



VPN のモニタリング

VPN のモニタリング セクションには、次のパラメータと統計情報が表示されます。

- 特定のリモート アクセス、LAN 間、WebVPN 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 Connection Graphs

セキュリティ アプライアンスの 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

このウィンドウを使用して、表示したり、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、ウィンドウに表示するデフォルトのタイトルを表示します。このアトリビュートは、特に印刷またはエクスポートする前にウィンドウ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トンネルのタイプを示します。1 つのウィンドウ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、このボックスにリストされているアクティブなトンネルタイプを 1 つのウィンドウに表示します。
強調表示されているエントリは、Remove をクリックすると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 ボックスから Selected Graphs ボックスに、選択したトンネル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、選択したトンネルタイプを移動します。
- **Show Graphs: Selected Graphs** : Selected Graphs ボックスに表示されるトンネルタイプのグラフで構成されるウィンドウを表示します。表示されるウィンドウの各タイプには、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ることができます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	—	•	—	—

Sessions

Monitoring > VPN > VPN Connection Graphs > Sessions

このパネルを使用して、表示したり、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、ウィンドウに表示するデフォルトのタイトルを示します。このアトリビュートは、特に印刷またはエクスポートする前にウィンドウ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 つのウィンドウ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 つのウィンドウ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ウィンドウを表示します。表示されるウィンドウの各タイプには、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ることができます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	—	•	—	—

VPN Statistics

これらのパネルには、特定のリモート アクセス、LAN 間、WebVPN 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

Monitoring > VPN > VPN Statistics > Sessions

このパネルを使用して、このサーバのセッション統計情報を表示します。

フィールド

- **Session types (unlabeled)** : 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。
 - Remote Access : リモート アクセス セッションの数を示します。
 - LAN-to-LAN : LAN 間セッションの数を示します。
 - WebVPN : WebVPN セッションの数を表示します。
 - SSL VPN Client : SSL VPN Client (SVC) 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。
 - 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 : 最後にセキュリティ アプライアンス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** : 次のテーブルの統計情報が存在するセッションのタイプを指定します。
 - Session type (unlabeled) : 監視するセッションタイプを指定します。デフォルトは、Remote Access です。
 - Session filter (unlabeled) : 次のテーブルでフィルタをオンにするカラム ヘッダーを指定します。デフォルトは、--All Sessions-- です。
 - Filter name (unlabeled) : 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することはできません。
 - Filter : フィルタリング オペレーションを実行します。

このパネルの 2 番目のテーブル (同様にラベルなし) 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。

- **Remote Access** : このテーブルの値がリモート アクセス トラフィックに関連することを示します。
 - Username/Tunnel Group : セッションのユーザ名またはログイン名、およびトンネル 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。
 - 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がある場合に表示します。
 - 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) と、セッションの長さを表示します。時刻は 24 時間表記で表示されます。
 - Client Type/Version : 接続されているクライアントのタイプとソフトウェア バージョン番号 (rel. 7.0_int 50 など) をユーザ名別に表示します。
 - Bytes Tx/Bytes Rx : セキュリティ アプライアンスとリモート 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。
 - NAC Result and Posture Token : セキュリティ アプライアンスでネットワーク アドミッション コントロールを設定している場合のみ、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、リモート ホストのポスチャを正常に検証しました。
Rejected : ACS は、リモート ホストのポスチャを正常に検証できませんでした。
Exempted : リモート ホストは、セキュリティ アプライアンスで設定した Posture Validation Exception リストに従って、ポスチャ検証から除外されています。
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 : セキュリティ アプライアンスは、ポスチャ検証に成功した後、リモート ホストとの EAPoUDP 通信を失いました。
N/A : NAC は、VPN NAC グループ ポリシーに従ってリモート ホストでディセーブルになっています。
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、システムの監視やレポート作成、デバッグ、ロギングに役立つ情報の取得を目的として、ポスチャ トークンをセキュリティ アプライアンスにダウンロードします。NAC Result フィールドに続く Posture Token フィールドの一般的な値は、Healthy、Checkup、Quarantine、Infected または Unknown です。
- LAN-to-LAN : 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。
 - Tunnel Group/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) と、セッションの長さを表示します。時刻は 24 時間表記で表示されます。
 - Bytes Tx/Bytes Rx : セキュリティ アプライアンスとリモート 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示します。
- WebVPN : このテーブルの値が WebVPN 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) と、セッションの長さを表示します。時刻は 24 時間表記で表示されます。
 - Client Type/Version : 接続されているクライアントのタイプとソフトウェア バージョン番号 (rel. 7.0_int 50 など) をユーザ名別に表示します。
 - Bytes Tx/Bytes Rx : セキュリティ アプライアンスとリモート 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示します。
- E-Mail Proxy : このテーブルの値が WebVPN 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) と、セッションの長さを表示します。時刻は 24 時間表記で表示されます。
- Client Type/Version : 接続されているクライアントのタイプとソフトウェア バージョン番号 (rel. 7.0_int 50 など) をユーザ名別に表示します。
- Bytes Tx/Bytes Rx : セキュリティアプライアンス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、セキュリティアプライアンスは、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、セキュリティアプライアンス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)、セキュリティアプライアンスには、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 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。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Sessions Details

Monitoring > VPN > VPN Statistics > Sessions >Details

Session Details ウィンドウには、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タ情報が表示されます。

Session Details ウィンドウの一番上にある 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がある場合に表示されます。
- **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上のクライアントのタイプとソフトウェアバージョン番号 (rel. 7.0_int 50 など)。
- **Bytes Tx and Bytes Rx** : セキュリティ アプライアンス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、セキュリティ アプライアンスでネットワーク アドミッション コントロールを設定している場合のみ、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、リモートホストのポストチャを正常に検証しました。
- **Rejected** : ACS は、リモートホストのポストチャを正常に検証できませんでした。
- **Exempted** : リモートホストは、セキュリティ アプライアンスで設定した Posture Validation Exception リストに従って、ポストチャ検証から除外されています。
- **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** : セキュリティ アプライアンスは、ポストチャ検証に成功した後、リモートホストとの EAPoUDP 通信を失いました。
- **N/A** : NAC は、VPN NAC グループポリシーに従ってリモートホストで無効になっています。
- **Unknown** : ポストチャ検証が進行中です。

ポストチャトークンは、Access Control Server で設定可能な情報文字列です。ACS は、システムの監視やレポート作成、デバッグ、ロギングに役立つ情報の取得を目的として、ポストチャトークンをセキュリティ アプライアンスにダウンロードします。NAC Result に続く一般的なポストチャトークンは、Healthy、Checkup、Quarantine、Infected または Unknown です。

Session Details ウィンドウの 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、セッションへのセキュリティ アプライアンス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アトリビュート。
次のアトリビュートは、IKE セッションに適用されます。
次のアトリビュートは、IPSec セッションに適用されます。
次のアトリビュートは、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。成功した場合は、Revalidation Time Interval と最後に成功したポスチャ検証から経過した秒数との差となります。
 - 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、最後のポスチャ検証からポスチャで変更があったかどうかを示すために、セキュリティ アプライアンスがリモート ホストに行う要求です。
 - 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。成功しなかった場合は、次のポスチャ検証試行までの残り秒数になります。
 - Posture Token : Access Control Server で設定可能な情報文字列。ACS は、システムの監視やレポート作成、デバッグ、ロギングに役立つ情報の取得を目的として、ポスチャ トークンをセキュリティ アプライアンスにダウンロードします。一般的なポスチャ トークンには、Healthy、Checkup、Quarantine、Infected、Unknown があります。
 - 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 ポリシーをセキュリティ アプライアンス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。セキュリティ アプライアンスは、リモート ホストの HTTP (ポート 80) および HTTPS (ポート 443) 要求がある場合に、Redirect URL 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、セキュリティ アプライアンスはリモート ホストから HTTP 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が検証されるまで有効です。そのため、ACS は新しいアクセス ポリシーをダウンロードしますが、新しいアクセス ポリシーには、別のリダイレクト URL が含まれている場合もまったく含まれていない場合もあります。
- 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。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	—	•	—	—

Sub-session Details – NAC Details

Monitoring > VPN > VPN Statistics > Sessions > Details > More

NAC Details ウィンドウでは、NAC セッションの統計情報およびステート情報を表示したり、セッションやトンネル グループを再検証または初期化することができます。

このウィンドウの統計情報およびステート情報のアトリビュートは次のとおりです。

- Reval Int (T): 再検証の時間間隔。成功した各ポスチャ検証の間に必要とされる間隔(秒数)です。

- **Reval Left (T)** : 次の再検証までの時間。最後のポストチャ検証試行が失敗した場合は 0 です。成功した場合は、**Revalidation Time Interval** と最後に成功したポストチャ検証から経過した秒数との差となります。
- **SQ Int (T)** : ステータス クエリーの時間間隔。成功したポスト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、最後のポストチャ検証からポストチャで変更があったかどうかを示すために、セキュリティ アプライアンスがリモート ホストに行く要求です。
- **EoU Age (T)** : EAPoUDP セッション経過時間。最後に成功したポストチャ検証から経過した秒数。
- **Hold Left (T)** : 残りの遅延時間。最後のポストチャ検証が成功した場合は 0 秒です。失敗した場合は、次のポストチャ検証試行までの残り秒数になります。
- **Posture Token** : Access Control Server で設定可能な情報文字列。ACS は、システムの監視やレポート作成、デバッグ、ロギングを支援するための情報提供を目的として、ポストチャ トークンをセキュリティ アプライアンスにダウンロードします。一般的なポストチャ トークンには、Healthy、Checkup、Quarantine、Infected、Unknown があります。
- **Redirect URL** : ポスト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 ポリシーをセキュリティ アプライアンス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部分です。セキュリティ アプライアンスは、リモート ホストの HTTP (ポート 80) および HTTPS (ポート 443) 要求がある場合に、**Redirect URL** にリダイレクトします。アクセス ポリシーに **Redirect URL** が含まれない場合、セキュリティ アプライアンスはリモート ホストから HTTP 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トチャが検証されるまで有効です。そのため、ACS は新しいアクセス ポリシーをダウンロードしますが、新しいアクセス ポリシーには、別のリダイレクト URL が含まれている場合もまったく含まれていない場合もあります。

このウィンドウのボタンは、次のとおりです。



(注)

ポストチャ検証の対象のセッションをすべて再検証または初期化する場合は、**Monitoring > VPN > VPN Statistics > NAC Session Summary** を選択します。

- **Revalidate Session** : ピアのポストチャまたは割り当てられているアクセス ポリシー (ある場合には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、新しい無条件のポストチャ検証を開始します。このボタンをクリックするまで有効なポストチャ検証と割り当てられているアクセス ポリシーは、新しいポスト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。セッションがポストチャ検証から免除されている場合、このボタンをクリックしてもセッションに影響はありません。
- **Initialize Session** : ピアのポストチャ、または割り当てられているアクセス ポリシー (ある場合には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、EAPoUDP アソシエーションがパーズされ、新しい無条件のポストチャ検証が開始されます。再検証の間は NAC のデフォルトの ACL が有効になるため、セッションの初期化によってユーザ トラフィックが中断されることがあります。セッションがポストチャ検証から免除されている場合、このボタンをクリックしてもセッションに影響はありません。
- **Revalidate Tunnel Group** : 選択したセッション、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) の専用のトンネル グループにあるピアのポストチャ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、新しい無条件のポストチャ検証を開始します。このボタンをクリックするまでトンネル グループの各セッションで有効なポストチャ検証と割り当てられているアクセス ポリシーは、新しいポスト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。ポスト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 Tunnel Group** : 選択したセッション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) の専用のトンネル グループにあるピアのポストチャが変更され、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、選択したセッションの専用のトンネルグループにあるポスチャ検証で使用される EAPoUDP アソシエーションと、アクセス ポリシー (ある場合にはダウンロードされた ACL) がパージされ、有効なピアの新しい無条件のポスチャ検証が開始されます。再検証の間は NAC のデフォルトの ACL が有効になるため、セッションの初期化によってユーザ トラフィックが中断されることがあります。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。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	—	•	—	—

Encryption Statistics

Monitoring > VPN > VPN Statistics > Encryption Statistics

このパネルには、セキュリティ アプライアンスで、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 : セキュリティ アプライアンス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。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	—	•	—	—

NAC Session Summary

Monitoring > VPN > VPN Statistics > NAC Session Summary

NAC Session Summary ウィンドウでは、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** : セキュリティ アプライアンスで設定された 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、これらの要求に応答しません。セキュリティ アプライアンスの設定でクライアントレス ホストがサポートされている場合、Access Control Server は、それらのピアのセキュリティ アプライアンスに、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 ポリシーをダウンロードします。サポートされていない場合、セキュリティ アプライアンスは NAC のデフォルトの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、セキュリティ アプライアンスが EAPoUDP 通信を失ったピアの数。NAC Hold Timer アトリビュート (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、セキュリティ アプライアンス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なポスチャ検証と、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、セキュリティ アプライアンス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 ポリシーをページし、新しい無条件のポスチャ検証を開始します。再検証の間は NAC のデフォルトの ACL が有効になるため、セッションの初期化によってユーザ トラフィックが中断されることがあります。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。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	—	•	—	—

Protocol Statistics

Monitoring > VPN > VPN Statistics > Protocol Statistics

このパネルには、セキュリティ アプライアンス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 Sessions : 現在アクティブなセッションの数を示します。
- Cumulative Sessions : セキュリティ アプライアンスが最後にブートまたはリセットされて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。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Global IKE/IPSec Statistics

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

このパネルには、セキュリティ アプライアンス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。
- Global IKE/IPSec 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。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	—	•	—	—

Crypto Statistics**Monitoring > VPN > VPN Statistics > Crypto Statistics**

このパネルには、セキュリティ アプライアンス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。
- Crypto 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。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	—	•	—	—

Compression Statistics**Monitoring > VPN > VPN Statistics > Compression Statistics**

このパネルには、セキュリティ アプライアンス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 : IPSec VPN、WebVPN または SSL VPN Client などのすべての VPN タイプ、または 1 つの VPN タイプ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。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	—	•	—	—

Cluster Loads**Monitoring > VPN > VPN Statistics > Cluster Loads**

このパネルを使用して、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 (最下位) ~ 10 (最上位) の整数にする必要があります。プライオリティは、VPN ロードバランシング クラスタ内のどのデバイスがクラスタのマスター デバイスまたはプライマリ デバイスになるのかを決定するための 1 つの方法として、マスター選定プロセスで使われます。
 - Model : このサーバのセキュリティ アプライアンスのモデル名と番号を示します。
 - 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。
 - Session : 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。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	—	•	—	—

WebVPN SSO Statistics

Monitoring > VPN > WebVPN > SSO Statistics

このパネルには、セキュリティ アプライアンス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 サーバの SSO に関するものだけです。

フィールド

- Show Statistics For : 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
 - Web エージェントの URL
 - 保留中の要求の数
 - 認可要求の数
 - 再送信の数
 - 許可の数
 - 拒否の数
 - タイムアウトの数
 - 認識されなかった応答の数
- Refresh : SSO Statistics テーブルに表示される統計情報を更新します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	システム
			コンテキスト	
•	—	•	—	—

