CHAPTER 47

プロパティのモニタリング

この章は、次の内容で構成されています。

AAA サーバ

このペインでは、AAA サーバの統計情報を表示およびリフレッシュできます。

フィールド

- [Server Group]：設定されているサーバ グループ、または何も設定されていない場合は [LOCAL] を表示します。
- [Protocol]：AAA でサーバ グループが使用するプロトコルを表示します。
- [IP address]：設定されている AAA サーバの IP アドレスを表示します。
- [Status]：設定されている AAA サーバのステータス（[Active] または [Inactive]）を表示します。

AAA サーバのリストの下は、設定されている各サーバの統計情報です。統計情報をクリアするには、[Clear Server Statistics] をクリックします。サーバ ステータスをリフレッシュするには、[Update Server Status] をクリックします。

モード

次の表は、この機能を使用できるモードを示したものです。

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
•	•	•	•	—

Device Access

このペインでは、管理セッション、AAA にロックアウトされたユーザ、および認証されたユーザをモニタできます。この項では、次のトピックについて取り上げます。

- AAA Local Locked Out Users
- Authenticated Users
- ASDM/HTTPS セッション
- Secure Shell Sessions
- Telnet Sessions

AAA Local Locked Out Users

[AAA Local Locked Out Users] ペインでは、ログイン試行が失敗したために、ASDM からロックアウトされたユーザのリストを表示できます。また、選択したロックアウト条件またはすべてのロックアウトをクリアすることもできます。

フィールド

- [Currently locked out users]：現在ロックアウトされているユーザのリストを表示します。
- [Lock Time]：ユーザがシステムからロック アウトされてからの経過時間を指定します。
- [Failed Attempts]：失敗したログイン試行回数を指定します。
- [User]：ログイン試行に失敗したユーザ名。
- [Clear lockout]：選択したユーザのロックアウト条件をクリアする場合にクリックします。
- [Clear all lockouts]：すべてのユーザのロックアウト条件をクリアする場合にクリックします。すべてのロックアウトをクリアする前に、ロックアウト条件のリストを更新することをお勧めします。

モード

次の表は、この機能を使用できるモードを示したものです。

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
•	•	•	•	—

Authenticated Users

このペインでは、セキュリティ アプライアンスの使用を認証されているユーザを表示できます。各行が 1 ユーザを表します。

フィールド

- [User]：セキュリティ アプライアンスの使用を認証されているユーザのユーザ名を表示します。
- [IP Address]：セキュリティ アプライアンスの使用を認証されているユーザの IP アドレスを表示します。
- [Dynamic ACL]：セキュリティ アプライアンスの使用を認証されているユーザのダイナミック アクセス リストを表示します。
- [Inactivity Timeout]：セッションがタイムアウトになってユーザが切断されるまでに、選択したユーザが非アクティブのままでいなければならない時間を表示します。
- [Absolute Timeout]：セッションが閉じ、ユーザが切断されるまでに、選択したユーザが接続したままでいられる時間を表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

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
•	•	•	•	—

ASDM/HTTPS セッション

[ASDM/HTTPS] ペインでは、現在接続中の ASDM/HTTPS セッションを表示できます。

フィールド

- [Session ID]：接続中の ASDM/HTTPS セッションの名前を表示します。
- [IP Address]：このセキュリティ アプライアンスへの接続が許可されている各ホストまたはネットワークの IP アドレスを表示します。
- [Disconnect]：接続中の ASDM/HTTPS セッションを切断する場合に選択します。

モード

次の表は、この機能を使用できるモードを示したものです。

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
•	•	•	•	—

Secure Shell Sessions

[Secure Shell Sessions] ペインでは、SSH プロトコルを使用して管理アクセスのために、セキュリティ アプライアンスに接続されているホストを表示できます。

フィールド

- [Client]：選択した SSH セッションのクライアント タイプを表示します。
- [User]：選択した SSH セッションのユーザ名を表示します。
- [State]：選択した SSH セッションのステートを表示します。
- [Version]：セキュリティ アプライアンスへの接続に使用されている SSH のバージョンを表示します。
- [Encryption (in)]：選択したセッションで使用されているインバウンド暗号化方法を表示します。
- [Encryption (out)]：選択したセッションで使用されているアウトバウンド暗号化方法を表示します。
- [HMAC (in)]：選択したインバウンド SSH セッションに設定されている HMAC を表示します。
- [HMAC (out)]：選択したアウトバウンド SSH セッションに設定されている HMAC を表示します。
- [SID]：選択したセッションのセキュア ID を表示します。
- [Disconnect]：接続中の SSH セッションを切断する場合にクリックします。

モード

次の表は、この機能を使用できるモードを示したものです。

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
•	•	•	•	—

Telnet Sessions

[Telnet Sessions] ペインでは、現在接続中の Telnet セッションを表示できます。

フィールド

- [Session ID]：接続中の Telnet セッションの名前を表示します。
- [IP Address]：Telnet を通したセキュリティ アプライアンスへの接続が許可されている各ホストの IP アドレスを表示します。
- [Disconnect]：接続中の Telnet セッションを切断する場合にクリックします。

モード

次の表は、この機能を使用できるモードを示したものです。

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
•	•	•	•	—

Connection Graphs

[Connection Graphs] ペインでは、セキュリティ アプライアンスの接続情報をグラフ形式で表示できます。NAT に関する情報と、UDP 接続、AAA パフォーマンスおよび検査情報などのパフォーマンス モニタリング情報を表示できます。この項では、次のトピックについて取り上げます。

- Perfmon
- Xlates

Perfmon

[Perfmon] ペインでは、パフォーマンス情報をグラフ形式で表示できます。1 つのグラフ ウィンドウに表示する統計情報のタイプは 4 つまで選択できます。複数のグラフ ウィンドウを同時に開くことができます。

フィールド

- [Available Graphs]：グラフ化できるコンポーネントを一覧表示します。
  - [AAA Perfmon]：セキュリティ アプライアンスの AAA パフォーマンス情報を表示します。
  - [Inspection Perfmon]：セキュリティ アプライアンスの検査パフォーマンス情報を表示します。
  - [Web Perfmon]：URL アクセスおよび URL サーバ要求などのセキュリティ アプライアンスの Web パフォーマンス情報を表示します。
  - [Connections Perfmon]：セキュリティ アプライアンスの接続パフォーマンス情報を表示します。
  - [Xlate Perfmon]：セキュリティ アプライアンスの NAT パフォーマンス情報を表示します。
- [Graph Window Title]：グラフ タイプを追加するグラフ ウィンドウ名を表示します。既存のウィンドウ タイトルを使用するには、ドロップダウン リストからいずれかを選択します。新しいウィンドウにグラフを表示するには、新しいウィンドウ タイトルを入力します。
- [Add]：[Available Graphs] リストで選択したエントリを [Selected Graphs] リストに移動するには、このフィールドをクリックします。
- [Remove]：選択した統計タイプを [Selected Graphs] フィールドから削除する場合にクリックします。
- [Show Graphs]：新しいグラフ ウィンドウ、または更新したグラフ ウィンドウを表示するには、このフィールドをクリックします。

モード

次の表は、この機能を使用できるモードを示したものです。

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
•	•	•	•	—

Xlates

このペインでは、アクティブなネットワーク アドレス変換をグラフ形式で表示できます。1 つのグラフ ウィンドウに表示する統計情報のタイプは 4 つまで選択できます。複数のグラフ ウィンドウを同時に開くことができます。

フィールド

- [Available Graphs]：グラフ化できるコンポーネントを一覧表示します。
  - [Xlate Utilization]：セキュリティ アプライアンスの NAT の使用状況を表示します。
- [Graph Window Title]：グラフ タイプを追加するグラフ ウィンドウ名を表示します。既存のウィンドウ タイトルを使用するには、ドロップダウン リストからいずれかを選択します。新しいウィンドウにグラフを表示するには、新しいウィンドウ タイトルを入力します。
- [Add]：[Available Graphs] リストで選択したエントリを [Selected Graphs] リストに移動するには、このフィールドをクリックします。
- [Remove]：[Selected Graphs] リストから選択したエントリを削除するには、このフィールドをクリックします。
- [Show Graphs]：新しいグラフ ウィンドウ、または更新したグラフ ウィンドウを表示するには、このフィールドをクリックします。

モード

次の表は、この機能を使用できるモードを示したものです。

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
•	•	•	•	—

CRL

このペインでは、選択した CA 証明書の関連付けられた CRL を表示またはクリアできます。

フィールド

- [CA Certificate Name]：ドロップダウン リストから選択した証明書の名前を選択します。
- [View CRL]：選択した CRL を表示するには、このフィールドをクリックします。

- [Clear CRL]：選択した CRL をキャッシュからクリアするには、このフィールドをクリックします。
- [CRL Info]：*表示専用*。詳細な CRL 情報を表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

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
•	•	•	•	—

DNS Cache

セキュリティ アプライアンス では、特定のクライアントレス SSL VPN および certificate コマンドに送信された外部 DNS クエリーの DNS 情報のローカル キャッシュを提供します。各 DNS 変換要求は、ローカル キャッシュで最初に検索されます。ローカル キャッシュに情報がある場合、結果の IP アドレスが戻されます。ローカル キャッシュで要求を解決できない場合、設定されているさまざまな DNS サーバに DNS クエリーが送信されます。外部 DNS サーバによって要求が解決された場合、結果の IP アドレスと、対応するホスト名が一緒にローカル キャッシュに格納されます。

特記事項

- DNS キャッシュ エントリには、タイムスタンプが付いています。タイムスタンプは、未使用のエントリをエージング アウトするために使われます。エントリがキャッシュに追加されると、タイムスタンプが初期化されます。エントリにアクセスするたびに、タイムスタンプは更新されます。DNS キャッシュは、設定されている時間間隔ですべてのエントリをチェックし、設定されているエージング アウト タイマーを過ぎたエントリをパージします。
- 新しいエントリが到着して、サイズを超えているかメモリ不足のためにキャッシュに空き領域がない場合、エントリの経過時間に基づいてキャッシュを 3 分の 1 に減らします。一番古いエントリが削除されます。

フィールド

- [Host]：ホストの DNS 名を表示します。
- [IP Address]：ホスト名に解決するアドレスを示します。
- [Permanent]：エントリが **name** コマンドで作成されたかどうかを示します。
- [Idle Time]：セキュリティ アプライアンスが最後にそのエントリを参照してからの経過時間を指定します。
- [Active]：エントリがエージング アウトしたかどうかを示します。キャッシュに適切なスペースがないときに、このエントリは削除されることがあります。
- [Clear Cache]：DNS キャッシュ全体をクリアします。

モード

次の表は、この機能を使用できるモードを示したものです。

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
•	•	•	•	—

IP Audit

[IP Audit] ペインでは、情報シグニチャおよび攻撃シグニチャに一致するパケットの数をグラフ形式、または表形式で表示できます。各グラフ タイプには、この機能がイネーブルになっているすべてのインターフェイスの合計パケット数が表示されます。

フィールド

- [Available Graphs]：モニタリングに使用可能なシグニチャのタイプを一覧表示します。各シグニチャ タイプの詳細については、「IP Audit Signatures」を参照してください。1 つのグラフ ウィンドウに表示する統計情報のタイプは 4 つまで選択できます。複数のグラフ ウィンドウを同時に開くことができます。
  - [IP Options]：次のシグニチャのパケット数を表示します。
    Bad Options List (1000)
    Timestamp (1002)
    Provide s, c, h, tcc (1003)
    SATNET ID (1005)
  - [IP Route Options]：次のシグニチャのパケット数を表示します。
    Loose Source Route (1004)
    Record Packet Route (1001)
    Strict Source Route (1006)
  - [IP Attacks]：次のシグニチャのパケット数を表示します。
    IP Fragment Attack (1100)
    Impossible IP Packet (1102)
    IP Teardrop (1103)
  - [ICMP Requests]：次のシグニチャのパケット数を表示します。
    Echo Request (2004)
    Time Request (2007)
    Info Request (2009)
    Address Mask Request (2011)
  - [ICMP Responses]：次のシグニチャのパケット数を表示します。
    Echo Reply (2000)
    Source Quench (2002)
    Redirect (2003)

Time Exceeded (2005)

Parameter Problem (2006)

- [ICMP Replies]：次のシグニチャのパケット数を表示します。
  Unreachable (2001)

  Time Reply (2008)

  Info Reply (2010)

  Address Mask reply (2012)
- [ICMP Attacks]：次のシグニチャのパケット数を表示します。
  Fragmented ICMP (2150)

  Large ICMP (2151)

  Ping of Death (2154)
- [TCP Attacks]：次のシグニチャのパケット数を表示します。
  No Flags (3040)

  SYN & FIN Flags Only (3041)

  FIN Flag Only (3042)
- [UDP Attacks]：次のシグニチャのパケット数を表示します。
  Bomb (4050)

  Snork (4051)

  Chargen (4052)
- [DNS Attacks]：次のシグニチャのパケット数を表示します。
  Host Info (6050)

  Zone Transfer (6051)

  Zone Transfer High Port (6052)

  All Records (6053)
- [FTP Attacks]：次のシグニチャのパケット数を表示します。
  Improper Address (3153)

  Improper Port (3154)
- [RPC Requests to Target Hosts]：次のシグニチャのパケット数を表示します。
  Port Registration (6100)

  Port Unregistration (6101)

  Dump (6102)
- [YP Daemon Portmap Requests]：次のシグニチャのパケット数を示します。
  ypserv Portmap Request (6150)

  ypbind Portmap Request (6151)

  yppasswdd Portmap Request (6152)

  ypupdated Portmap Request (6153)

  ypxfrd Portmap Request (6154)
- [Miscellaneous Portmap Requests]：次のシグニチャのパケット数を示します。

mountd Portmap Request (6155)

rexd Portmap Request (6175)

- [Miscellaneous RPC Calls]：次のシグニチャのパケット数を示します。
  rexd Attempt (6180)
- [RPC Attacks]：次のシグニチャのパケット数を表示します。
  statd Buffer Overflow (6190)
  Proxied RPC (6103)

- [Add]：選択したグラフ タイプを [Selected Graphs] リストに追加するには、このフィールドをクリックします。
- [Remove]：[Selected Graphs] リストから選択したグラフ タイプを削除するには、このフィールドをクリックします。
- [Show Graphs]：新しいグラフ ウィンドウ、または更新したグラフ ウィンドウを表示するには、このフィールドをクリックします。
- [Selected Graphs]：[Selected Graphs] リストに表示するグラフ タイプを一覧表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

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
•	•	•	•	—

System Resources Graphs

このペインでは、セキュリティ アプライアンスのメモリ、CPU およびブロックの使用状況を表示できます。この項では、次のトピックについて取り上げます。

- Blocks
- CPU
- Memory

Blocks

[Blocks] では、空きメモリ ブロックと使用中のメモリ ブロックを表示できます。1 つのグラフ ウィンドウに表示する統計情報のタイプは 4 つまで選択できます。複数のグラフ ウィンドウを同時に開くことができます。

フィールド

- [Available Graphs]：グラフ化できるコンポーネントを一覧表示します。
  - [Blocks Used]：セキュリティ アプライアンスで使用中のメモリ ブロックを表示します。
  - [Blocks Free]：セキュリティ アプライアンスの空きメモリ ブロックを表示します。

- [Graph Window Title] : グラフ タイプを追加するグラフ ウィンドウ名を表示します。既存のウィンドウ タイトルを使用するには、ドロップダウン リストからいずれかを選択します。新しいウィンドウにグラフを表示するには、新しいウィンドウ タイトルを入力します。
- [Add] : [Available Graphs] リストで選択したエントリを [Selected Graphs] リストに移動するには、このフィールドをクリックします。
- [Remove] : [Selected Graphs] リストから選択した統計タイプを削除するには、このフィールドをクリックします。
- [Show Graphs] : 新しいグラフ ウィンドウ、または更新したグラフ ウィンドウを表示するには、このフィールドをクリックします。

モード

次の表は、この機能を使用できるモードを示したものです。

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
•	•	•	•	—

CPU

このペインでは、CPU の使用状況を表示できます。1 つのグラフ ウィンドウに表示する統計情報のタイプは 4 つまで選択できます。複数のグラフ ウィンドウを同時に開くことができます。

フィールド

- [Available Graphs] : グラフ化できるコンポーネントを一覧表示します。
  - [CPU Utilization] : セキュリティ アプライアンスの CPU の使用状況を表示します。
- [Graph Window Title] : グラフ タイプを追加するグラフ ウィンドウ名を表示します。既存のウィンドウ タイトルを使用するには、ドロップダウン リストからいずれかを選択します。新しいウィンドウにグラフを表示するには、新しいウィンドウ タイトルを入力します。
- [Add] : [Available Graphs] リストで選択したエントリを [Selected Graphs] リストに移動するには、このフィールドをクリックします。
- [Remove] : [Selected Graphs] リストから選択したグラフ タイプを削除するには、このフィールドをクリックします。
- [Show Graphs] : 新しいグラフ ウィンドウ、または更新したグラフ ウィンドウを表示するには、このフィールドをクリックします。

モード

次の表は、この機能を使用できるモードを示したものです。

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
•	•	•	•	—

Memory

このペインでは、メモリの使用状況を表示できます。1 つのグラフ ウィンドウに表示する統計情報のタイプは 4 つまで選択できます。複数のグラフ ウィンドウを同時に開くことができます。

フィールド

- [Available Graphs] : グラフ化できるコンポーネントを一覧表示します。
  - [Free Memory] : セキュリティ アプライアンスの空きメモリを表示します。
  - [Used Memory] : セキュリティ アプライアンスの使用中のメモリを表示します。
- [Graph Window Title] : グラフ タイプを追加するグラフ ウィンドウ名を表示します。既存のウィンドウ タイトルを使用するには、ドロップダウン リストからいずれかを選択します。新しいウィンドウにグラフを表示するには、新しいウィンドウ タイトルを入力します。
- [Add] : [Available Graphs] リストで選択したエントリを [Selected Graphs] リストに移動するには、このフィールドをクリックします。
- [Remove] : [Selected Graphs] リストから選択したグラフ タイプを削除するには、このフィールドをクリックします。
- [Show Graphs] : 新しいグラフ ウィンドウ、または更新したグラフ ウィンドウを表示するには、このフィールドをクリックします。

モード

次の表は、この機能を使用できるモードを示したものです。

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
•	•	•	•	—

WCCP

Web Cache Communication Protocol（WCCP）は IPv4 トラフィック フローをリアルタイムで Web キャッシュにリダイレクトします。ASDM では、WCCP を使用するインターフェイスのパケット リダイレクションを監視できます。WCCP は、ロードバランシング、スケーリング、耐障害性、およびフェールセーフ サービスも提供します。ロードバランシングは、宛先 IP アドレスに基づくハッシュによって提供されます。ハッシュ値を使用して、トラフィック フローの出力インターフェイスが選択さ

れます。また、このプロトコルを使用すると、セキュリティ アプライアンスと WCCP クライアントでサービス グループを形成してサービスをサポートすることもできます。この項では、次のトピックについて取り上げます。

- Service Groups
- Redirection

Service Groups

このペインでは、サービス グループ、表示モード、およびハッシュ設定を表示およびリフレッシュできます。

フィールド

- [Service Group]：ドロップダウン リストから該当するサービス グループを選択します。
- [Display Mode]：ドロップダウン リストから表示モードを選択します。
- [Destination IP Address]：宛先 IP アドレスを指定します。
- [Source IP Address]：送信元 IP アドレスを指定します。
- [Destination Port]：宛先ポート番号を指定します。
- [Source Port]：送信元ポート番号を指定します。

Redirection

このペインでは、WCCP インターフェイスの統計情報を要約または詳細形式で表示およびリフレッシュできます。

フィールド

- [Show Summary]：統計情報を要約形式で表示するには、このオプションを選択します。
- [Show Details]：統計情報を詳細形式で表示するには、このオプションを選択します。