Nways Manager

Nways VPN Manager ユーザーズ・ガイド

GA88-7014-00
(英文原典：GA27-4233-00)

Nways Manager

Nways VPN Manager ユーザーズ・ガイド

GA88-7014-00
(英文原典：GA27-4233-00)

お願い

本書の情報および本書に記載されている製品 (またはプロダクト) をご使用になる際は、その前に、79ページの『付録. 特記事項』を必ずお読みください。

本書は、IBM Nways VPN Manager に適用されます。

本マニュアルについてご意見やご感想がありましたら

http://www.ibm.com/jp/manuals/main/mail.html

からお送りください。今後の参考にさせていただきます。
なお、日本 IBM 発行のマニュアルはインターネット経由でもご購入いただけます。詳しくは

http://www.infocr.co.jp/ifc/books/

をご覧ください。（URL は、変更になる場合があります）

原 典： GA27-4233-00
Nways Manager
Nways VPN Manager User's Guide

発 行： 日本アイ・ビー・エム株式会社

担 当： ナショナル・ランゲージ・サポート

第1刷 1999.8

この文書では、平成明朝体™W3、平成明朝体™W9、平成角ゴシック体™W3、平成角ゴシック体™W5、および平成角ゴシック体™W7を使用しています。この(書体*)は、(財）日本規格協会と使用契約を締結し使用しているものです。フォントとして無断複製することは禁止されています。

注* 平成明朝体™W3、平成明朝体™W9、平成角ゴシック体™W3、
平成角ゴシック体™W5、平成角ゴシック体™W7

目次

第1章 はじめに

この章では、VPN Manager について簡単に説明し、それをサポートする IBM ハードウェア・コンポーネントのリストを記載し、VPN Manager を使用するために必要なハードウェアとソフトウェアの要件を示します。

VPN Manager の概要

Nways VPN Managerは、IBM 開発のバーチャル・プライベート・ネットワークのモニター、イベント報告、障害追及、動作制御、およびアプリケーションの起動に必要な機能を提供します。

ハードウェア・サポート

Nways VPN Manager バージョン 2.0 は、次の装置に実装されている VPN 機能のモニターおよび動作制御を行います。

- IBM 2210 Nways ルーター
- IBM 2212 Nways アクセス・ユーティリティー
- IBM 2216 Nways マルチアクセス・コネクター
- IBM ネットワーク・ユーティリティー

ハードウェアおよびソフトウェアの前提条件

Nways VPN Managerは、次のいずれかのプラットフォーム用の Nways エレメント・マネージャー バージョン 2.0 が必要です。

- AIX
- HP-UX
- Windows NT

Nways エレメント・マネージャーの最小ハードウェア要件が、Nways VPN Managerの要件より上回っているので、追加のハードウェア要件はありません。

第2章 VPN の概要

バーチャル・プライベート・ネットワーク (VPN) は、イントラネットからの情報をインターネットのような公衆 IP ネットワークを介して安全に伝送する手段を、エンド・ユーザーに提供します。 VPN は、レイヤー 2 トンネル、IPSec トンネル、およびポリシーで構成することができます。レイヤー 2 トンネルは、リモート・ダイヤルイン・ユーザーに対して VPN 機能を提供します。 IPSec トンネルは、IP ユーザーに対して VPN 機能を提供します。ポリシーは、リソースへのアクセス制御を提供します。

この章では、次の項目について概説します。
- レイヤー 2 トンネル伝送
- IPSec トンネル伝送
- ポリシー

レイヤー 2 トンネル伝送

レイヤー 2 トンネル伝送プロトコルは、公衆 IP ネットワークを介して、私設ポイント・ポイント・プロトコル (PPP) トラフィックを安全に伝送することができます。 2 種類のネットワーク・モデルを採用した、3 種類のレイヤー 2 トンネル伝送プロトコルがあります。 3 種類のレイヤー 2 トンネル伝送プロトコルとは、レイヤー 2 トンネル伝送プロトコル (L2TP)、レイヤー 2 転送 (L2F) プロトコル、およびポイント・ポイント・トンネル伝送プロトコル (PPTP) です。 2 種類のネットワーク・モデルとは、強制的トンネル伝送と自発的トンネル伝送です。

用語

ネットワーク・アクセス・サーバー (NAS) は、*公衆交換電話網* (PSTN) やサービス総合ディジタル網 (ISDN) のような交換ネットワーク構造に接続されている装置で、ポイント・ポイント・プロトコル (PPP) のエンド・システムが組み込まれています。 L2TP トンネルを開始する能力を備えている NAS を、*L2TP アクセス集線装置* (LAC) と呼んでいます。 NAS は、着呼の開始側であり、発呼の受信側になります。ゲートウェイは、PPP を終了する能力を備えた装置で、通信のサーバー側を担当します。ゲートウェイは、*L2TP* ネットワーク・サーバー (LNS) とも呼ばれます。ゲートウェイは、発呼の開始側であり、着呼の受信側になります。

強制的トンネル伝送

強制的トンネル伝送は、トンネル伝送を可能にするソフトウェアを持たないダイヤルイン・クライアントが、ネットワーク・アクセス・サーバー (NAS) から企業ネットワーク

にトンネル伝送する PPP セッションを開始できます。このモデルでは、PPP セッションはクライアントとゲートウェイの間に存在し、トンネルは NAS とゲートウェイの間に存在します。

自発的トンネル伝送

一方、自発的トンネル伝送は、ダイヤルイン・クライアントはトンネル伝送が使用可能であることが必要です。このモデルでは、クライアントは、最初にサービス・プロバイダーにダイヤルしてインターネットにアクセスします。サービス・プロバイダーへの接続が確立された後、クライアントはゲートウェイへのレイヤー 2 トンネルを確立し、この新たに確立したトンネルを介して、エンド・エンドの PPP セッションを確立します。このモデルでは、PPP セッションとトンネルが、クライアントとゲートウェイの間に存在します。

レイヤー 2 トンネル伝送プロトコル

レイヤー 2 トンネル伝送は、次のプロトコルを使用します。

L2TP レイヤー 2 トンネル伝送プロトコルは、レイヤー 2 転送 (L2F) プロトコルおよびポイント・ポイント・トンネル伝送プロトコル (PPTP) から発展した、インターネット技術特別調査委員会 (IETF) 標準トラック・プロトコルです。 L2TP は、事前割り当て UDP ポート 1701 を初期トンネル制御メッセージ・ハンドシェークに使用し、接続の両側の利用可能な UDP ソース・ポートを選択できます。 UDP は、トンネル伝送の PPP パケットのパケット転送にも使われます。L2TP は、強制的トンネル伝送と自発的トンネル伝送の両方のネットワーク・モデルを利用します。

L2F レイヤー 2 転送プロトコルは、本来は Cisco Systems によって開発された、非標準ベースのレイヤー 2 トンネル伝送プロトコルです。これは、事前割り当て UDP ポート 1701 (固定) を、トンネル伝送や発呼制御メッセージの伝送だけでなく、NAS からゲートウェイへのトンネル伝送の PPP パケットの転送にも使用します。 L2F は、強制的トンネル伝送モデルを採用しています。

PPTP ポイント・ポイント・トンネル伝送プロトコルは、本来は Microsoft 社がその Windows 95 および Windows NT プラットフォームに組み込んだ、もう 1 つの非標準ベースのレイヤー 2 トンネル伝送プロトコルです。 PPTP は、TCP を使用してトンネルおよびセッションの両方の制御構造をオープンします。セッションが確立された後、PPP パケットは汎用ルーティング・カプセル化 (GRE) を使ってトンネル伝送されます。 PPTP は、自発的トンネル伝送ネットワーク・モデルを採用しています。

レイヤー 2 トンネル伝送機能

レイヤー 2 トンネル伝送プロトコルは、直接的または間接的に、認証、暗号化、および圧縮を提供できます。

レイヤー 2 トンネル伝送プロトコルは、トンネル認証を直接提供でき、ユーザー認証を間接的に提供できます。トンネル認証は、NAS とゲートウェイ間で実行されます。ユーザー認証は、ベースのポイント・ポイント・プロトコルによって実行されます。

レイヤー 2 トンネル伝送プロトコルは、データ暗号化を間接的に提供できます。どのレイヤー 2 トンネル伝送プロトコルも、アプリケーション層で暗号化されたデータを転送できます。 L2TP は、データ暗号化を実行できる IPSec と一緒に使用できます。 PPTP は、Microsoft ポイント・ポイント暗号化 (MPPE) 機能を使用できます。

レイヤー 2 トンネル伝送プロトコルは、データ圧縮を間接的に提供できます。レイヤー 2 トンネル伝送プロトコルは、データ圧縮機能を備えた、ベースのポイント・ポイント・プロトコルを使ってこれを達成します。

IPSec トンネル伝送

IPSec は、公衆 IP ネットワークを介して IP トラフィックを安全に伝送するトンネル・メカニズムを定義した、インターネット技術特別調査委員会 (IETF) 標準です。 IPSec トンネルには、1 対のトンネルが使用されています。つまり、IPSec キー管理トンネルと IPSec データ管理トンネルです。 IPSec キー管理トンネルは、フェーズ 1 トンネルまたはインターネット・キー交換 (IKE) トンネルとも呼ばれ、1 つまたは複数の後続の IPSec フェーズ 2 ユーザー・データ・トンネルの制御トンネルです。 IPSec トンネルは、エンド・エンド間またはゲートウェイ・ゲートウェイ間のどちらかのネットワーク・モデルに組み込まれるのが一般的です。

用語

認証 とは、受信したデータが送信されたデータと同一であること、および提示された送信側が実際の送信側であることを確認する特性をいいます。 IPSec 認証の方式には、事前共用キーを手作業で入力する方法と、ディジタル署名を使用する方法があります。ディジタル署名を使用すると、認証に加えて、メッセージが送信側に固有に関連付けられることや、受信側が忘れることがないことも保証されます。 IPSec トンネル認証方式では、通常、メッセージ・ダイジェスト 5 (MD5: 128 ビット・ハッシュ) およびセキュア・ハッシュ・アルゴリズム (SHA: 160 ビット・ハッシュ) が使われます。

整合性 とは、データが、知らないうちに変更されることなく、ソースからあて先に伝送されることを保証する特性です。 IPSec 整合性方式では、通常、ハッシュ・メッセージ認証コード・メッセージ・ダイジェスト 5 (HMAC-MD5: 2x128 ビット・ハッシュ) およびハッシュ・メッセージ認証コード・メッセージ・セキュア・ハッシュ・アルゴリズム (HMAC-SHA: 2x160 ビット・ハッシュ) が使われます。

機密性 とは、対象の受信側は送信内容を理解できるが、それ以外の者は送信内容を判別できない通信の特性をいいます。機密性を提供するために、IPSec ではカプセル化と暗号化が使われます。元の IP データ・パケットは、カプセル化されて IPSec データ・パケット

に入れられます。トンネル・モード (通常、ゲートウェイで使用) では、元の IP ヘッダーとペイロードがカプセル化されます。トランスポート・モード (通常、ホストで使用) では、元のペイロードだけがカプセル化されます。 IPSec 暗号化方式では、通常、データ暗号化規格 (DES - 56 ビット暗号化)、トリプル・データ暗号化規格 (DES-3 - 3x56 ビット暗号化)、および商業データ・マスキング機能 (CMDF - 40 ビット暗号化) が使われます。

セキュリティー・アソシエーション (SA) とは、1 組の共用セキュリティー情報を設定する、特定の 1 組のネットワーク接続の間の関係をいいます。セキュリティー・アソシエーションは、秘密キー、暗号アルゴリズム、認証アルゴリズム、およびカプセル化モードに基づいて折衝します。 IKE は、Diffie-Hellman キー協定プロトコル (グループ 1: 768 ビット・キーイング、グループ 2: 1024 ビット・キーイング) を使用して、2 つの IPSec エンティティー間の共有秘密 (つまり、キー) を生成します。IKE は、以前は ISAKMP/Oakley (Internet Security Association and Key Management protocol slash Oakley Protocol) と呼ばれていたものです。SA の期間は、存続時間 (秒数で表した期間) または存続サイズ (KB で表した期間) で指定します。

エンド・エンド間のトンネル伝送

エンド・エンド間 IPSec トンネル伝送では、ネットワークの片側の IP ホストが、ネットワークの反対側の IP ホストと安全に通信できます。このモデルは、特定の対等間 (Peer-To-Peer) モデルに似ており、IP ホストは両方とも IPSec が使用可能であることが必要です。 IPSec トンネルは、2 つの IP ホストの間に、1 つのキー管理トンネルと 1 つのデータ管理トンネルとで構成されています。

ゲートウェイ・ゲートウェイ間のトンネル伝送

ゲートウェイ・ゲートウェイ間 IPSec トンネル伝送では、ネットワークの片側の 1 つまたは複数の IP ホストが、ネットワークの反対側の 1 つまたは複数の IP ホストと安全に通信できます。このモデルは任意間 (Any-To-Any) モデルに似ており、ゲートウェイは IPSec が使用可能でなければなりませんが、IP ホストはどれも IPSec が使用可能である必要はありません。 IPSec トンネルは、2 つのゲートウェイの間に、1 つのキー管理トンネルと 1 つまたは複数のデータ管理トンネルによって構築されます。ゲートウェイは、公衆インターフェースを介して接続し、公衆インターフェースやその背後の私設インターフェースを保護します。私設インターフェースには、IP サブネット、一定範囲の IP アドレス、または単一の IP アドレスが含まれます。

キー管理

IPSec キー管理トンネルは、インターネット・キー交換 (IKE) トンネルまたは IPSec フェーズ 1 トンネルとも呼ばれ、1 つまたは複数の後続の IPSec フェーズ 2 ユーザー・データ・トンネルの制御トンネルです。 IPSec キー管理トンネルは、メイン・モード (6 メッセージ交換を使用) またはアグレッシブ・モード (3 メッセージ交換を使用) のどち

らかで折衝されます。折衝では、エンティティーの認証、共有秘密 (Shared Secret) の設定、およびセキュリティー・アソシエーションのパラメーターの設定が行われます。折衝が正常に完了すると、IPSec キー管理トンネルは、単一の両方向セキュリティー・アソシエーション (SA) を使用して通信します。特定の IPSec キー管理トンネルの存続時間の途中で SA が満了し、新しい SA が作成されることもあります。

データ管理

IPSec データ管理トンネルは、IPSec フェーズ 2 ユーザー・データ・トンネルまたは IPSec トンネルとも呼ばれ、IP トラフィックを安全に伝送するのに使われます。 IPSec データ管理トンネルは、クィック・モード (3 メッセージ交換を使用) で折衝されます。折衝では、アイデンティティーの交換、再生防止 (Replay Prevention) を実施するか否かの決定、完全転送秘密 (Perfect Forward Secrecy) が必要な場合のキーの生成、断片ビット複写禁止 (Don’t Copy Fragment Bit) の以後の取り扱いに関する合意、およびセキュリティー・アソシエーションのパラメーターの設定が行われます。セキュリティー・パラメーターは、認証ヘッダー (AH) 処理属性、またはカプセル化セキュリティー・ペイロード (ESP) 処理属性、あるいは、その両方から構成されます。 AH と ESP は、どちらもパケット整合性とデータ原点認証を行いますが、暗号化を行うのは ESP だけです。 IPSec データ管理トンネルは、1 つまたは複数のインバウンド SA と、1 つまたは複数のアウトバウンド SA を使用します。特定の IPSec データ管理トンネルの存続時間の途中で SA の期限が切れて、新しい SA が作成されることもあります。この切り替え期間中は、元の各インバウンド SA に対して、実際には 2 つの SA (CURRENT 状況のものが 1 つと、EXPIRING 状況のものが 1 つ) が存在することになります。

IPSec トンネル伝送機能

IPSec トンネル伝送は、認証、暗号化、および整合性を直接提供できます。

認証はトンネル・ベースで実施され、任意選択で、パケット・ベースで行うこともできます。トンネル認証は、事前共用キーまたはディジタル署名を使って、IKE 相手側によって実施されます。

パケット認証は、HMAC-MD5 または HMAC-SHA アルゴリズムを使って、AH または ESP 処理で行います。暗号化は、任意選択で、パケット・ベースで ESP 処理により行われます。パケット暗号化には、DES、DES-3、または CMDF アルゴリズムが使われます。

整合性は、任意選択で、パケット・ベースで行われます。整合性は、AH または ESP 処理のどちらかで行うことができ、HMAC-MD5 または HMAC-SHA アルゴリズムを使用します。

ポリシー

ポリシーは、プロファイルとアクションから構成されます。プロファイルは、接続のソースとあて先の 1 組の属性を定義します。アクションは、実際上は、IPSec キー管理、IPSec データ管理、差別化サービス、および RSVP に使用される、アクションまたはサブポリシーの集合です。接続を確立するときに、定義されたポリシー・プロファイルが一致するか検索されます。プロファイルの一致が検出されると、アクション提案が交換されます。提案フェーズが正常に完了すると、接続が確立され、定義されたポリシーの現行インスタンスが作成されます。単一の定義ポリシーから複数のポリシー・インスタンスが作成されることもあります。

ポリシー・コンポーネントの関係

VPN ポリシーには、有効期間、トラフィック・プロファイル、および少なくとも 1 つのポリシー・アクションが含まれているポリシー条件を指定する必要があります。「有効期間」コンポーネントの定義は、装置特定の情報を含んでいないので、複数のポリシーに適用できます。「トラフィック・プロファイル」コンポーネントの定義は、装置特定の IP アドレス情報が含まれているので、そのポリシーに固有です。 IPSec アクションの「キー管理アクション」および「キー管理提案」コンポーネントの定義は、どちらも装置特定の情報を含んでいないので、複数のポリシーに適用できます。 IPSec アクションの「データ管理アクション」コンポーネントの定義は、装置特定の IP アドレス情報が含まれているので、そのポリシーに固有です。 IPSec アクションの「データ管理アクション」、「データ管理提案」、「認証ヘッダー (AH) 変換」、および「カプセル化セキュリティー・ペイロード (ESP) 変換」コンポーネントの定義は、いずれも装置特定の情報を含んでいないので、複数のポリシーに適用できます。「差別化サービス・アクション」および「RSVP アクション」コンポーネントの定義は、どちらも装置特定の情報を含んでいないので、複数のポリシーに適用できます。次の表は、VPN ポリシーのコンポーネントの関係を示しています。

ポリシー・コンポーネント	関係
ポリシー条件	ポリシーは、有効期間とトラフィック・プロファイルを含んでいなければならない
有効期間	複数のポリシーで共用できる
トラフィック・プロファイル	「全トラフィック・プロファイル」以外は、ポリシーに固有
ポリシー・アクション	ポリシーは、少なくとも 1 つのアクションを含んでいなければならない
IPSec アクション	キー管理とデータ管理アクションが含まれていなければならない
キー管理 (KM) アクション	複数のポリシーで共用できる
キー管理 (KM) 提案	複数のキー管理アクションで共用できる
データ管理 (DM) アクション	ポリシーに固有 (IP アドレス情報を含む)
データ管理 (DM) 提案	複数のデータ管理アクションで共用できる
AH 変換	複数のデータ管理提案で共用できる
ESP 変換	複数のデータ管理提案で共用できる
差別化サービス・アクション	複数のポリシーで共用できる
RSVP アクション	複数のポリシーで共用できる

LDAP

Light Weight Directory Access Protocol (LDAP) は、X.500 ディレクトリー・アクセス・プロトコル (DAP) から発展したインターネット・ディレクトリー規格で、クライアント装置が、イントラネット / インターネット上のディレクトリー・サーバーに、オープンにアクセスできる機能を提供します。このプロトコルは、クライアントとサーバー間で TCP/IP を介して、スキーマに基づくテキスト形式の交換を行うことによって、この機能を提供します。クライアントとサーバーは、1 つまたは複数のスキーマをサポートし、各スキーマを使って、関連のオブジェクトの集合を定義します。

Directory-Enabled Networking Initiative (DEN) は、その仕様の中で、LDAP を情報にアクセスするのに使用するメカニズムとして識別しています。 DEN は 1997 年に創設され、現在は IBM、Microsoft、Cisco Systems、Netscape など、さまざまなベンダーによってサポートされています。設立の目的は、ユーザー、ネットワーク装置、およびアプリケーションに関する情報を保管する統合ディレクトリーの情報モデル仕様を提供することです。ネットワーク業界は現在、DEN を、複数ベンダーの製品が LDAP サーバーを使ってトポロジーや構成に関するデータの保管や検索ができるインテリジェント・ネットワーク構築のかぎを握る存在とみています。

VPN の観点から見ると、ポリシー構成アプリケーションと VPN 装置は、LDAP サーバーと通信する LDAP クライアントになります。ポリシー構成アプリケーションは、LDAP サーバーと対話して、VPN ポリシーの作成、更新、削除を行います。 VPN 装置は、LDAP サーバーと対話して、その VPN ポリシーを検索します。 LDAP クライアントと

LDAP サーバー間の交換は、ポリシー・スキーマ (VPN ポリシーを表現するオブジェクトやデータを定義したもの) に基づいて行われます。

装置の相互関係

すべての VPN 装置の VPN ポリシーは、ポリシー構成アプリケーションを使って定義します。 VPN ポリシーは LDAP サーバーに保管され、後に初期設定時や、ポリシー構成アプリケーションから要求されたとき、または VPN モニター・アプリケーションから要求されたときに、VPN 装置にダウンロードされます。

第3章 VPN リスト・マネージャーの使用

この章は、次の項から成っています。

- VPN リストの概要
- VPN リスト・マネージャー情報パネルの概要
- VPN 装置リストの概要

VPN リストの概要

Nways VPN リストでは、VPN リスト・マネージャーと呼ばれる Nways サービスによって維持されている装置のリストを表示できます。このサービスは、このアプリケーションのユーザーや NetView および OpenView のデータベースから装置を受け取ります。NetView や OpenView から装置をリストに追加するためは、その装置が、IBM が開発したとおりに、バーチャル・プライベート・ネットワークをサポートすることを検証するフィルター・テストに合格しなければなりません。このアプリケーションを使えば、VPN リスト・マネージャーのすべてのクライアントがアクセスするユーザーの装置リストに装置を追加することによって、装置をリストに追加できます。これは、NetView や OpenView が知らない装置、あるいは VPN リスト・マネージャーのこのリリースに組み込まれたとおりに、フィルター・テストに合格しない装置にとって便利です。

このアプリケーションを使って、ユーザーは VPN リスト・マネージャーを制御できます。 VPN リスト・マネージャーのリストをリセットしたり、あるいは、ユーザーが手作業で追加したリストにアクセスしたり、NetView や OpenView のデータベースで変更されている新しい装置がないかを検査して、装置をリストに追加することができます。装置がフィルター・テストに合格できるかどうかは、最初のフィルター・テストでは合格していても、以降のソフトウェアの更新によって変わる可能性があります。

このアプリケーションは、装置のリストを表形式で表示し、スクロール、検索、分類を行えます。リストの中の装置をクリックすると、その装置の詳細が表示され、VPN モニター・アプリケーションを起動して、この装置に関する特定の VPN 情報を見ることができます。

VPN リスト・マネージャー情報パネルの概要

このパネルには、次のセクションがあります。

- Information (情報)
- Log File Settings (ログ・ファイルの設定)
- Reset VPN Manager List (VPN Manager リストのリセット)
- Password (パスワード)

- Change Password (パスワードの変更)

あるセクションをパネルの表示可能域に置くには、パネルの左側の選択リストの該当するセクションの名前を 1 回だけクリックします。

Control Action Priorities (制御アクションの優先順位)

VPN リスト・マネージャーは、このパネルから一度に 1 つのアクションしか実行しません。このパネルで複数の変更を要求すると、VPN リスト・マネージャーは次の体系を使用して、実行するアクションを決めます。

1. パスワードの変更
2. ログ状況の変更
3. リストのリセット

Information

このセクションには、次のフィールドがあります。

VPN List Manager Host Name:
VPN リスト・マネージャーが実行されているシステムのホスト名。

VPN List Manager IP Address:
VPN リスト・マネージャーが実行されているシステムの IP アドレス。

VPN List Manager Version:
実行されている VPN リスト・マネージャーのバージョン。

VPN List Started on:
VPN リスト・マネージャーが開始された時刻と日付。

Current Time on VPN List Manager:
VPN リスト・マネージャーが実行されているシステムの現在の時刻と日付。

Number of Devices:
VPN リスト・マネージャーが維持しているリスト内の現在の装置の数。

この数を、このクライアントで使用されている装置の数と比較します。両方の数が同じでない場合は、「VPN Device List」パネル上の「**Refresh**」ボタンを使用して、VPN リスト・マネージャーからクライアント・リストを最新表示します。

Number of Clients:
リストが変更されたときに更新通知を受け取るために VPN リスト・マネージャーに登録されたクライアントの数。変更は、他のクライアントから行われたり、VPN リスト・マネージャーが OpenView や Netview から新しい装置が検出または追加されたことを通知された結果として行われることがあります。

This Client Notify Status:

このクライアントは、リストが変更されたときに VPN リスト・マネージャーから更新を受け取るかどうかを示します。

クライアントの更新通知の登録は、VPN Manager アプリケーションの初期設定時に行われます。状況は *enabled* でなければなりません。状況が *enabled* でないときは、VPN List マネージャーへの接続に問題があることを示しています。再度「VPN Device List (VPN 装置リスト)」パネルを表示し、「VPN List Manager Control (VPN リスト・マネージャー制御)」パネルに戻って、状況が変更されたかどうかを見てください。

Log File Settings

このセクションには、次のフィールドがあります。

Current Logging Status:

VPN リスト・マネージャーがその活動をファイルに記録しているかどうかを示します。この状況を変更するには、ユーザーは現行パスワードを入力し、「**Apply**」をクリックして、変更をアクティブにします。

ログ・ファイルが作成されている場合、その名前は vpnlist.log で、他の Nways Manager のログ・ファイルと同じ場所にあります。

Reset List

このセクションには、次のフィールドがあります。

Current System Device Status:

VPN リスト・マネージャーが維持している装置の NetView または OpenView (システム) データベースにリスト・マネージャーがアクセスできたかどうかを示します。

可能な値は、次のとおりです。

Failed to Load

VPN リスト・マネージャーは、システム・データベースにアクセスできなかったので、装置リストをロードできなかったことを示します。

Unknown

VPN リスト・マネージャーは、システム・データベースの状況を知らないことを示します。これは VPN リスト・マネージャーに問題があることを示しています。

Loaded

正常な状態で、システムが VPN リスト・マネージャーの装置に対する要求に応答したことを示しています。これは、VPN リスト・マネージャーが VPN 可能な装置をそのリストに正常に追加したことを示しています。

Waiting for System to Respond

VPN リスト・マネージャーは、まだシステム・データベースから装置を追加していないことを示しています。システムはまだネットワークから装置情報を収集中で、そのタスクが完了したら、装置情報を VPN リスト・マネージャーに渡します。

Loading in progress...

現在、システムは装置に関する情報を VPN リスト・マネージャーに渡している最中であることを示します。

Current User Device Status

ユーザーが手作業で VPN リスト・マネージャーに追加した装置の状況を示します。

可能な値は、次のとおりです。

Failed to Load

VPN リスト・マネージャーは指定されたユーザー・ファイルをロードできなかったことを示します。これはユーザー・ファイルに問題があることを示しています。

Unknown

VPN リスト・マネージャーは、ユーザー・ファイルの状況を知らないことを示します。これは VPN リスト・マネージャーに問題があることを示しています。

Loaded

これは、ユーザー・ファイルが VPN リスト・マネージャーによって読み取られた後の正常な状態です。 VPN リスト・マネージャーがユーザー・ファイル内の装置を自身の装置リストに正常に追加したことを示しています。

Loading in progress...

VPN リスト・マネージャーは、現在ユーザー・ファイルを読み取り中であることを示しています。

Reset List

装置の現行リストを最新表示したり、追加できます。リストをリセットするには、現行のパスワードを入力する必要があります。「**Apply**」をクリックすると、選択されたリセット・タイプを使ってリストがリセットされます。

Password

このセクションには、次のフィールドがあります。

Current Password:

VPN リスト・マネージャーに装置リストを変更させるには、ユーザーが有効なパ

スワードを入力する必要があります。 VPN リスト・マネージャーの装置リストを変更すると、この VPN リスト・マネージャーを使用する他のクライアントに影響を与えるので注意が必要です。

デフォルト・パスワードは **OK** です。

Change Password

このセクションには、次のフィールドがあります。

Change Password
このアクションは、ユーザーに現行のパスワードの入力を求めます。新規パスワードは、確認のために 2 回入力する必要があります。新規パスワードを入力した後、「**Apply**」をクリックすると、現行パスワードが変更されます。

VPN Device List パネルの概要

「VPN Device List (VPN 装置リスト)」パネルには、次のセクションがあります。

- Devices (装置)
- Details (詳細)
- Print (印刷)

Devices

このセクションには、次のフィールドとボタンがあります。

Device Table
装置テーブルは、現在の VPN リスト・マネージャー装置リスト内の装置に関する情報を表形式で表示し、ユーザーは情報を検索したり、情報をスクロールしたり、個々の装置を選択できます。

テーブルの行の中のデータ上にポインターを置き、それをクリックして行を選択すると、パネルに表示されている他の情報が、選択した行を反映して更新されます。

テーブル内の列を選択すると、選択された列内のデータに基づいて、テーブルが昇順または降順に分類されます。

行をダブルクリックすると、「**Monitor**」ボタンをクリックし、その装置の VPN モニターのアプリケーションを立ち上げたのと同じ機能が実行されます。

テーブルには、次の列が表示されます。

Device Name
ユーザーまたはネットワーク管理プラットフォームが装置に与えた名前。

IP Address
装置の IP アドレス。

Device Type
この装置の装置タイプ。

Search Fields
検索フィールドでは、アスタリスク (*) をワイルドカード文字として使います。ワイルドカードは、フィールドの先頭、末尾、またはその両方で使用できます。ワイルドカードは、検索ストリングの内部では使えません。装置の探索は、装置名、IP アドレス、またはその両方で行えます。

Device Name
探索する名前。

IP Address
探索する IP アドレス。

Search Button
現行リスト表示の最上行の情報を使用して探索します。

Search Next Button
現行リスト表示の現在選択されている行の後の行に入力された情報を使用して探索します。

Details

このセクションには、次のフィールドとボタンがあります。

Total Number of Devices in List:
現在表示されているリスト内の装置の総数を示します。

Device Name:
現行装置のユーザー定義名。

IP Address:
現行装置の IP アドレス。

Read Community Name:
現行装置の SNMP 読み取りアクセス・コミュニティー名。装置は、読み取りと書き込みの複数のアクセス・レベルを持っていることがあります。これは読み取り専用アクセスに関連した名前です。

Write Community Name:
現行装置の SNMP 書き込みアクセス・コミュニティー名。装置は、読み取りと書き込みの複数のアクセス・レベルを持っていることがあります。これは読み取り・書き込みアクセスに関連した名前です。

Device Type:
現行装置の装置タイプ。

Add Button:
このボタンをクリックすると、入力された情報を使用して、新しい装置がリストに追加されます。

Change Button:
手作業でリストに追加した装置の属性を変更します。システムがリストに追加した装置を変更するときは、システム管理プラットフォームを使って行います。

Delete Button:
手作業でリストに追加した装置を削除します。システムが追加された装置を削除するときは、システム管理プラットフォームを使って行います。

Monitor Button:
現行装置上の VPN モニターのアプリケーションを立ち上げます。

Print

このセクションでは、リストに表示された情報を印刷できます。各印刷ページに含めるヘッダーとフッターのテキストを入力することができます。

このセクションには、次のフィールドとボタンが表示されます。

Header:
各ページの上部に印刷するヘッダー・テキストを入力します。

Footer:
各ページの下部に印刷するフッター・テキストを入力します。

Print Button
このボタンを押すと、プリンター選択リストが表示されます。正しいプリンター・タイプ用にフォーマットされた出力を生成できるプリンターを選択します。

注: システムにプリンターが定義されていない場合、印刷機能は装置リストをフォーマットできず、「VPN Device List」パネルに戻って、次のメッセージを出します。

```
Print Cancelled
```

第4章 VPN モニター

VPN モニターは、ネットワーク内の VPN 対応装置、およびこれらの装置を使用する VPN に対して、モニター、イベント報告、障害追及、動作制御、およびアプリケーション起動の機能を提供します。

この章では、VPN Manager ウィンドウに関する情報を提供します。次の項が含まれています。

- VPN モニター・ウィンドウ
- VPN モニターの機能

VPN モニター・ウィンドウ

VPN モニター・ウィンドウは、3 つの部分から構成されます。

- Navigation Tree (ナビゲーション・ツリー)
- Information Panel (情報パネル)
- Message Area (メッセージ域)

Navigation Tree パネル

ナビゲーション・ツリーは階層構造で、管理対象装置についての一定範囲の管理情報を表示できます。

アイコン

ナビゲーション・ツリーは、モニター対象リソースを表現するのに、いくつかのアイコンを使用します。

フォルダー 1 つまたは複数の従属項目を表わす上位レベルのリソース。たとえば、ツリーの一番上のフォルダーは、通常は装置自体を表わします。後続のレベルの他のフォルダーは、構成情報や障害情報を表します。

各フォルダーの中には、そのフォルダーの全体情報を構成する各項目が入っています。フォルダーに示される状況は、直属の各項目の状況から計算されます。フォルダーの横のプラス符号 (+) をクリックすると、そのフォルダーの中の項目が表示され、項目に対してアクションを取ることができます。

ページ 情報だけから成る従属リソース (構成情報など)。このリソースは、項目、管理される装置、ユーザーのアクセス権限などに応じて、ユーザーが変更できる場合と、できない場合があります。

ナビゲート

アイコンの横のプラス符号 (+) をクリックしてフォルダーを展開表示すると、従属項目が表示されます。

アイコンの横のマイナス符号 (-) をクリックしてフォルダーを縮小すると、従属項目が隠れます。

Information パネル

「Information (情報)」パネルは、「Navigation Tree」(ナビゲーション・ツリー) パネルで選択された機能に関する情報を表示します。このパネルから、VPN モニターのすべての機能を実行できます。

Message Area

Message Area (メッセージ域) は、VPN モニターのアプリケーションからの状況情報を表示します。

VPN モニターの機能

VPN モニターは、次の機能を提供します。
- モニター
- イベント報告
- 動作制御
- 障害追及
- アプリケーションの起動

以下では、VPN を管理するためのこれらの機能の使用法と、ナビゲーション・ツリー内の各機能の位置を説明します。

モニター

VPN モニターは、トンネル、クライアント、ポリシーなど、ネットワークのさまざまな側面に関する情報を表示します。 第6章 VPN モニター Global Status フォルダーは、VPN ネットワークの各エレメントの状況に関する一般情報を提供します。詳しい情報を表示したい場合は、第7章 VPN モニター Tunnels フォルダー、 第8章 VPN モニター Clients フォルダー、第10章 VPN モニター Policies フォルダー、および 第9章 VPN モニター Quality of Service フォルダーを使用してください。

これらのフォルダーは、ネットワーク内の各エレメントの状況について重要な情報を提供します。

イベント報告

VPN に関する追加情報を提供するために、VPN モニターのアプリケーションは、ネットワーク内で発生したイベントのログとカウンターを提供します。これらは、第11章 VPN Monitor Events フォルダーに表示されます。

Events (イベント) フォルダーは、レイヤー 2 トンネルとセッションの成功や失敗のイベント・ログとカウンター、および IPSec トンネルや暗号化の成功や失敗のイベント・ログとカウンターを表示します。

動作制御

VPN モニターのアプリケーションを使用すると、管理ワークステーションからトンネル、クライアント、およびポリシーを制御できます。 第12章 VPN モニター Operational フォルダーを使用して、IPSec およびレイヤー 2 トンネルの使用可能 / 使用不可、クライアントの使用可能 / 使用不可、およびポリシーのリフレッシュを行うことができます。

障害追及

ネットワーク内の接続問題を追跡する他に、VPN モニターのアプリケーションは、第13章 VPN モニター Tests フォルダーでさまざまなツールを提供し、ユーザーが潜在的な接続性をテストしたり、ネットワークに構築する前に新しいポリシーの効果をテストしたり、指定のトンネルや指定のホストへの往復時間をテストしたりするのを支援します。

アプリケーションの起動

VPN モニターのアプリケーションは、ネットワークを管理するのに役立ついくつかのアプリケーションを起動できます。これには、次のものが含まれます。

- Telnet
- モニター対象装置の JMA
- MIB ブラウザー
- Web ブラウザー

第5章 VPN モニター General フォルダー

VPN モニター General (一般) フォルダーは、ネットワーク内の VPN 装置に関する情報を提供します。このフォルダーには 2 つの従属項目が含まれています。

- Identification (識別)
- Administration (管理)

Identification

「Identification (識別)」パネルは、選択された VPN 装置を説明する一般情報を提供します。このパネルには次のフィールドがあり、装置の MIB から検索された情報が入っています。

Description
装置の説明。

Device ID
装置のシステム・オブジェクト識別子 (SYSOID)。

Contact
装置の MIB に入っている接続情報。許可ユーザーは、この情報を「Identification」パネルから変更できます。

Domain Name
装置が使用する IP ドメイン名。許可ユーザーは、この情報を「Identification」パネルから変更できます。

Location
装置の場所の情報。許可ユーザーは、この情報を「Identification」パネルから変更できます。

Up Time
装置が前回に始動または再始動された以降に経過した時間の長さ。

System Services
装置の機能を表す数値。

System Service Functions
「System Services (システム・サービス)」番号で表された機能のテキスト記述。

Administration

「Administration (管理)」パネルは、VPN モニターが装置と通信するのに使用する SNMP パラメーターを表示します。許可ユーザーは、この情報を「Administration」パネルから変更できます。

「Administration」パネルには、次のフィールドがあります。

IP Address
SNMP 要求に使われる IP アドレス。

Community Name (Read)
読み取り要求に使われる SNMP コミュニティー名。

Community Name (Write)
書き込み要求に使われる SNMP コミュニティー名。

Remote Port
SNMP 要求に使われる装置上のポート。

Timeout (ms)
SNMP 要求に使われるタイムアウト値 (ミリ秒)。

Retries SNMP 要求に使われる再試行回数。

Polling Interval
SNMP 要求に使われるポーリング間隔 (ミリ秒)。

第6章 VPN モニター Global Status フォルダー

VPN モニター Global Status (グローバル状況) フォルダーは、選択された装置上の VPN 処理のビューを表示します。このフォルダーには、次の従属項目が含まれています。

- At-A-Glance (一覧)

At-A-Glance

「At-A-Glance (一覧)」パネルは、選択された装置上の VPN 処理に関する要約情報を提供します。これには、次のセクションが含まれています。

- Levels (レベル)
- Tunnels (トンネル)
- Clients (クライアント)
- Policy (ポリシー)
- Events (イベント)

Levels

「Levels」セクションは、装置が使用している MIB とプロトコル・コードに関する情報を提供します。ここには、次のフィールドがあります。

Layer-2 MIB Version
装置が使用しているレイヤー 2 MIB のバージョン。

Layer-2 Protocol Version
装置が使用しているレイヤー 2 プロトコル・コードのバージョン。

IPSec MIB Version
装置が使用している IPSec MIB のバージョン。

Policy MIB Version
装置が使用しているポリシー MIB のバージョン。

Tunnels

「Tunnels」セクションは、この装置上の現在アクティブのレイヤー 2 および IPSec トンネルの数に関する情報を提供します。

Clients

「Clients」セクションは、この装置上の現在アクティブのレイヤー 2 セッションの数を表示します。

Policy

「Policy」セクションは、現在装置が使用している VPN ポリシーに関する情報を提供します。ここには、次のフィールドがあります。

Policy Up Time
現行のポリシー・コンポーネント・コードのアップ時間。

Device Up Time
装置のアップ時間。

Device Current Time
装置が使用している現在時間。

Hours from UTC
装置が使用している時間と協定世界時 (UTC) の差。

Current Config Source
現行ポリシー構成のソース。

Policy Load Status
ポリシーをロードする最後の試行の結果。

Events

「Events」セクションは、この装置の VPN モニターによってモニターされているイベントに関する情報を提供します。ここには、次のフィールドがあります。

Layer-2 Tunnel Successes
正常に活動化された、この装置のレイヤー 2 トンネルの数。

Layer-2 Tunnel Failures
活動化を試みたが成功しなかった、この装置のレイヤー 2 トンネルの数。

Layer-2 Session Successes
正常に活動化された、この装置のレイヤー 2 セッションの数。

Layer-2 Session Failures
この装置のレイヤー 2 セッション活動化に失敗した試行回数。

IPSec In Authentications
正常に行われたインバウンド IPSec 認証の数。

IPSec In Authentication Failures
失敗したインバウンド IPSec 認証の試行回数。

IPSec In Decryptions
正常に行われたインバウンド IPSec 復号の数。

IPSec In Decryption Failures
失敗したインバウンド IPSec 復号の試行回数。

IPSec Out Authentications
正常に行われたアウトバウンド IPSec 認証の数。

IPSec Out Authentication Failures
失敗したアウトバウンド IPSec 認証の試行回数。

IPSec Out Encryptions
正常に行われたアウトバウンド IPSec 暗号化の数。

IPSec Out Encryption Failures
失敗したアウトバウンド IPSec 暗号化の試行回数。

第7章 VPN モニター Tunnels フォルダー

VPN モニター Tunnels (トンネル) フォルダーには、選択された装置が使用するレイヤー 2 および IPSec トンネルの状況に関する情報が入っています。このフォルダーには、次の従属項目があります。

- Layer-2 Tunnels (レイヤー 2 トンネル) フォルダー
- IPSec Tunnels (IPSec トンネル) フォルダー

Layer-2 Tunnels フォルダー

「Layer-2 Tunnels (レイヤー 2 トンネル)」フォルダーは、選択された装置上のアクティブとプレビアス・レイヤー 2 トンネルに関する情報を提供します。このフォルダーには、次の従属項目があります。

- Active Tunnels (アクティブ・トンネル) パネル
- Previous Tunnels (プレビアス・トンネル) パネル

Active フォルダー

「Layer-2 Active Layer-2 Tunnels (レイヤー 2 アクティブ・レイヤー 2 トンネル)」フォルダーは、選択された装置に関連したすべてのアクティブなレイヤー 2 トンネルの情報を提供します。このフォルダーには、次の従属項目があります。

- Status (状況) パネル
- Attributes (属性) パネル
- Statistics (統計) パネル
- End-Points (エンド・ポイント) パネル

Status パネル

「Status (状況)」パネルは、選択された装置に関連したアクティブのレイヤー 2 トンネルの状況に関する情報を提供します。ここには、次のフィールドがあります。

Tunnel トンネルのインデックス番号。

Status トンネルの状況: active (アクティブ) または destroy (破棄)。許可ユーザーは、この値を「Status」パネルから変更できます。

Type トンネルのタイプ: L2TP、L2F、PPTP。

Remote Host
このトンネルに関連したリモート・ホストの名前。

Active Time
トンネルがアクティブになっている時間の長さ。

Active Sessions
このトンネルに関連したアクティブ・セッションの数。

Previous Sessions
このトンネルに関連した以前のアクティブ・セッションの数。

Destroy All Tunnels
すべてのレイヤー 2 トンネルの破棄を起動します。許可ユーザーは、この値を「Status」パネルから変更できます。

Attributes パネル

「Attributes (属性)」パネルは、選択されたトンネルの属性に関する情報を提供します。ここには、次のフィールドがあります。

Local Control ID
トンネルのローカル制御 ID。

Peer Control ID
トンネルの相手側制御 ID。

Control State
トンネルの制御状態。

Control Timouts
このトンネルで記録された制御タイムアウトの回数。

Remote Host
このトンネルに関連したリモート・ホストの名前。

Remote Vendor Name
リモート・ホストのベンダーの名前。

Remote Firmware Version
リモート・ホストで実行されているファームウェアのバージョン。

Remote Protocol Version
リモート・ホストが使用しているプロトコル・バージョン。

Init Connect
トンネルがローカル・ホストによって生成されたのかどうかを示します。

Local Receive Packet Window
ローカル・ホストが使用する受信パケット・ウィンドウのサイズ。

Remote Receive Packet Window
リモート・ホストが使用する受信パケット・ウィンドウのサイズ。

Next Send Sequence
次の送信シーケンス番号の値。

Next Receive Sequence
次の受信シーケンス番号の値。

Statistics パネル

「Statistics (統計)」パネルは、指定されたレイヤー 2 トンネルについての統計を提供します。ここには、次のフィールドがあります。

In Bytes
このトンネルを介して受信したバイト数。

In Packets
このトンネルを介して受信したパケットの数。

In Discarded Packets
このトンネルを介して受信中に廃棄されたパケットの数。

Out Bytes
ローカル・ホストがこのトンネルを介して送信したバイト数。

Out Packets
ローカル・ホストがこのトンネルを介して送信したパケットの数。

Out Discarded Packets
ローカル・ホストがこのトンネルを介して送信中に廃棄したパケットの数。

End Points パネル

「End Points (エンド・ポイント)」パネルは、選択されたトンネルのエンド・ポイントに関する情報を提供します。ここには、次のフィールドがあります。

Remote IP Address
選択されたトンネルに関連したリモート IP アドレス。

Local IP Address
選択されたトンネルのローカル IP アドレス。

Source Port
このトンネルに関連したローカル・ホストのポート。

Destination Port
このトンネルに関連したリモート・ホストのポート。

Previous Tunnels フォルダー

「Previous Layer-2 Tunnels (以前のレイヤー 2 トンネル)」フォルダーは、選択された装置に関連した、指定の以前のレイヤー 2 トンネルの要約と統計情報を提供します。情報を表示する以前のエントリーの数は、「Summary」パネルで指定できます。「Previous Layer-2 Tunnels」フォルダーには、次の従属項目があります。

- Summary panel (要約パネル)
- Statistics panel (統計パネル)

Summary パネル

「Summary (要約)」パネルは、選択された以前にアクティブであったレイヤー 2 トンネルに関する情報を提供します。ここには、次のフィールドがあります。

Order トンネルが終了した順序。

Tunnel トンネルのインデックス。

Type トンネルのタイプ: L2TP、L2F、PPTP。

Remote Host
トンネルに関連したリモート・ホストの名前。

Remote IP Address
トンネルに関連したリモート IP アドレス。

Remote Port
トンネルに関連したリモート・ポート。

Local IP Address
トンネルに関連したローカル IP アドレス。

Local Port
トンネルに関連したローカル・ポート。

Total Sessions
トンネルを使用したアクティブ・セッションの合計数。

Tunnel Up Time
トンネルがアクティブであった時間の長さ。

Statistics パネル

「Statistics」(統計) パネルは、以前のトンネルの使用に関する情報を提供します。ここには、次のフィールドがあります。

In Bytes
モニターされた装置がこのトンネルを介して受信したバイト数。

In Packets
モニターされた装置がこのトンネルを介して受信したパケットの数。

In Discarded Packets
モニターされた装置がこのトンネルを介して受信中に廃棄したパケットの数。

Out Bytes
モニターされた装置がこのトンネルを介して送信したバイト数。

Out Packets
モニターされた装置がこのトンネルを介して送信したパケットの数。

Out Discarded Packets
モニターされた装置がこのトンネルを介して送信中に廃棄したパケットの数。

IPSec Tunnels フォルダー

「IPSec Control Tunnels (IPSec 制御トンネル)」フォルダーは、選択された装置上のアクティブと以前の IPSec トンネルに関する情報を提供します。このフォルダーには、次の従属項目があります。
- Active Tunnels (アクティブ・トンネル) フォルダー
- Previous Tunnels (以前のトンネル) フォルダー

Active Tunnels フォルダー

「IPSec Active Tunnels (IPSec アクティブ・トンネル)」フォルダーは、アクティブ IPSec 制御トンネルおよびユーザー・データ・トンネルに関する情報を提供します。このフォルダーには、次の従属項目があります。
- IPSec Control Tunnels (IPSec 制御トンネル) フォルダー
- IPSec User-Data Tunnels (IPSec ユーザー・データ・トンネル) フォルダー

IPSec Control Tunnels フォルダー

「IPSec Control Tunnels (IPSec 制御トンネル)」フォルダーは、選択された装置に関連したアクティブ IPSec 制御トンネルに関する情報を提供します。このフォルダーには、次のパネルがあります。
- Status (状況)
- Attributes (属性)
- Statistics (統計)
- Processing (処理)

Status: 「Status」パネルは、選択された IPSec 制御トンネルの状況に関する情報を提供します。ここには、次のフィールドがあります。

Tunnel 選択されたトンネルのインデックス番号。

Status トンネルの状況: active (アクティブ) または destroy (破棄)。許可ユーザーは、この値を「Status」パネルから変更できます。

ID 選択されたトンネルの ID。

Remote Name
トンネルのリモート名。

Remote Address
トンネルのリモート IP アドレス。

Local Name
トンネルのローカル名。

Local Address
トンネルのローカル IP アドレス。

Up Time
トンネルがアクティブになっていた時間の長さ。

Destroy All Tunnels
すべてのアクティブ IPSec 制御トンネルの破棄を起動します。許可ユーザーは、この値を「Status」パネルから変更できます。

Attributes: 「Attributes (属性)」パネルは、選択された IPSec 制御トンネルの属性に関する情報を提供します。ここには、次のフィールドがあります。

Negotiation Mode
選択された IPSec 制御トンネルが、リモート・ホストとの新しい接続を折衝するのに使用しているモード。

SA Lifetime
トンネルのセキュリティー・アソシエーションの存続時間 (秒)。

SA Refresh Threshold Percent
セキュリティー・アソシエーション・リフレッシュしきい値パーセント。

Total SA Refreshes
実行されたセキュリティー・アソシエーション・リフレッシュの数。

Statistics: このパネルは、選択された IPSec 制御パネルに関する統計を提供します。ここには、次のフィールドがあります。

In Bytes
モニターされた装置がこのトンネルを介して受信したバイト数。

In Packets
モニターされた装置がこのトンネルを介して受信したパケットの数。

In Dropped Packets
モニターされた装置がこのトンネルを介して受信中に廃棄したパケットの数。

Out Bytes
モニターされた装置がこのトンネルを介して送信したバイト数。

Out Packets
モニターされた装置がこのトンネルを介して送信したパケットの数。

Out Dropped Packets
モニターされた装置がこのトンネルを介して送信中に廃棄したパケットの数。

Processing: このパネルは、選択された IPSec 制御トンネルに関連する処理に関する情報を提供します。ここには、次のフィールドがあります。

In Notifys
このトンネルを介して受信した通知の数。

In Proposals
このトンネルを介して受信した提案の数。

In Invalid Proposals
このトンネルを介して受信した無効の提案の数。

In Rejected Proposals
このトンネルを介して受信し、拒否された提案の数。

In SA Deletes
このトンネルを介して受信したセキュリティー・アソシエーション削除の数。

Out Notifys
このトンネルを介して送信した通知の数。

Out Proposals
このトンネルを介して送信した提案の数。

Out Invalid Proposals
このトンネルを介して送信した無効の提案の数。

Out Rejected Proposals
このトンネルを介して送信し、拒否された提案の数。

Out SA Deletes
このトンネルを介して送信したセキュリティー・アソシエーション削除の数。

Active IPSec User-Data Tunnels フォルダー

このフォルダーは、選択された装置に関連したアクティブ IPSec ユーザー・データ・トンネルに関する情報を提供します。このフォルダーには、次の従属項目があります。

- Status (状況) パネル
- Attributes (属性) パネル
- Statistics (統計) パネル
- End Points (エンド・ポイント) パネル
- Security Protection Indices (セキュリティー保護インデックス) パネル

Status パネル: このパネルは、選択された IPSec ユーザー・データ・トンネルの状況に関する情報を提供します。ここには、次のフィールドがあります。

Tunnel 選択されたトンネルのインデックス番号。

Status トンネルの状況: active (アクティブ) または destroy (破棄)。許可ユーザーは、この値を「Status」パネルから変更できます。

Remote IP Address
トンネルのリモート IP アドレス。

Local IP Address
トンネルのローカル IP アドレス。

Up Time
トンネルがアクティブになっていた時間の長さ。

Total Security Association Refreshes
実行されたセキュリティー・アソシエーション・リフレッシュの合計数。

Current Security Associations
現行のセキュリティー・アソシエーションの数。

Expired Security Associations
期限切れしたセキュリティー・アソシエーションの数。

Destroy All Tunnels
すべてのアクティブ IPSec ユーザー・データ・トンネルの破棄を起動します。許可ユーザーは、この値を「Status」パネルから変更できます。

Attributes パネル: このパネルは、選択された IPSec ユーザー・データ・トンネルの属性に関する情報を提供します。ここには、次のフィールドがあります。

ID トンネルのインデックス番号。

Control Tunnel
この IPSec ユーザー・データ・トンネルに関連した IPSec 制御トンネルのインデックス番号。

Key Type
トンネルのキー・タイプ。

Encapsulation Mode
トンネルのカプセル化モード。

Security Association Lifetime
トンネルのセキュリティー・アソシエーションの存続時間 (秒)。

Security Association Refresh Threshold Percent
セキュリティー・アソシエーション・リフレッシュしきい値パーセント。

In SA Encryption
このトンネルで使用されるインバウンド暗号化タイプ。

In SA Authentication
このトンネルで使用されるインバウンド認証アルゴリズム。

Out SA Encryption
このトンネルで使用されるアウトバウンド暗号化タイプ。

Out SA Authentication
このトンネルで使用されるアウトバウンド認証アルゴリズム。

Statistics パネル: このパネルは、選択された IPSec ユーザー・データ・トンネルの使用統計を提供します。ここには、次のフィールドがあります。

In Bytes
このトンネルを介して受信したバイト数。

In Byte Counter Wraps
着信バイト・カウンターが折り返した回数。

In Decompressed Bytes
このトンネルを介して受信した解凍バイト数。

In Decompressed Byte Wraps
着信解凍バイト・カウンターが折り返した回数。

In Packets
このトンネルを介して受信したパケットの数。

In Dropped Packets
このトンネルを介して受信中に廃棄されたパケットの数。

In Authentications
このトンネルで実行されたインバウンド認証の数。

In Authentication Failures
このトンネルで実行されて失敗したインバウンド認証の数。

In Decryptions
このトンネルで実行されたインバウンド復号の数。

In Decryption Failures
このトンネルで実行されて失敗したインバウンド復号の数。

Out Bytes
このトンネルを介して送信したバイト数。

Out Byte Counter Wraps
発信バイト・カウンターが折り返した回数。

Out Decompressed Bytes
このトンネルを介して送信した解凍バイト数。

Out Decompressed Byte Wraps
発信解凍バイト・カウンターが折り返した回数。

Out Packets
このトンネルを介して送信したパケットの数。

Out Dropped Packets
このトンネルを介して送信中に廃棄されたパケットの数。

Out Authentications
このトンネルで実行されたアウトバウンド認証の数。

Out Authentication Failures
このトンネルで実行されて失敗したアウトバウンド認証の数。

Out Encryptions
このトンネルで実行されたアウトバウンド暗号化の数。

Out Encryption Failures
このトンネルで実行されて失敗したアウトバウンド暗号化の数。

End Points パネル: このパネルは、選択されたトンネルのエンド・ポイントに関する情報を提供します。ここには、次のフィールドがあります。

Local Name
トンネルのローカル名。

Local Type
ローカル・アドレス・タイプ: subnet (サブネット) または range (範囲)。

Local Protocol
トンネルのローカル・プロトコル。

Local Subnet Mask
トンネルで使用されるローカル・サブネット・マスク。

Local Low IP Address
トンネルのローカル下位 IP アドレス。

Local High IP Address
トンネルのローカル上位 IP アドレス。

Local Port
トンネルが使用するローカル・ポート。

Remote Name
トンネルのリモート名。

Remote Type
リモート・アドレス・タイプ: subnet (サブネット) または range (範囲)。

Remote Protocol
トンネルのリモート・プロトコル。

Remote Subnet Mask
トンネルで使用されるリモート・サブネット・マスク。

Remote Low IP Address
トンネルのリモート下位 IP アドレス。

Remote High IP Address
トンネルのリモート上位 IP アドレス。

Remote Port
トンネルが使用するリモート・ポート。

Security Protection Indices パネル: このパネルは、トンネルが使用しているセキュリティー保護インデックス (SPI) に関する情報を提供します。ここには、次のフィールドがあります。

SPI トンネルが使用しているセキュリティー保護インデックス。

Direction
SPI が適用されているトラフィックの方向: in (インバウンド) または out (アウトバウンド)。

Value SPI の値。

Protocol
SPI で使用されるプロトコル。

Previous IPSec User-Data Tunnels フォルダー

このフォルダーは、もうアクティブでなくなっている IPSec ユーザー・データ・トンネルに関する情報を提供します。このフォルダーには、次のパネルがあります。

- Summary (要約) パネル
- Statistics (統計) パネル

Summary パネル: このパネルは、以前の IPSec ユーザー・データ・トンネルに関する要約情報を提供します。ここには、次のフィールドがあります。

Order トンネルが終了した順序。

ID トンネルの ID。

Remote IP Address
トンネルが使用したリモート IP アドレス。

Local IP Address
トンネルが使用したローカル IP アドレス。

Up Time
トンネルがアクティブであった時間の長さ。

Total SA Refreshes
このトンネルで実行されたセキュリティー・アソシエーション・リフレッシュの数。

Total SAs
このトンネルのセキュリティー・アソシエーションの合計数。

Statistics パネル: このパネルは、選択された以前にアクティブであった IPSec ユーザー・データ・トンネルの使用統計を提供します。ここには、次のフィールドがあります。

In Bytes
このトンネルを介して受信したバイト数。

In Byte Counter Wraps
着信バイト・カウンターが折り返した回数。

In Decompressed Bytes
このトンネルを介して受信した解凍バイト数。

In Decompressed Byte Wraps
着信解凍バイト・カウンターが折り返した回数。

In Packets
このトンネルを介して受信したパケットの数。

In Dropped Packets
このトンネルを介して受信中に廃棄されたパケットの数。

In Authentications
このトンネルで実行されたインバウンド認証の数。

In Authentication Failures
このトンネルで実行されて失敗したインバウンド認証の数。

In Decryptions
このトンネルで実行されたインバウンド復号の数。

In Decryption Failures
このトンネルで実行されて失敗したインバウンド復号の数。

Out Bytes
このトンネルを介して送信したバイト数。

Out Byte Counter Wraps
発信バイト・カウンターが折り返した回数。

Out Decompressed Bytes
このトンネルを介して送信した解凍バイト数。

Out Decompressed Byte Wraps
発信解凍バイト・カウンターが折り返した回数。

Out Packets
このトンネルを介して送信したパケットの数。

Out Dropped Packets
このトンネルを介して送信中に廃棄されたパケットの数。

Out Authentications
このトンネルで実行されたアウトバウンド認証の数。

Out Authentication Failures
このトンネルで実行されて失敗したアウトバウンド復号の数。

Out Encryptions

このトンネルで実行されたアウトバウンド暗号化の数。

Out Encryption Failures

このトンネルで実行されて失敗したアウトバウンド暗号化の数。

第8章 VPN モニター Clients フォルダー

VPN モニター Clients (クライアント) フォルダーは、レイヤー 2 セッションに関する情報を提供します。このフォルダーには、次のサブフォルダーが含まれています。

- Layer-2 Sessions (レイヤー 2 セッション)

Layer-2 Sessions フォルダー

このフォルダーは、選択された装置のレイヤー 2 セッションに関する情報を提供します。これには、次のサブフォルダーが含まれています。

- Active Sessions (アクティブ・セッション)
- Previous Sessions (以前のセッション)

Active Sessions フォルダー

このフォルダーは、選択された装置のアクティブのレイヤー 2 セッションに関する情報を提供します。このフォルダーには、次のパネルがあります。

- Status (状況)
- Statistics (統計)

Status フォルダー

このフォルダーは、選択されたレイヤー 2 セッションに関する状況情報を提供します。このフォルダーには、次のパネルがあります。

- Status (状況)
- Attributes (属性)
- Statistics (統計)

Status パネル: このパネルは、選択されたレイヤー 2 セッションの状況に関する情報を提供します。ここには、次のフィールドがあります。

Tunnel 選択されたセッションが使用するトンネルのインデックス。

Session
セッションのインデックス。

Status セッションの状況: active (アクティブ) または destroy (破棄)。許可ユーザーは、この値を「Status」パネルから変更できます。

Session Up Time
セッションがアクティブになっている時間の長さ。

Connect BPS
接続の速度 (ビット / 秒)。

Authentication Method
このセッションで使用される認証方式。

Encryption/Decryption
このセッションの暗号機能標識。 True (真) は、セッションで暗号化と復号が使用されることを示します。False (偽) は、それらが使用されないことを示します。

Destroy All Sessions
すべてのレイヤー 2 セッションの破棄を起動します。許可ユーザーは、この値を「Status」パネルから変更できます。

Attributes パネル: このパネルは、選択されたセッションの属性をリストします。ここには、次のフィールドがあります。

Remote Name
セッションのリモート名。

Line State
セッションのライン状態。

Local ID
セッションのローカル ID。

Remote ID
セッションのリモート ID。

Device Number
セッションで使用されている装置番号。

Serial Number
セッションで使用されている装置の通し番号。

Bearer Type
セッションで使用されている伝達タイプ: digital (ディジタル) または analog (アナログ)。

Framing Type
セッションで使用されているフレーム・タイプ: synchronous (同期) または asynchronous (非同期)。

Local Packet Window
ローカル・パケット・ウィンドウのサイズ。

Remote Packet Window
リモート・パケット・ウィンドウのサイズ。

Timeouts
このセッション中に発生したタイムアウトの回数。

Next Send Sequence
次の送信シーケンス番号の値。

Next Receive Sequence
次の受信シーケンス番号の値。

Remote PPD
リモート・パケット処理遅延の長さ。

Statistics パネル: このパネルは、選択されたレイヤー 2 セッションの統計情報を提供します。ここには、次のフィールドがあります。

In Bytes
受信したバイト数。

In Uncompressed Bytes
受信した非圧縮バイト数。

In Packets
受信したパケットの数。

In Discarded Packets
受信中に廃棄されたパケットの数。

Out Bytes
送信したバイト数。

Out Uncompressed Bytes
送信した非圧縮バイト数。

Out Packets
送信したパケットの数。

Out Discarded Packets
送信中に廃棄されたパケットの数。

Previous Layer-2 Sessions フォルダー

このフォルダーは、選択された装置の以前のレイヤー 2 セッションに関する情報を提供します。これには、次の従属項目が含まれています。
- Summary (要約) パネル
- Statistics (統計) パネル

Summary パネル: このパネルは、選択された装置上の選択されたレイヤー 2 セッションに関する要約情報を提供します。ここには、次のフィールドがあります。

Order セッションが終了した順序。

Tunnel セッションで使用されたトンネルのインデックス。

Session
以前にアクティブであったセッションのインデックス。

Authentication Method
セッションで使用された認証方式。

Encryption/Decryption
セッションの暗号機能標識。 True (真) は、セッションで暗号機能が使用されたことを示します。False (偽) は、それが使用されなかったことを示します。

Up Time
セッションがアクティブであった時間の長さ。

Statistics パネル: このパネルは、選択された装置上の以前にアクティブであったレイヤー 2 セッションに関する統計情報を提供します。ここには、次のフィールドがあります。

In Bytes
受信したバイト数。

In Uncompressed Bytes
受信した非圧縮バイト数。

In Packets
受信したパケットの数。

In Discarded Packets
受信中に廃棄されたパケットの数。

Out Bytes
送信したバイト数。

Out Uncompressed Bytes
送信した非圧縮バイト数。

Out Packets
送信したパケットの数。

Out Discarded Packets
送信中に廃棄されたパケットの数。

第9章 VPN モニター Quality of Service フォルダー

このフォルダーは、リソース予約プロトコル (RSVP) を使用する、選択されたセッションのサービス品質に関する情報を提供します。これには、次の従属項目があります。

- RSVP

RSVP フォルダー

このフォルダーには、選択されたセッションで使用されるリソース予約プロトコル (RSVP) に関する情報が入っています。このフォルダーには、次のパネルがあります。

- Sessions (セッション)
- Sender PATH Messages (送信側 PATH メッセージ)
- Upstream RESV Messages (アップストリーム RESV メッセージ)

Sessions パネル

このパネルは、選択されたセッションの RSVP 情報を提供します。ここには、次のフィールドがあります。

Session Index
セッション・インデックス。

Session Type
セッション・タイプ。

IP Protocol
セッションで使用される IP プロトコル。

Destination Address
セッションのあて先アドレス。

Destination Port
セッションのあて先ポート。

Number of Senders
セッションの送信側の数。

Number of RSVP Requests Received
選択された装置が受信した RSVP 要求の数。

Number of RSVP Requests Sent
選択された装置が送信した RSVP 要求の数。

Sender PATH Messages パネル

このパネルには、選択されたセッションのパス情報が入っています。ここには、次のフィールドがあります。

Session Index
セッションのインデックス。

Sender Index
このセッションに関連した送信側のインデックス。

Session Type
セッションのタイプ。

IP Protocol
セッションの IP プロトコル。

Destination Address
このセッションに関連したあて先アドレス。

Destination Port
このセッションに関連したあて先ポート。

Source Address
このセッションに関連したソース・アドレス。

Source Port
このセッションに関連したソース・ポート。

IPv6 Flow Identifier
このセッションの IPv6 フロー識別子。

Previous Hop Address
直前のホップの IP アドレス。

Previous Hop Logical Interface Handle
直前のホップの論理インターフェース・ハンドル。

Last Interface Index
最後のインターフェース・インデックス。

Average BPS
このセッションの平均接続速度 (ビット / 秒)。

Peak BPS
このセッションのピーク接続速度 (ビット / 秒)。

Maximum Expected Bytes
この接続で可能な最大バイト数。

Minimum Message Size
セッションで使用する最小メッセージ・サイズ。

Maximum Message Size
セッションで使用する最大メッセージ・サイズ。

Refresh Message Interval
このセッションで送信するリフレッシュ・メッセージの間隔。

Previous Hop Is RSVP
直前のホップが RSVP ホップであったかどうかを示します。

Path Message Last Change
パス・メッセージが前回に変更された時刻。

Policy この送信側に関連したポリシー。

Last TTL Value
このセッションで使用する最終活動時間の値。

Non-IS Hop Detected
このセッションで非 IS ホップが検出されたかどうかを示します。

Hop Count
このセッションのホップ・カウント。

Path Bandwidth
パッチ帯域幅。

Minimum Path Latency
最小パス待ち時間。

Maximum Transmission Unit
このセッションの最大伝送単位 (MTU) サイズ。

Guaranteed Service
このセッションではサービスが保証されるかどうかを示します。

Break In Service
このセッションでサービス違反が発生したかどうかを示します。

Hop Count Override
このセッションのホップ・カウント・オーバーライド。

Path Bandwidth Override
このセッションのパス帯域幅オーバーライド。

Minimum Path Latency Override
このセッションの最小パス待ち時間オーバーライド。

Maximum Transmission Unit Override
このセッションの最大伝送単位オーバーライド。

Upstream RESV Messages パネル

このパネルは、選択されたセッションのアップストリーム RESV メッセージに関する情報を提供します。ここには、次のフィールドがあります。

Session Index
セッションのインデックス。

Request Index
要求のインデックス。

Session Type
セッション・タイプ。

IP Protocol
このセッションで使用する IP プロトコル。

Destination Address
このセッションに関連したあて先アドレス。

Destination Port
このセッションに関連したあて先ポート。

Source Address
このセッションに関連したソース・アドレス。

Source Port
このセッションに関連したソース・ポート。

Previous Hop Address
直前のホップの IP アドレス。

Previous Hop Logical Interface Handle
直前のホップの論理インターフェース・ハンドル。

Last Interface Index
最後のインターフェース・インデックス。

Quality of Service
このセッションに要求されたサービス品質の区分。

Average BPS
この接続の平均速度 (ビット / 秒)。

Peak BPS
この接続のピーク速度 (ビット / 秒)。

Maximum Expected Bytes
この接続で可能な最大バイト数。

Minimum Message Size
この接続で使用する最小メッセージ・サイズ。

Maximum Message Size
この接続で使用する最大メッセージ・サイズ。

Refresh Message Interval
この接続のリフレッシュ・メッセージ間隔。

Scope スコープ・オブジェクトの値。

Shared Reservation
共用予約の標識。

Explicit Senders
明示的な送信側の標識。

Next Hop Is RSVP Hop
次のホップが RSVP ホップかどうかを示します。

Last Change
前回の変更の時刻。

Policy この要求に関連したポリシー。

Last TTL Value
受信した最後の活動時間の値。

IPv6 Flow Identifier
IPv6 フロー識別子。

第10章 VPN モニター Policies フォルダー

このフォルダーには、VPN 接続を制御するのに使用されるポリシーに関する情報が入っています。このフォルダーには、次の従属項目があります。

- Device (装置) フォルダー
- Conditions (条件) フォルダー
- Actions (アクション) フォルダー

Device フォルダー

「Device (装置)」フォルダーは、選択された装置用に作成されたポリシーに関する情報を提供します。このフォルダーには、次のパネルがあります。

- Policies (ポリシー)
- Filter Rules (フィルター規則)
- Policy to Rule (制御ポリシー)

「Device」フォルダーのポリシー情報の 3 つのパネルには、すべて同じフィールドがあります。フィールドは、次のとおりです。

Policy Name
ポリシーの名前。

Status ポリシーの状況: enable (使用可能) または disable (使用不可)。許可ユーザーは、この値を「Policies」パネルから変更できます。

Priority
ポリシーの優先順位。

Validity
ポリシーの有効標識。

IPSec Manual ID
手作業で設定された IPSec トンネル ID。

Matches
このポリシーの一致の数。

Validity Period
このポリシーの有効期間の名前。

Traffic Profile
このポリシーのトラフィック・プロファイルの名前。

Key Management Action
このポリシーのキー管理アクションの名前。

Data Management Action
このポリシーのデータ管理アクションの名前。

Differential Services Action
このポリシーの差別化サービス・アクションの名前。

RSVP Action
このポリシーの RSVP アクションの名前。

Conditions フォルダー

「Policy Conditions (ポリシー条件)」フォルダーは、選択されたポリシーの有効期間およびポリシー・アクションに関する情報を提供します。このフォルダーには、次の従属項目が含まれています。

- Validity Periods (有効期間) パネル
- Traffic Profiles (トラフィック・プロファイル) フォルダー

Validity Periods パネル

「Validity Periods (有効期間)」パネルは、すべての有効期間の定義を表示します。ここには、次のフィールドがあります。

Validity Period Name
有効期間の名前。

Start Date and Time
有効期間の開始日時。

End Date and Time
有効期間の終了日時。

Month Mask
有効期間の月数を決めるのに使われるマスク。

Days Mask
有効期間の日数を決めるのに使われるマスク。

Start Time of Day
有効期間の開始時刻。

End Time of Day
有効期間の終了時刻。

Traffic Profiles フォルダー

「Traffic Profiles (トラフィック・プロファイル)」フォルダーは、ポリシーに関連したトラフィック・プロファイルに関する情報を提供します。このフォルダーには、次のパネルがあります。

- Base Profiles (基本プロファイル)
- Ingress/Egress Profiles (入側 / 出側プロファイル)
- Remote ID Profiles (リモート ID プロファイル)

Base Profiles パネル: 「Base Profiles (基本プロファイル)」パネルは、ポリシーに関連した基本プロファイルに関する情報を提供します。ここには、次のフィールドがあります。

Traffic Profile Name
トラフィック・プロファイルの名前。

Low Protocol
下位プロトコル番号。

High Protocol
上位プロトコル番号。

Source Low IP Address
このプロファイルに関連した下位ソース IP アドレス。

Source High IP Address
このプロファイルに関連した上位ソース IP アドレス。

Source High Port
このプロファイルに関連した上位ポート。

Source Low Port
このプロファイルに関連した下位ポート。

Destination of Low IP Address
下位あて先 IP アドレス。

Destination of High IP Address
上位あて先 IP アドレス。

Destination Low Port
下位あて先ポート番号。

Destination High Port
上位あて先ポート番号。

Type-of-Service Byte Mask
type-of-service バイト・マスク。

Type-of-Service Byte Match
type-of-service バイト突き合わせ値。

Local ID Type
ローカル ID タイプ。

Local ID Value
ローカル ID 値。

Remote ID Group Name
リモート ID グループ名。

Ingress/Egress Profiles: このビューは、入側 / 出側プロファイルに関する情報を提供します。ここには、次のフィールドがあります。

Traffic Profile Name
トラフィック・プロファイルの名前。

Traffic Profile Ingress/Egress Index
対のインターフェースのインデックス。

Ingress IP Address
インバウンド・トラフィックの IP アドレス。

Egress IP Address
アウトバウンド・トラフィックの IP アドレス。

Remote ID Profiles パネル: このパネルは、トラフィック・プロファイルに関連したリモート ID に関する情報を提供します。ここには、次のフィールドがあります。

Traffic Profile Name
トラフィック・プロファイルの名前。

Traffic Profile Remote Group
リモート・グループの名前。

Index リモート ID のインデックス。

Type リモート ID のタイプ。

Value リモート ID の値。

Authentication Mode
このリモート ID で使用される認証モード。

Actions フォルダー

このフォルダーは、IPSec キー管理、IPSec データ管理、差別化サービス、およびリソース予約プロトコル (RSVP) に関する情報を提供します。このフォルダーには、次の従属項目があります。

- IPSec フォルダー
- Differential Services (差別化サービス) パネル
- RSVP パネル

IPSec フォルダー: 「IPSec」フォルダーは、IPSec キー管理および IPSec データ管理に関する情報を提供します。このフォルダーには、次の従属項目があります。

- Key Management (キー管理) フォルダー
- Data Management (データ管理) フォルダー

Key Management フォルダー: 「Key Management (キー管理)」フォルダーは、IPSec キー管理に関する情報を提供します。このフォルダーには、次のパネルがあります。

- Actions (アクション)

- Proposals (提案)
- Actions-to-Proposals (アクションと提案)
- Active Instances (アクティブ・インスタンス)

Actions パネル: 「Actions (アクション)」パネルは、キー管理アクションに関する情報を提供します。ここには、次のフィールドがあります。

Key Management Action Name
キー管理アクションの名前。

Exchange Mode
交換モード。

Connection SA Lifetime
接続のセキュリティー・アソシエーションの存続時間 (秒)。

Connection SA Lifesize
接続のセキュリティー・アソシエーションの存続サイズ (KB)。

Policy Role
ポリシーの役割。

Minimum Percent Refresh
最小セキュリティー・アソシエーション・リフレッシュ・パーセント。

Auto Start
自動開始標識: true (真) または false (偽)。

Matches
このアクションの一致の数。

Proposals パネル: このパネルは、キー管理提案に関する情報を提供します。ここには、次のフィールドがあります。

Key Management Proposal Name
キー管理提案の名前。

Authentication Method
この提案で使われる認証方式。

Hash Algorithm
この提案で使われるハッシュ・アルゴリズムの名前。

Cipher Algorithm
この提案で使われる暗号アルゴリズムの名前。

Diffie Hellman Group ID
この提案の diffie hellman グループ ID。

SA Lifetime
セキュリティー・アソシエーション存続時間 (秒)。

SA Lifesize
セキュリティー・アソシエーション存続サイズ (KB)。

Actions-To-Proposals パネル: このパネルは、キー・アクションとキー提案に関する情報を提供します。ここには、次のフィールドがあります。

Key Management Action Name
キー管理アクションの名前。

Proposal Name
キー管理提案の名前。

Proposal Order
キー管理提案の順序。

Action Details
「Action」パネルの情報の要約。詳しくは、Actions パネルを参照してください。

Proposal Details
「Proposals」パネルの情報の要約。詳しくは、Proposals パネルを参照してください。

Active Instances パネル: このパネルは、アクティブのキー管理インスタンスに関する情報を提供します。ここには、次のフィールドがあります。

Action Name
キー管理アクションの名前。

Create Order
このアクションが作成された順序。

KM Tunnel ID
キー管理トンネル ID。

KM Tunnel Index
キー管理トンネル・インデックス。

Action Details
「Action」パネルの情報の要約。詳しくは、Actions パネルを参照してください。

Status アクティブ・トンネルの状況: active (アクティブ) または destroy (破棄)。許可ユーザーは、この値を「Active Instances」パネルから変更できます。

IPSec Data Management フォルダー: このフォルダーは、IPSec データ管理に関する情報を提供します。このフォルダーには、次の従属項目が含まれています。

- Actions (アクション) パネル
- Proposals (提案) パネル
- Active Instances (アクティブ・インスタンス) パネル
- Transforms (変換) フォルダー
- Correlations (相関) フォルダー

Actions パネル: このパネルは、IPSec データ管理アクションに関する情報を提供します。ここには、次のフィールドがあります。

Data Management Action Name
データ管理アクションの名前。

Type アクションのタイプ: permit (許可) または deny (拒否)。

Tunnel Start IP Address
トンネルの開始 IP アドレス。

Tunnel End IP Address
トンネルの終了 IP アドレス。

Local Proxy Type
ローカル・プロキシーのタイプ。

Local Proxy Value
ローカル・プロキシーの値。

Local Proxy Protocol
ローカル・プロキシーのプロトコル。

Local Proxy Source Port
ローカル・プロキシー・ソース・ポート番号。

Remote Proxy Type
リモート・プロキシーのタイプ。

Remote Proxy Value
リモート・プロキシーの値。

Remote Proxy Protocol
リモート・プロキシーのプロトコル。

Remote Proxy Source Port
リモート・プロキシー・ソース・ポート番号。

SA Refresh Threshold Percent
セキュリティー・アソシエーション・リフレッシュしきい値。

Minimum SA Refresh Threshold Percent
最小セキュリティー・アソシエーション・リフレッシュしきい値。

Tunnel-In-Tunnel
トンネル内トンネル標識。

Auto Start
自動開始の設定: enable (使用可能) または disable (使用不可)。

Don't Fragment Bit Handling
「断片ビット処理禁止」標識。

Replay Prevention
再生防止の設定。

Matches
このアクションの一致の数。

Proposals パネル: このパネルは、データ管理提案に関する情報を提供します。ここには、次のフィールドがあります。

Name データ管理アクションの名前。

Perfect-Forward-Secrecy
完全転送秘密の設定: enable (使用可能) または disable (使用不可)。

Diffie Hellman Group ID
diffie hellman グループ ID。

Active Instances パネル: このパネルは、アクティブのデータ管理インスタンスに関する情報を提供します。ここには、次のフィールドがあります。

Data Management Action
データ管理アクションの名前。

Creation Order
データ管理アクションが作成された順序。

Key Management Tunnel ID
キー管理トンネル ID。

Data Management Tunnel Index
データ管理トンネル・インデックス。

Data Management Action Details
「Data Management Action」パネルの要約。詳しくは、59ページの『Actions パネル』を参照してください。

Key Management Action Details
「Key Management Action」パネルの要約。詳しくは、57ページの『Actions パネル』を参照してください。

Transforms フォルダー: このフォルダーは、データ管理の変換に関する情報を提供します。このフォルダーには、次のパネルがあります。

- AH Transforms (AH 変換)
- ESP Transforms (ESP 変換)
- IPCOMP Transforms (IPCOMP 変換)

AH Transforms パネル: このパネルは、認証ヘッダー (AH) 変換に関する情報を提供します。ここには、次のフィールドがあります。

AH Transform Name
認証ヘッダー変換の名前。

Encapsulation Algorithm
AH 変換で使われるカプセル化アルゴリズム。

Integrity Algorithm
AH 変換で使われる整合性アルゴリズム。

SA Lifetime
セキュリティー・アソシエーション存続時間 (秒)。

SA Lifesize
セキュリティー・アソシエーション存続サイズ (KB)。

ESP Transforms パネル: このパネルは、カプセル化セキュリティー・ペイロード (ESP) 変換に関する情報を提供します。ここには、次のフィールドがあります。

ESP Transform Name
ESP 変換の名前。

Encapsulation Algorithm
ESP 変換で使われるカプセル化アルゴリズム。

Integrity Algorithm
ESP 変換で使われる整合性アルゴリズム。

SA Lifetime
セキュリティー・アソシエーション存続時間 (秒)。

SA Lifesize
セキュリティー・アソシエーション存続サイズ (KB)。

IPCOMP Transforms パネル: このパネルは、IPCOMP 変換に関する情報を提供します。ここには、次のフィールドがあります。

Name IPCOMP 変換の名前。

IPCOMP Algorithm
圧縮アルゴリズムの名前。

IPCOMP Vendor Algorithm
ベンダー・アルゴリズムの名前。

SA Lifetime
セキュリティー・アソシエーション存続時間 (秒)。

SA Lifesize
セキュリティー・アソシエーション存続サイズ (KB)。

Correlation フォルダー: このフォルダーは、IPSec データ管理提案とアクティブ変換の間の相関についての情報を提供します。このフォルダーには、次のパネルがあります。

- Data Management Proposal Correlation (データ管理提案相関)
- AH Correlation (AH 相関)
- ESP Correlation (ESP 相関)
- IPCOMP Correlation (IPCOMP 相関)

Data Management Proposal Correlation パネル: このパネルは、データ管理提案の相関に関する情報を提供します。ここには、次のフィールドがあります。

Action Name
データ管理アクションの名前。

Proposal Name
データ管理提案の名前。

Proposal Order
データ管理提案の順序。

Data Management Action Details
「Data Management Actions」パネルの要約。詳しくは、59ページの『Actions パネル』を参照してください。

Data Management Proposal Details
「Data Management Proposals」パネルの要約。詳しくは、60ページの『Proposals パネル』を参照してください。

AH Correlation パネル: このパネルは、認証ヘッダー (AH) 相関に関する情報を提供します。ここには、次のフィールドがあります。

Proposal Name
データ管理提案の名前。

AH Transform Name
AH 変換の名前。

AH Transform Order
AH 変換の順序。

Data Management Action Details
「Data Management Actions」パネルの要約。詳しくは、59ページの『Actions パネル』を参照してください。

AH Transform Details
「AH Transform」パネルの要約。 60ページの『AH Transforms パネル』 を参照してください。

ESP Correlation パネル: このパネルは、カプセル化セキュリティー・ペイロード (ESP) 相関に関する情報を提供します。ここには、次のフィールドがあります。

Proposal Name
データ管理提案の名前。

ESP Transform Name
ESP 変換の名前。

ESP Transform Order
ESP 変換の順序。

Data Management Action Details
「Data Management Actions」パネルの要約。詳しくは、59ページの『Actions パネル』を参照してください。

ESP Transform Details
「ESP Transform」パネルの要約。 61ページの『ESP Transforms パネル』 を参照してください。

IPCOMP Correlation パネル: このパネルは、IPCOMP 相関に関する情報を提供します。ここには、次のフィールドがあります。

Proposal Name
データ管理提案の名前。

IPCOMP Transform Name
IPCOMP 変換の名前。

IPCOMP Transform Order
IPCOMP 変換の順序。

Data Management Action Details
「Data Management Actions」パネルの要約。詳しくは、59ページの『Actions パネル』を参照してください。

IPCOMP Transform Details
「IPCOMP Transform」パネルの要約。 61ページの『IPCOMP Transforms パネル』を参照してください。

Differential Services Actions パネル: このパネルは、すべての差別化サービス・アクションの定義を表示します。ここには、次のフィールドがあります。

Differential Services Action Name
差別化サービス・アクションの名前。

Permission
アクションの許可値: permit (許可) または deny (拒否)。

Queue Priority
アクションの待ち行列優先順位。

Bandwidth Type
アクションの帯域幅タイプ。

Bandwidth Share
アクションの帯域幅共用。

TOS Mask
type-of-service バイト・マスク。

TOS Match
type-of-service バイト突き合わせ。

Matches
このアクションの一致の数。

RSVP Actions: このパネルは、すべての RSVP アクションの定義を表示します。ここには、次のフィールドがあります。

Name RSVP アクションの名前。

Permission
アクションの許可値: permit (許可) または deny (拒否)。

Max Rate/Flow
最大速度 / フロー (KB)。

Max Token-Bucket/Flow
最大トークン・バケット / フロー。

Max Flow Duration
最大フローの持続時間 (秒)。

Min Delay
最小遅延 (秒)。

Differential Services Action
差別化サービス・アクションの名前。

Differential Services Action Details
「Differential Services Action」パネルの要約。詳しくは、63ページの『Differential Services Actions パネル』を参照してください。

第11章 VPN Monitor Events フォルダー

VPN Monitor Events (イベント) フォルダーは、VPN モニターによって実行されたイベント報告に関する情報を提供します。このフォルダーには、次の従属項目があります。

- Layer-2 Authentication (レイヤー 2 認証) フォルダー
- IPSec Authentication/Encryption (IPSec 認証 / 暗号化) フォルダー

Layer-2 Authentication フォルダー

このフォルダーは、モニターされた装置が実行した レイヤー 2 認証に関する情報を提供します。このフォルダーには、次のパネルがあります。

- Statistics (統計)
- Tunnel Failure Log (トンネル障害ログ)
- Session Failure Log (セッション障害ログ)

Statistics パネル

このパネルは、モニターされた装置が実行した レイヤー 2 認証に関する統計を提供します。ここには、次のフィールドがあります。

Tunnel Successes
活動化されたレイヤー 2 トンネルの数。

Tunnel Failures
認証できなかったので活動化されなかったレイヤー 2 トンネルの数。

Session Successes
活動化されたレイヤー 2 セッションの数。

Session Failures
認証できなかったので活動化されなかったレイヤー 2 セッションの数。

Tunnel Failure Log パネル

このパネルは、認証できなかったのでオープンされなかったレイヤー 2 トンネルに関する情報を提供します。ここには、次のフィールドがあります。

Failure Number
障害の番号。

Host 障害が起きたトンネルのホスト。

IP Address
障害が起きたトンネルの IP アドレス。

Time 障害の時刻。

Session Failure Log パネル

このパネルは、認証できなかったのでオープンされなかったレイヤー 2 セッションに関する情報を提供します。ここには、次のフィールドがあります。

Failure Number
障害の番号。

User ID
障害が起きたトンネルに関連したユーザー ID。

Time 障害の時刻。

IPSec Authentication/Encryption フォルダー

このフォルダーは、モニターされた装置が実行した IPSec 認証および暗号化に関する情報を提供します。このフォルダーには、次のパネルがあります。

- Statistics (統計)
- IPSec Failure Log (IPSec 障害ログ)

Statistics パネル

このパネルは、モニターされた装置が実行した IPSec 認証および暗号化に関する統計を提供します。ここには、次のフィールドがあります。

In Authentications
実行された IPSec インバウンド認証の数。

In Authentication Failures
失敗した IPSec インバウンド認証の数。

In Decryptions
実行された IPSec インバウンド復号の数。

In Decryption Failures
失敗した IPSec インバウンド復号の数。

Out Authentications
実行された IPSec アウトバウンド認証の数。

Out Authentication Failures
失敗した IPSec アウトバウンド認証の数。

Out Encryptions
実行された IPSec アウトバウンド暗号化の数。

Out Encryptions Failures
失敗した IPSec アウトバウンド暗号化の数。

IPSec Failure Log パネル

このパネルは、IPSec 認証および暗号化の障害に関する情報を提供します。ここには、次のフィールドがあります。

Failure Number
障害の番号。

Reason
障害の理由。

Time 障害の時刻。

Tunnel ID
障害のトンネル ID。

SA SPI
障害のセキュリティー・アソシエーション保護インデックス。

Source IP Address
障害のソース IP アドレス。

Destination IP Address
障害のあて先 IP アドレス。

第12章 VPN モニター Operational フォルダー

このフォルダーは、モニター対象装置の動作に関する情報を提供します。このフォルダーには、次の従属項目があります。

- Tunnels (トンネル) フォルダー
- Clients (クライアント) フォルダー
- Policies (ポリシー) フォルダー
- LDAP フォルダー
- Traps (トラップ) フォルダー

Tunnels フォルダー

このフォルダーは、レイヤー 2 履歴テーブルとログ・テーブルのサイズ、アクティブ・レイヤー 2 トンネル、アクティブ IPSec 制御トンネル、およびアクティブ IPSec ユーザー・トンネルの表示および動作機能を提供します。このフォルダーには、次のパネルがあります。

- Table Size (テーブル・サイズ)
- Inactivate Layer-2 Tunnels (レイヤー 2 トンネルの非活動化)
- Inactivate IPSec Control Tunnels (IPSec 制御トンネルの非活動化)
- Inactivate IPSec User Tunnels (IPSec ユーザー・トンネルの非活動化)

Table Size パネル

このパネルは、レイヤー 2 履歴テーブルおよびログ・テーブルのサイズに関する情報を提供します。ここには、次のフィールドがあります。

Layer-2 History Tables
保持する必要がある、以前のレイヤー 2 トンネルおよびセッションのエントリー数。許可ユーザーは、この値を「Table Size」パネルから変更できます。

Layer-2 Authentication Failure Tables
レイヤー 2 認証障害テーブル内に保持するエントリー数。許可ユーザーは、この値を「Table Size」パネルから変更できます。

Inactivate Layer-2 Tunnels パネル

このパネルでは、許可ユーザーがレイヤー 2 トンネルを非活動化できます。ここには、次のフィールドがあります。

Active Layer-2 Tunnels Details
「Active Layer-2 Tunnels」(アクティブ・レイヤー 2 トンネル) パネルの要約。

Status 単一トンネルの破棄を起動します。許可ユーザーは、この値を「Inactivate Layer-2 Tunnels」パネルから変更できます。

Destroy All Tunnels
すべてのトンネルの破棄を起動します。許可ユーザーは、この値を「Inactivate Layer-2 Tunnels」パネルから変更できます。

Inactivate IPSec Control Tunnels パネル

このパネルでは、許可ユーザーが IPSec 制御トンネルを非活動化できます。ここには、次のフィールドがあります。

Active IPSec Control Tunnel Details
「Active IPSec Control Tunnels」(アクティブ IPSec 制御トンネル) パネルの要約。

Status 単一トンネルの破棄を起動します。許可ユーザーは、この値を「Inactivate IPSec Control Tunnels」パネルから変更できます。

Destroy All Tunnels
すべてのトンネルの破棄を起動します。許可ユーザーは、この値を「Inactivate IPSec Control Tunnels」パネルから変更できます。

Inactivate IPSec User Tunnels パネル

このパネルでは、許可ユーザーが IPSec ユーザー・トンネルを非活動化できます。ここには、次のフィールドがあります。

Active IPSec user Tunnel Details
「Active IPSec user Tunnels」(アクティブ IPSec ユーザー・トンネル) パネルの要約。

Status 単一トンネルの破棄を起動します。許可ユーザーは、この値を「Inactivate IPSec user Tunnels」パネルから変更できます。

Destroy All Tunnels
すべてのトンネルの破棄を起動します。許可ユーザーは、この値を「Inactivate IPSec user Tunnels」パネルから変更できます。

Clients フォルダー

このフォルダーは、レイヤー 2 セッションの表示および制御機能を提供します。このフォルダーには、次のパネルがあります。

- Inactivate Layer-2 Sessions (レイヤー 2 セッションの非活動化)

Inactivate Layer-2 sessions パネル

このパネルでは、許可ユーザーがレイヤー 2 セッションを非活動化できます。ここには、次のフィールドがあります。

Active Layer-2 Sessions Details
「Active Layer-2 Sessions」(アクティブ・レイヤー 2 セッション) パネルの要約。

Status 単一セッションの破棄を起動します。許可ユーザーは、この値を「Inactivate Layer-2 Sessions」パネルから変更できます。

Destroy All sessions
すべてのセッションの破棄を起動します。許可ユーザーは、この値を「Inactivate Layer-2 Sessions」パネルから変更できます。

Policies フォルダー

このフォルダーは、VPN 装置のポリシーの表示および制御機能を提供します。このフォルダーには、次のパネルがあります。

- Enable/Disable Policies (ポリシーの使用可能 / 使用不可)
- Reload Device Policies (装置のポリシーの再ロード)

Enable/Disable Policies パネル

このパネルでは、ユーザーは選択した装置のポリシーを使用可能または使用不可にできます。ここには、次のフィールドがあります。

Policy Details
「Policies」(ポリシー) パネルの要約。

Status ポリシーの使用可能または使用不可を起動します。許可ユーザーは、この値をこのパネルから変更できます。

Reload Device Policies パネル

このパネルでは、ユーザーはモニターされる装置が使用するポリシーを再ロードできます。ここには、次のフィールドがあります。

Administrative Definition Details
管理 Lightweight Directory Access Protocol (LDAP) 定義の要約。詳しくは、72ページの『Administrative Parameters パネル』を参照してください。

Operational Definition Details
動作 LDAP 定義の要約。詳しくは、72ページの『Operational Parameters パネル』を参照してください。

Reload Policies
ポリシーの再ロードを起動します。許可ユーザーは、このパネルからポリシーを再ロードできます。

LDAP フォルダー

このフォルダーは、Lightweight Directory Access Protocol (LDAP) パラメーターの表示および制御機能を提供します。このフォルダーには、次のパネルがあります。

- Operational Parameters (動作パラメーター)
- Administrative Parameters (管理パラメーター)

Operational Parameters パネル

このパネルは、LDAP 動作パラメーターに関する情報を提供します。ここには、次のフィールドがあります。

Status 定義の状況: enable (使用可能) または disable (使用不可)。

Primary LDAP Server IP Address
1 次 LDAP サーバーの IP アドレス。

Secondary LDAP Server IP Address
2 次 LDAP サーバーの IP アドレス。

LDAP Server Level
LDAP サーバーのレベル。

Policy Base Name
装置のポリシー・ベース・オブジェクトの名前。

Port LDAP サーバーが使用するポート番号。

Timeout
LDAP サーバーが使用するタイムアウト値。

Retry Interval
LDAP サーバーが使用する再試行間隔。

User ID
LDAP サーバーのユーザー ID。

Administrative Parameters パネル

このパネルは、LDAP パラメーターの制御機能を提供します。「Operational Parameters」(動作パラメーター) パネルと同じフィールドが入っていますが、このパネルでは、許可ユーザーがパラメーターの値を変更できます。

Traps フォルダー

このフォルダーは、VPN トラップの表示および制御機能を提供します。このフォルダーには、次のパネルがあります。

- Layer-2 Trap Control (レイヤー 2 トラップ制御)
- IPSec Trap Control (IPSec トラップ制御)

Layer-2 Trap Control パネル

このパネルは、選択された装置のレイヤー 2 トラップに関する情報と、その制御機能を提供します。許可ユーザーは、このパネル内のすべてのフィールドの値を変更できます。「Layer-2 Trap Control (レイヤー 2 トラップ制御)」パネルには、次のフィールドがあります。

Tunnel Start Traps
トンネル開始トラップ処理の状況: enable (使用可能) または disable (使用不可)。

Tunnel Stop Traps
トンネル停止トラップ処理の状況: enable (使用可能) または disable (使用不可)。

Tunnel Authentication Failure Traps
トンネル認証障害トラップ処理の状況: enable (使用可能) または disable (使用不可)。

User Authentication Failure Traps
ユーザー認証障害トラップ処理の状況: enable (使用可能) または disable (使用不可)。

IPSec Trap Control パネル

このパネルは、選択された装置の IPSec トラップに関する情報と、その制御機能を提供します。許可ユーザーは、このパネル内のすべてのフィールドの値を変更できます。「IPSec Trap Control (IPSec トラップ制御)」パネルには、次のフィールドがあります。

Control Tunnel Start Traps
制御トンネル開始トラップ処理の状況: enable (使用可能) または disable (使用不可)。

Control Tunnel Stop Traps
制御トンネル停止トラップ処理の状況: enable (使用可能) または disable (使用不可)。

User-Data Tunnel Start Traps
ユーザー・データ・トンネル開始トラップ処理の状況: enable (使用可能) または disable (使用不可)。

User-Data Tunnel Stop Traps
ユーザー・データ・トンネル停止トラップ処理の状況: enable (使用可能) または disable (使用不可)。

Authentication Failure Traps
認証障害トラップ処理の状況: enable (使用可能) または disable (使用不可)。

Decryption Failure Traps
復号障害トラップ処理の状況: enable (使用可能) または disable (使用不可)。

第13章 VPN モニター Tests フォルダー

このフォルダーでは、ユーザーはホストとの間のポリシー、接続性、および応答時間をテストできます。このフォルダーには、次の従属項目が含まれています。

- Policy Test (ポリシー・テスト) パネル
- Layer-2 Tests (レイヤー 2 テスト) フォルダー
- Remote Ping (リモート Ping) パネル

Policy Test パネル

このパネルでは、ポリシー・テストを実施し、その結果を検討できます。テストを開始するには、ソース・アドレスとあて先アドレス、ソース・ポートとあて先ポート、使用するプロトコル、および要求されるサービスのタイプを指定します。テストが完了すると、選択されたポリシーとアクションが表示されます。「Policy Test (ポリシー・テスト)」パネルには、次のフィールドがあります。

Test Index
テストのインデックス。

Result テストの結果。

Status テストのエントリーの状況。

Source IP Address
テストに使用するソース IP アドレス。この値は、ここで変更できます。

Source Port
テストに使用するソース・ポート。この値は、ここで変更できます。

Destination IP Address
テストに使用するあて先 IP アドレス。この値は、ここで変更できます。

Destination Port
テストに使用するあて先ポート。この値は、ここで変更できます。

Protocol
テストに使用するプロトコル。この値は、ここで変更できます。

TOS Byte
テストに使用する type-of-service バイト。この値は、ここで変更できます。

Key Management Policy
選択されたキー管理ポリシー。

Key Management Action
選択されたキー管理アクション。

Data Management Policy
選択されたデータ管理ポリシー。

Data Management Action
選択されたデータ管理アクション。

Diff Services Policy
選択された差別化サービス・ポリシー。

Diff Services Action
選択された差別化サービス・アクション。

RSVP Policy
選択された RSVP ポリシー。

RSVP Action
選択された RSVP アクション。

Layer-2 Tests フォルダー

このフォルダーでは、レイヤー 2 トンネルの接続性と応答時間をテストできます。このフォルダーには、次のパネルがあります。

- Layer-2 Connection Test (レイヤー 2 接続テスト)
- Layer-2 Response Time Test (レイヤー 2 応答時間テスト)

Layer-2 Connection Test パネル

このパネルでは、ホストへの潜在的なレイヤー 2 接続性をテストできます。テストを開始するには、潜在的ホストの名前を選択します。テストが完了すると、接続の可用性が表示されます。このパネルには、次のフィールドがあります。

Test Index
テストのインデックス。

Host 接続性をテストするホスト。この値は、ここで変更できます。

Result テストの結果。

Tunnel Type
テストに使用するトンネル・タイプ。

Layer-2 Response Time Test パネル

このパネルでは、アクティブ・ホストの応答時間をテストできます。テストを開始するには、アクティブ・ホストの名前を選択します。テストが完了すると、選択されたホストへのパケットの往復時間が表示されます。このパネルには、次のフィールドがあります。

Test Index
テストのインデックス。

Host 接続性をテストするホスト。この値は、ここで変更できます。

Result テストの結果。

Round Trip Time
テスト・パケットの往復時間。

Remote Ping パネル

このパネルでは、現行の VPN 装置から別の装置への応答時間をテストできます。 Ping を開始するには、テストに使用するリモート・ホストの IP アドレス、パケット・サイズ、タイムアウト値を指定します。テストが完了すると、そのホストへのパケットの往復時間が表示されます。このパネルには、次のフィールドがあります。

IP Address
Ping する IP アドレス。この値は、ここで変更できます。

Packet Size
Ping に使用するパケット・サイズ。この値は、ここで変更できます。

Timeout Value
Ping に使用するタイムアウト値。この値は、ここで変更できます。

Result Ping の結果。

Ping Time
テストの往復時間。

付録. 特記事項

本書において、日本では発表されていないIBM製品（機械およびプログラム）、プログラミングまたはサービスについて言及または説明する場合があります。しかし、このことは、弊社がこのようなIBM製品、プログラミングまたはサービスを、日本で発表する意図があることを必ずしも示すものではありません。本書で、 IBMライセンス・プログラムまたは他のIBM製品に言及している部分があっても、このことは当該プログラムまたは製品のみが使用可能であることを意味するものではありません。これらのプログラムまたは製品に代えて、IBMの知的所有権を侵害することのない機能的に同等な他社のプログラム、製品またはサービスを使用することができます。ただし、IBMによって明示的に指定されたものを除き、これらのプログラムまたは製品に関連する稼働の評価および検証はお客様の責任で行っていただきます。

IBMおよび他社は、本書で説明する主題に関する特許権（特許出願を含む）商標権、または著作権を所有している場合があります。本書は、これらの特許権、商標権、および著作権について、本書で明示されている場合を除き、実施権、使用権等を許諾することを意味するものではありません。実施権、使用権等の許諾については、下記の宛先に、書面にてご照会ください。

〒106-0032 東京都港区六本木3丁目2-31
AP事業所
IBM World Trade Asia Corporation
Intellectual Property Law & Licensing

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

本書において IBM 以外の Web サイトに言及していることがありますが、便宜上記載しただけであり、決してそれらの Web サイトを推奨するものではありません。それらの Web サイトにある資料は、この IBM プロダクトの資料の一部ではなく、それらの Web サイトは、お客様の自己責任のもとでご使用ください。

商標

次の用語は、IBM Corporation の米国およびその他の国における商標です。

DB2
Nways
IBM
DB2 Universal Database

Java および Java ベースの商標とロゴは、Sun Microsystems, Inc. の商標または登録商標です。

Microsoft、Windows、Windows NT、および Windows 95 と Windows 98 のロゴは、Microsoft Corporation の商標または登録商標です。

Pentium は、Intel Corporation の登録商標です。

Netfinity は、Tivoli Systems, Inc. の商標です。

UNIX は、X/Open Company Limited から独占的にライセンスされる登録商標です。

Freelance Graphics は、Lotus Development Corporation の商標です。

他の会社名、製品名、およびサービス名は、それぞれ各社の商標または登録商標です。

Printed in Japan

Nways Management Web サイト:

http://www.networking.ibm.com/netmgt

GA88-7014-00

日本アイ・ビー・エム株式会社
〒106-8711　東京都港区六本木3-2-12