。

フィールド

- [Graph Window Title]：[Show Graphs] をクリックしたときに、ペインに表示されるデフォルトのタイトルを表示します。この属性は、特に印刷またはエクスポートする前にペインでデータを確認するときに便利です。タイトルを変更するには、ドロップダウン リストから他のタイトルを選択するか、タイトルを入力します。
- [Available Graphs]：表示できるアクティブなトンネルのタイプを示します。1 つのペインにまとめて表示するタイプごとにエントリを選択し、[Add] をクリックします。
- [Selected Graphs]：選択したトンネルのタイプを示します。

  [Show Graphs] をクリックすると、ASDM は、リストされているアクティブなトンネル タイプを 1 つのペインに表示します。

  強調表示されているエントリは、[Remove] をクリックした場合にリストから削除されるトンネルのタイプを示します。

- [Add] : [Available Graphs] カラムから [Selected Graphs] カラムに、選択したトンネル タイプを移動します。
- [Remove] : [Selected Graphs] カラムから [Available Graphs] カラムに、選択したトンネル タイプを移動します。
- [Show Graphs] : [Selected Graphs] カラムに表示されるトンネル タイプのグラフで構成されるペインを表示します。表示されるペイン内の各タイプには、[Graph] タブと [Table] タブがあり、アクティブなトンネル データの表示をクリックして切り替えられます。

Sessions

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

このペインを使用して、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。

フィールド

- [Graph Window Title] : [Show Graphs] をクリックしたときに、ペインに表示されるデフォルトのタイトルを表示します。この属性は、特に印刷またはエクスポートする前にペインでデータを確認するときに便利です。タイトルを変更するには、ドロップダウン リストから他のタイトルを選択するか、またはタイトルを入力します。
- [Available Graphs] : 表示できるアクティブなセッションのタイプを示します。1 つのペインにまとめて表示するタイプごとに、このボックスのエントリをクリックし、[Add] をクリックします。
- [Selected Graphs] : 選択したアクティブなセッションのタイプを示します。

  [Show Graphs] をクリックすると、ASDM は、このボックスにリストされているアクティブなセッション タイプを 1 つのペインにすべて表示します。

  強調表示されているエントリは、[Remove] をクリックするとリストから削除されるセッションのタイプを示します。
- [Add] : [Available Graphs] ボックスから [Selected Graphs] ボックスに、選択したセッション タイプを移動します。
- [Remove] : [Selected Graphs] ボックスから [Available Graphs] ボックスに、選択したセッション タイプを移動します。
- [Show Graphs] : [Selected Graphs] ボックスに表示されるセッション タイプのグラフで構成されるペインを表示します。表示されるペイン内の各タイプには、[Graph] タブと [Table] タブがあり、アクティブなセッション データの表示をクリックして切り替えられます。

VPN 統計情報

これらのペインには、特定のリモート アクセス、LAN 間、クライアントレス SSL VPN、または電子メール プロキシ セッションの詳細なパラメータおよび統計情報が表示されます。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。

[Sessions] ウィンドウ

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

このペインを使用して、適応型セキュリティ アプライアンスの VPN セッション統計情報を表示します。

フィールド

- [Session types]（ラベルなし）：各タイプの現在アクティブなセッションの数、合計制限および合計累積セッション数を一覧表示します。
  - [All Remote Access]：リモート アクセス セッションの数を示します。
  - [Site-to-Site]：LAN 間セッションの数を示します。
  - [Clientless SSL VPN]：クライアントレス ブラウザベースの VPN セッションの数を示します。
  - [AnyConnect Client]：クライアントベースの SSL VPN セッションの数を示します。バージョン 8.x 以降の ASA を使用する場合、バージョン 2.x 以降の AnyConnect SSL VPN クライアントとなります。
  - [SSL VPN–Inactive]：リモート コンピュータ上で非アクティブになっている SSL VPN セッションの数を示します。

    （注）　管理者は、非アクティブ状態のユーザ数をトレースし、統計情報を確認できるようになりました。ライセンス キャパシティに到達せず、新規ユーザがログインできるように、最長時間非アクティブなセッションはアイドルとマークされます（さらに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（『Cisco Security Appliance Command Reference Guide』を参照）を使用してアクセスすることもできます。

  - [SSL VPN–Total]：クライアントベースおよびクライアントレスの SSL VPN セッションの数を示します。
  - [E-mail Proxy]：電子メール プロキシ セッションの数を示します。
  - [VPN Load Balancing]：ロードバランシングが行われている VPN セッションの数を示します。
  - [Total]：アクティブな同時セッションの合計数を示します。
  - [Total Cumulative]：最後に ASA をリブートまたはリセットしたときからの累積セッション数を示します。
- [Filter By]：次のテーブル内の統計情報が示すセッションのタイプを指定します。
  - [Session type]（ラベルなし）：監視するセッション タイプを指定します。次のセッションのいずれかでフィルタ処理できます。IPsec サイツーサイト、すべてのリモート アクセス、AnyConnect クライアント、クライアントレス SSL VPN、IPsec (IKEv1) リモート アクセス、OSPFv3 IPsec、または電子メール プロキシ。

    選択するセッション タイプに応じて、結果テーブルのカラム ヘッダーが変わります。
  - [Filter name]（ラベルなし）：適用するフィルタの名前を指定します。Session filter リストに --All Sessions-- を指定した場合、このフィールドは使用できません。他の Session filter を選択した場合、このフィールドをブランクにできません。

    IPsec サイトツーサイト、AnyConnect クライアント、クライアントレス SSL VPN、または OSPFv3 IPsec のセッション タイプ フィルタを選択した場合、[Assigned IP Address Type] または [Public IP Address Type] でフィルタ処理することができます。

- [Filer value]：使用しているフィルタに対応する値を入力します。

  [Assigned IP Address Type] または [Public IP Address Type] でフィルタ処理する場合、このフィールドに IPv4 または IPv6 の IP アドレス タイプを指定します。

- [Filter]：フィルタリング オペレーションを実行します。

このペインの 2 番目のテーブル（これもラベルはありません）の内容は、[Filter By] リストの選択によって異なります。次のリストで、箇条書きの第 1 レベルは [Filter By] の選択を、第 2 レベルはこのテーブルのカラム ヘッダーを示します。

- [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 アドレスが表示されます。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。

  - [Protocol/Encryption]：このセッションで使用しているプロトコルとデータ暗号化アルゴリズムがある場合に表示されます。
  - [Login Time/Duration]：セッションがログインした日付と時刻（MMM DD HH:MM:SS）、およびセッションの長さを表示します。時刻の表示は 24 時間表示です。
  - [Client (Peer) Type/Version]：ユーザ名でソートされた接続されたクライアントのソフトウェア バージョン番号（例：rel.7.0_int 50）を示します。
  - [Bytes Tx/Bytes Rx]：ASA とリモート ピアまたはクライアントの間で送受信される合計バイト数を表示します。
- [IPsec Site-to-Site]：このテーブルの値が LAN 間のトラフィックに関連することを示します。
  - [Connection Profile/IP Address]：トンネル グループの名前とピアの IP アドレスを示します。
  - [Protocol/Encryption]：このセッションで使用しているプロトコルとデータ暗号化アルゴリズムがある場合に表示されます。
  - [Login Time/Duration]：セッションがログインした日付と時刻（MMM DD HH:MM:SS）、およびセッションの長さを表示します。時刻の表示は 24 時間表示です。
  - [Bytes Tx/Bytes Rx]：ASA とリモート ピアまたはクライアントの間で送受信される合計バイト数を表示します。

- [Clientless SSL VPN]：このテーブルの値がクライアントレス SSL VPN トラフィックに関連することを示します。
  - [Username/IP Address]：セッションのユーザ名またはログイン名、およびクライアントの IP アドレスを示します。
  - [Group Policy Connection Profile]：トンネル グループ ポリシーの接続プロファイルを表示します。
  - [Protocol/Encryption]：このセッションで使用しているプロトコルとデータ暗号化アルゴリズムがある場合に表示されます。
  - [Login Time/Duration]：セッションがログインした日付と時刻（MMM DD HH:MM:SS）、およびセッションの長さを表示します。時刻の表示は 24 時間表示です。
  - [Bytes Tx/Bytes Rx]：ASA とリモート ピアまたはクライアントの間で送受信される合計バイト数を表示します。
- [SSL VPN Client]：このテーブルの値が SSL VPN クライアント セッションのトラフィックに関連することを示します
  - [Username/IP Address]：セッションのユーザ名またはログイン名、およびクライアントの IP アドレスを示します。
  - [Group Policy Connection Profile]：トンネル グループ ポリシーの接続プロファイルを表示します。
  - [Protocol/Encryption]：このセッションで使用しているプロトコルとデータ暗号化アルゴリズムがある場合に表示されます。
  - [Login Time/Duration]：セッションがログインした日付と時刻（MMM DD HH:MM:SS）、およびセッションの長さを表示します。時刻の表示は 24 時間表示です。
  - [Bytes Tx/Bytes Rx]：ASA とリモート ピアまたはクライアントの間で送受信される合計バイト数を表示します。
- [E-Mail Proxy]：このテーブルの値がクライアントレス SSL VPN セッションのトラフィックに関連することを示します。
  - [Username/IP Address]：セッションのユーザ名またはログイン名、およびクライアントの IP アドレスを示します。
  - [Protocol/Encryption]：このセッションで使用しているプロトコルとデータ暗号化アルゴリズムがある場合に表示されます。
  - [Login Time/Duration]：セッションがログインした日付と時刻（MMM DD HH:MM:SS）、およびセッションの長さを表示します。時刻の表示は 24 時間表示です。
  - [Bytes Tx/Bytes Rx]：ASA とリモート ピアまたはクライアントの間で送受信される合計バイト数を表示します。

この項の残りの部分では、テーブルの近くや下にあるボタンおよびフィールドについて説明します。

- [Details]：選択したセッションの詳細を表示します。パラメータと値は、セッションのタイプによって異なります。
- [Logout]：選択したセッションを終了します。
- [Ping]：ネットワークの接続テストのために、ICMP `ping`（Packet Internet Groper）パケットを送信します。具体的には、ASA は、選択したホストに 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、Echo Reply メッセージを返し、ASA はテストしたホストの名前が記された Success メッセージ、および要求を送信して応答を受信するまでの経過時間を表示します。何らかの理由でシステムが到達不可能な場合（ホストがダウンしている、ICMP がホストで実

行していない、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 には、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。
- [Logout Sessions]：指定した Logout By 基準に合うすべてのセッションを終了します。
- [Refresh]：画面とそのデータを更新します。日付と時刻は、画面が最後に更新された日時を示します。

アクティブな AnyConnect セッションの表示

ステップ 1　[Monitoring] > [VPN] > [VPN Statistics] > [Sessions] を選択します。

ステップ 2　[Filter By] フィールドで、[AnyConnect Client] を選択します。

ステップ 3　[Session Filter] フィールド（ラベルなし）で、[Filter By] フィールドの横にある、さらにフィルタを調整するために使用するセッション タイプを選択します。次に、[Session Filter] フィールドの右側の [Session Value] フィールド（ラベルなし）を入力します。使用可能なセッション フィルタおよびセッション値は、次のとおりです。

セッション フィルタ	セッション値
Username	その後、ソートするユーザ名を入力します。
Assigned IP Address	割り当てられた IP アドレスとは、ASA から AnyConnect クライアントへの接続で割り当てられた IP アドレスです。 ソートする IPv4 または IPv6 のアドレスを入力します。
Assigned IP Address Type	IP バージョン 4 または IP バージョン 6 を選択します。
Public Address	パブリック IP アドレスは、企業からエンドポイントに割り当てられた IP アドレスです。 ソートする IPv4 または IPv6 のアドレスを入力します。
Public Address Type	IP バージョン 4 または IP バージョン 6 を選択します。
Encryption	セッションの暗号化タイプを選択します。
Connection Status	[Active] または [Inactive] を選択します。

ステップ 4　[Filter] をクリックします。

VPN セッションの詳細の表示

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

[Session Details] ペインには、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が表示されます。

[Session Details] ペインの一番上にある [Remote Detailed] テーブルには、次のカラムが表示されます。

- [Username] : セッションに関連付けられているユーザ名またはログイン名を示します。リモート ピア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 and Tunnel Group] : セッションに割り当てられているグループ ポリシーとセッションが確立されたトンネル グループの名前。
- [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。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。
- [Protocol/Encryption] : このセッションで使用しているプロトコルとデータ暗号化アルゴリズム（ある場合）。
- [Login Time and Duration] : セッションの開始日時とセッションの長さ。セッションの開始時刻は、24 時間表記で表示されます。
- [Client Type and Version] : リモート コンピュータのクライアントのタイプおよびソフトウェア バージョン番号（例 : rel.7.0_int 50）。
- [Bytes Tx and Bytes Rx] : ASA とリモート ピアの間で送受信される合計バイト数を示します。
- [NAC Result and Posture Token] : ASDM では、ASA でネットワーク アドミッション コントロールを設定している場合にだけ、このカラムに値が表示されます。

  [NAC Result] には、次の値のいずれかが表示されます。

  - [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ました。
  - [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（ある場合）。
- [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 セッションに適用されます。

  次の属性は、IPsec セッションに適用されます。

  次の属性は、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なしの認証が終わると、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）要求および 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 要求および 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。

Cluster Loads

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

このペインを使用して、VPN ロードバランシング クラスタ内のサーバ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。サーバがクラスタの一部でない場合、このサーバが 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。

フィールド

- [VPN Cluster Loads] : VPN ロードバランシング クラスタの現在の負荷分散を表示します。カラム ヘッダーをクリックすると、選択したカラムをソート キーとしてテーブルがソートされます。
  - [Public IP Address] : 外部から可視となっているサーバの IP アドレスを表示します。
  - [Role] : このサーバが、クラスタ内のマスター デバイスかバックアップ デバイスかを示します。
  - [Priority] : クラスタ内のこのサーバに割り当てられているプライオリティを示します。プライオリティは、1（最低）～ 10（最高）の範囲の整数である必要があります。プライオリティは、VPN ロード バランシング クラスタ内でクラスタのマスターまたはプライマリ デバイスになるデバイスを決定する方法の 1 つとして、マスター選出プロセスで使用されます。
  - [Model] : このサーバの ASA のモデル名と番号を示します。
  - [IPsec Load %] : サーバの容量に基づいて、サーバの合計容量のうち使用中の割合を示します。
  - [SSL Load %] : サーバの容量に基づいて、SSL サーバの合計容量のうち使用中の割合を示します。
  - [IPsec Sessions] : 現在アクティブなセッションの数を示します。
  - [SSL Sessions] : 現在アクティブなセッションの数を示します。
- [Refresh] : テーブルに更新後の統計情報をロードします。

Crypto Statistics

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

このペインには、ASA で現在アクティブなユーザおよび管理者セッションの暗号統計情報が表示されます。テーブルの各行は、1 つの暗号統計情報を表します。

フィールド

- [Show Statistics For] : 特定のプロトコル、[IKE Protocol]（デフォルト）、[IPsec Protocol]、[SSL Protocol]、または他のプロトコルを選択します。
- [Statistics] : 現在アクティブなセッションで使用中のすべてのプロトコルの統計情報を示します。
  - [Statistic] : 統計変数の名前を一覧表示します。このカラムの内容は、Show Statistics For パラメータで選択した値によって異なります。
  - [Value] : この行にある統計情報の数値。
- [Refresh] : [Crypto Statistics] テーブルに表示される統計情報を更新します。

Compression Statistics

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

このペインには、ASA で現在アクティブなユーザおよび管理者セッションの圧縮統計情報が表示されます。テーブルの各行は、1 つの圧縮統計情報を表します。

フィールド

- [Show Statistics For]: クライアントレス SSL VPN または SSL VPN クライアント セッションの圧縮統計情報を選択できます。
- [Statistics]：選択した VPN タイプの統計情報をすべて表示します。
  - [Statistic]：統計変数の名前を一覧表示します。このカラムの内容は、Show Statistics For パラメータで選択した値によって異なります。
  - [Value]：この行にある統計情報の数値。
- [Refresh]：[Compression Statistics] テーブルに表示される統計情報を更新します。

Encryption Statistics

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

このペインには、ASA で、現在アクティブなユーザおよび管理者セッションによって使用されるデータ暗号化アルゴリズムが表示されます。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。

フィールド

- [Show Statistics For]：特定のサーバやグループ、またはすべてのトンネル グループを選択します。
- [Encryption Statistics]：現在アクティブなセッションで使用中のすべてのデータ暗号化アルゴリズムの統計情報を示します。
  - [Encryption Algorithm]：この行の統計情報が適用される暗号化アルゴリズムを一覧表示します。
  - [Sessions]：このアルゴリズムを使用するセッションの数を一覧表示します。
  - [Percentage]：アクティブなセッションの合計に対する、このアルゴリズムを使用しているセッションの割合を数値で示します。このカラムの合計は 100 % になります（端数は処理）。
- [Total Active Sessions]：現在アクティブなセッションの数を示します。
- [Cumulative Sessions]：ASA を最後にブートまたはリセットしたときからのセッションの合計数を示します。
- [Refresh]：[Encryption Statistics] テーブルに表示される統計情報を更新します。

Global IKE/IPsec Statistics

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

このペインには、ASA で現在アクティブなユーザおよび管理者セッションのグローバル IKE/IPsec 統計情報が表示されます。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。

フィールド

- [Show Statistics For]：特定のプロトコル、[IKE Protocol]（デフォルト）または [IPsec Protocol] を選択します。
- [Statistics]：現在アクティブなセッションで使用中のすべてのプロトコルの統計情報を示します。
  - [Statistic]：統計変数の名前を一覧表示します。このカラムの内容は、Show Statistics For パラメータで選択した値によって異なります。
  - [Value]：この行にある統計情報の数値。

- [Refresh]：[Global IKE/IPsec Statistics] テーブルに表示される統計情報を更新します。

NAC Session Summary

[NAC Session Summary] ペインでは、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 セッションを表示できます。

フィールド

- [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] リストのエントリに一致するため、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 ホストをサポートする場合、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のポスチャ検証を開始します。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ているアクセス ポリシーをパージし、新しい無条件のポスチャ検証を開始します。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 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。

Protocol Statistics

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

このペインには、ASA で現在アクティブなユーザおよび管理者セッションによって使用されるプロトコルが表示されます。テーブルの各行は、1 つのプロトコル タイプを表します。

フィールド

- [Show Statistics For]：特定のサーバやグループ、またはすべてのトンネル グループを選択します。
- [Protocol Statistics]：現在アクティブなセッションで使用中のすべてのプロトコルの統計情報を示します。
  - [Protocol]：この行の統計情報が適用されるプロトコルを一覧表示します。
  - [Sessions]：このプロトコルを使用するセッションの数を一覧表示します。
  - [Percentage]：アクティブなセッションの合計に対する、このプロトコルを使用しているセッションの割合を数値で示します。このカラムの合計は 100 % になります（端数は処理）。
- [Total Active Tunnel]：現在アクティブなセッションの数を示します。
- [Cumulative Tunnels]：ASA を最後にブートまたはリセットしたときからのセッションの合計数を示します。
- [Refresh]：[Protocol Statistics] テーブルに表示される統計情報を更新します。

VLAN Mapping Sessions

このペインには、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が表示されます。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。

フィールド

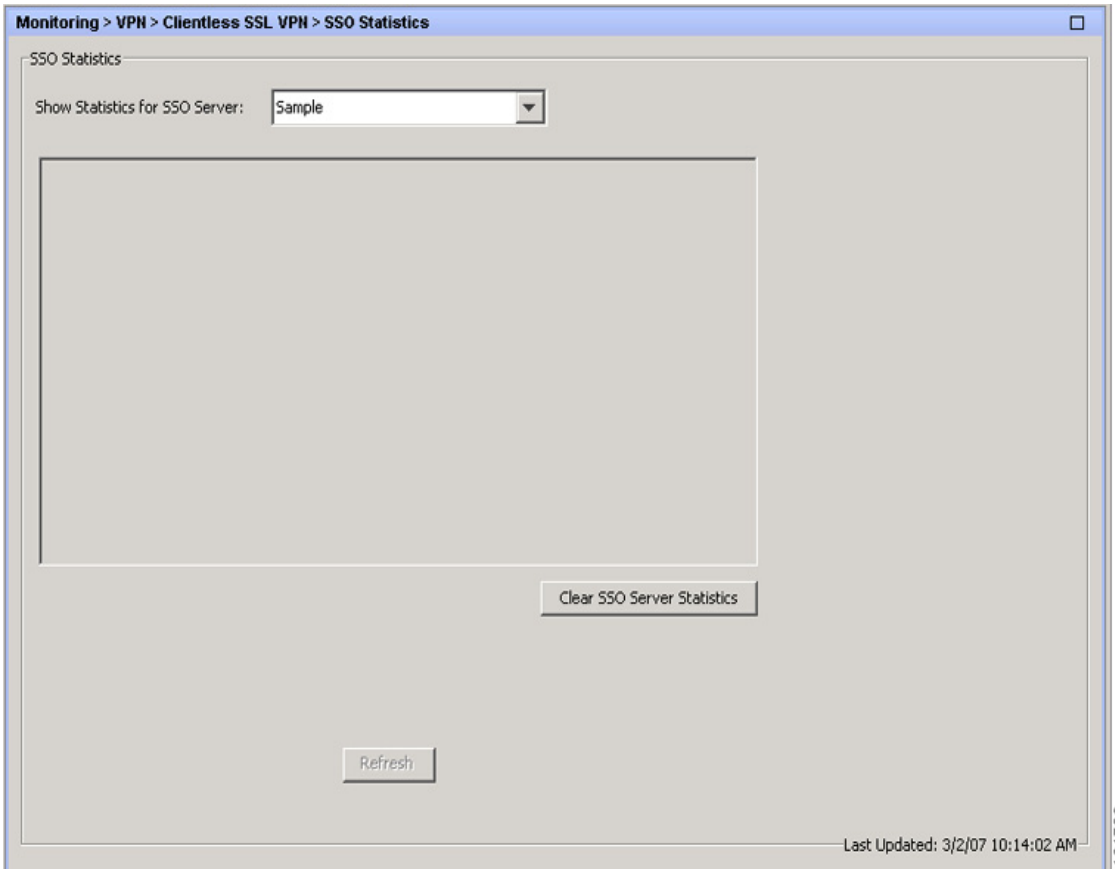
- [Active VLAN Mapping Sessions]：出力 VLAN に割り当てられている VPN セッションの数。

SSO Statistics for Clientless SSL VPN Session

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

このペインには、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）サーバの SSO 統計情報が表示されます。

（注） これらの統計情報は、SiteMinder サーバおよび SAML Browser Post Profile サーバの SSO に関するものだけです。



フィールド

- [Show Statistics For SSO Server]：SSO サーバを選択します。
- [SSO Statistics]：選択した SSO サーバで現在アクティブなセッションの統計情報を示します。次のような SSO 統計情報が表示されます。
  - SSO サーバの名前
  - SSO サーバのタイプ
  - 認証スキームのバージョン（SiteMinder サーバ）
  - Web エージェントの URL（SiteMinder サーバ）
  - アサーション コンシューマの URL（SAML POST サーバ）
  - 発行元（SAML POST サーバ）
  - 保留中の要求の数
  - 認可要求数
  - 再送信の数
  - 受け入れ数
  - 拒否数
  - タイムアウトの回数
  - 認識されない応答の数

- [Refresh]：[SSO Statistics] テーブルに表示される統計情報を更新します。
- [Clear SSO Server Statistics]：表示されているサーバの統計情報をリセットします。

VPN Connection Status for the Easy VPN Client

このペインを使用して、Easy VPN クライアントとして設定されている ASA のステータスを表示します。この機能は ASA 5505 だけに適用されます。

フィールド

[VPN Client Detail]：Easy VPN クライアントとして設定されている ASA 5505 の設定情報を表示します。

[Connect]：クライアント接続を確立します。

[Refresh]：[VPN Client Detail] パネルに表示されている情報をリフレッシュします。