Nways Manager

Nways VPN Manager Benutzerhandbuch

GA12-4795-00

Nways Manager

Nways VPN Manager Benutzerhandbuch

GA12-4795-00

Anmerkung

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts
sollten die allgemeinen Informationen unter Anhang A, „Bemerkungen“ auf Seite 79 lesen.

Diese Veröffentlichung ist eine Übersetzung des Handbuchs
Nways Manager - VPN Manager User's Guide
IBM Form GA27-4233-00,
herausgegeben von International Business Machines Corporation, USA

Informationen, die nur für bestimmte Länder Gültigkeit haben und für Deutschland, Österreich und die Schweiz nicht zutreffen, wurden in dieser Veröffentlichung im Originaltext übernommen.

Möglicherweise sind nicht alle in dieser Übersetzung aufgeführten Produkte in Deutschland angekündigt und verfügbar; vor Entscheidungen empfiehlt sich der Kontakt mit der zuständigen IBM Geschäftsstelle.

Änderung des Textes bleibt vorbehalten.

Herausgegeben von:
SW NLS Center
Kst. 2877
Juli 1999

Inhaltsverzeichnis

Einführung

Dieses Kapitel enthält eine Kurzbeschreibung von VPN Manager, eine Auflistung der unterstützten IBM Hardwarekomponenten sowie Angaben zur für die Verwendung von VPN Manager erforderlichen Hard- und Software,.

Informationen zu VPN Manager

Nways VPN Manager bietet Funktionen für Ereignisberichte, zum Starten von Anwendungen, zur Überwachung, zur Fehlerbehebung und zur Betriebssteuerung für die IBM Implementierung von virtuellen persönlichen Netzwerken (VPN).

Hardwareunterstützung

Version 2.0 von Nways VPN Manager bietet Funktionen zur Überwachung und Betriebssteuerung für das in den folgenden Einheiten implementierte VPN-Leistungsspektrum:

- IBM 2210 Nways Multiprotocol Router
- IBM 2212 Access Utility
- IBM 2216 Nways Multiaccess Connector
- IBM Network Utility

Hardware- und Softwarevoraussetzungen

Nways VPN Manager erfordert Nways Element Manager Version 2.0 für eine der folgenden Plattformen:

- AIX
- HP-UX
- Windows NT

Da die Mindesthardwarevoraussetzungen für Nways Element Manager jene für Nways VPN Manager überschreiten, gibt es keine zusätzlichen Hardwarevoraussetzungen.

Einführung in VPNs

Ein *virtuelles privates Netzwerk* (VPN) ermöglicht es Endbenutzern, Informationen von einem Intranet über ein öffentliches IP-Netzwerk wie das Internet sicher zu übertragen. Ein VPN kann sich aus Layer-2-Tunneln, IPSec-Tunneln und Policies zusammensetzen. Die Layer-2-Tunnel stellen das VPN-Leistungsspektrum für sich einwählende ferne Benutzer bereit. Die IPSec-Tunnel stellen das VPN-Leistungsspektrum für IP-Benutzer bereit. Die Policies ermöglichen die Zugriffssteuerung der Ressourcen.

Dieses Kapitel enthält eine Übersicht über folgende Themen:

- Layer-2-Tunnelung
- IPSec-Tunnelung
- Policies

Layer-2-Tunnelung

Mit Layer-2-Tunnelungsprotokollen kann privater PPP-Datenverkehr (PPP - Point-to-Point Protocol) sicher über ein öffentliches IP-Netzwerk transportiert werden. Es gibt drei Arten von Layer-2-Tunnelungsprotokollen, die zwei Netzwerkmodelle einsetzen. Die drei Arten des Layer-2-Tunnelungsprotokolls sind das Layer-2 Tunneling Protocol (L2TP), das Layer-2 Forwarding Protocol (L2F) und das Point-to-Point Tunneling Protocol (PPTP). Die zwei Netzwerkmodelle sind „compulsory“ Tunnelung und „voluntary“ Tunnelung.

Terminologie

Ein *Netzwerkzugangs-Server* (NAS - Network Access Server) ist eine Einheit, die an ein Wählnetz wie ein *öffentliches Telefonwählnetz* (PSTN - Public Switched Telephone Network) oder ein *dienstintegrierendes digitales Fernmeldenetz* (ISDN - Integrated Services Digital Network) angeschlossen ist und ein PPP-Endsystem enthält. Ein Netzwerkzugangs-Server, der einen L2TP-Tunnel einleiten kann, wird als *L2TP-Zugangskonzentrator* (LAC - L2TP Access Concentrator) bezeichnet. Der Netzwerkzugangs-Server ist der Initiator der ankommenden Anrufe und der Empfänger der abgehenden Anrufe. Ein Gateway ist eine Einheit, die zur PPP-Beendigung in der Lage ist und die Server-Seite der Datenfernverarbeitung handhabt. Ein Gateway wird auch als *L2TP-Netzwerk-Server* (LNS) bezeichnet. Der Gateway ist der Initiator der abgehenden Anrufe und der Empfänger der ankommenden Anrufe.

"Compulsory" Tunnelung

Durch „compulsory“ Tunnelung können sich einwählende Clients, für die keine Tunnelungssoftware aktiviert ist, eine PPP-Sitzung starten, die vom Netzwerkzugangs-Server im Tunnelungsverfahren an das Firmennetzwerk übertragen wird. In diesem Modell besteht die PPP-Sitzung zwischen dem Client und dem Gateway, und der Tunnel besteht zwischen dem Netzwerkzugangs-Server und dem Gateway.

"Voluntary" Tunnelung

Bei „voluntary“ Tunnelung andererseits müssen die sich einwählenden Clients zur Übertragung von Daten im Tunnelungsverfahren fähig sein. In diesem Modell wählt sich der Client anfänglich in seinen Servicegeber ein, um Internet-Zugriff zu erhalten. Nach der Herstellung der Verbindung zum Servicegeber erstellt der Client einen Layer-2-Tunnel zum Gateway und dann über den neu erstellten Tunnel eine Endpunkt-zu-Endpunkt-PPP-Sitzung. In diesem Modell bestehen die PPP-Sitzung und der Tunnel zwischen dem Client und dem Gateway.

Layer-2 Tunneling Protocol

Layer-2-Tunnelung setzt die folgenden Protokolle ein:

L2TP Das Layer-2 Tunneling Protocol ist ein IETF-Standardprotokoll (IETF - Internet Engineering Task Force), das aus dem Layer-2 Forwarding Protocol (L2F) und dem Point-to-Point Tunneling Protocol (PPTP) entstand. L2TP verwendet den bekannten UDP-Anschluß 1701 für den ersten Handshake der Tunnelsteuerungsnachrichten und kann verfügbare UDP-Quellenanschlüsse auf beiden Seiten der Verbindung auswählen. UDP wird auch als Pakettransport für im Tunnelungsverfahren übertragene PPP-Pakete verwendet. L2TP verwendet beide Netzwerkmodelle, d. h. „compulsory“ Tunnelung und „voluntary“ Tunnelung.

L2F Das Layer-2 Forwarding Protocol ist ein nicht auf Standards basierendes Layer-2-Tunnelungsprotokoll, das ursprünglich von Cisco Systems implementiert wurde. Es verwendet den bekannten UDP-Anschluß 1701 (fixiert) für die Übertragung von Tunnel- und Rufsteuerungsnachrichten sowie für den Transport von im Tunnelungsverfahren übertragenen PPP-Paketen vom Netzwerkzugangs-Server zum Gateway. L2F verwendet das Modell der „compulsory“ Tunnelung.

PPTP Das Point-to-Point Tunneling Protocol ist ein weiteres nicht auf Standards basierendes Layer-2-Tunnelungsprotokoll, das ursprünglich von Microsoft auf den Windows 95- und Windows NT-Plattformen implementiert wurde. PPTP verwendet TCP zum Öffnen der Tunnel- sowie Sitzungssteuerungsstrukturen. Nach der Herstellung der Sitzung werden PPP-Pakete unter Verwendung von GRE (Generic Routing Encapsulation) im Tunnelungsverfahren übertragen. PPTP verwendet das Netzwerkmodell der „voluntary“ Tunnelung.

Leistungsspektrum der Layer-2-Tunnelung

Die Layer-2-Tunnelungsprotokolle können direkt oder indirekt Authentifizierung, Verschlüsselung und Komprimierung bereitstellen.

Die Layer-2-Tunnelungsprotokolle können direkt Tunnelauthentifizierung und indirekt Benutzerauthentifizierung bereitstellen. Tunnelauthentifizierung wird zwischen dem Netzwerkzugangs-Server und dem Gateway ausgeführt. Benutzerauthentifizierung wird durch das zugrundeliegende Point-to-Point Tunneling Protocol ausgeführt.

Die Layer-2-Tunnelungsprotokolle können indirekt Datenverschlüsselung bereitstellen. Alle Layer-2-Tunnelungsprotokolle können auf der Anwendungsschicht verschlüsselte Daten transportieren. L2TP kann mit IPSec verwendet werden, das Datenverschlüsselung ausführen kann. PPTP kann die MPPE-Einrichtung (MPPE - Microsoft Point-to-Point Encryption) verwenden.

Die Layer-2-Tunnelungsprotokolle können indirekt Datenkomprimierung bereitstellen. Sie erzielen dies durch die Verwendung des zugrundeliegenden Point-to-Point Protocol, das Daten komprimieren kann.

IPSec-Tunnelung

IPSec ist ein IETF-Standard (IETF - Internet Engineering Task Force), der einen Tunnelmechanismus zum sicheren Transportieren von IP-Datenverkehr über ein öffentliches IP-Netzwerk definiert. IPSec-Tunnel werden mit Hilfe eines Tunnelpaars implementiert. Es gibt einen IPSec-Schlüsselmanagementtunnel und einen IPSec-Datenmanagementtunnel. Ein IPSec-Schlüsselmanagementtunnel wird häufig als ein Phase-1-
Tunnel oder als ein IKE-Tunnel (IKE - Internet Key Exchange) bezeichnet und ist ein Steuertunnel für mindestens einen anschließenden IPSec-Phase-2-Benutzerdatentunnel. IPSec-Tunnel werden in der Regel nach dem Endpunkt-zu-Endpunkt- oder Gateway-zu-Gateway-Netzwerkmodell implementiert.

Terminologie

Authentifizierung bedeutet die Kenntnis, daß die empfangenen Daten mit den gesendeten Daten übereinstimmen und daß der angebliche Sender auch wirklich der tatsächliche Sender ist. Die IPSec-Authentifizierungsmethode kann ein manuell eingegebener vorab bekannter gemeinsamer Schlüssel (Pre-Shared Key) oder eine digitale Unterschrift (Digital Signature) sein. Abgesehen von der Authentifizierung garantieren digitale Unterschriften, daß die Nachricht eindeutig dem Sender zugeordnet wird und vom Empfänger nicht geändert werden kann. Im IPSec-Tunnelauthentifizierungsschema werden in der Regel MD5 (Message Digest 5) mit dem 128-Bit-Hash-Verfahren und SHA (Secure Hash Algorithm) mit dem 160-Bit-Hash-Verfahren verwendet.

Integrität bedeutet die Sicherstellung, daß Daten so von der Quelle zur Zieladresse übertragen werden, daß jegliche Änderung festgestellt wird. Im IPSec-Integritätsschema werden in der Regel HMAC-MD5 (Hashed Message Authentication Code Message Digest 5) mit dem 2x128-Bit-Hash-Verfahren und HMAC-SHA (Hashed Message Authentication Code Message Secure Hash Algorithm) mit dem 2x160-Bit-Hash-Verfahren verwendet.

Vertraulichkeit bedeutet Datenübertragung, die so gestaltet ist, daß die erwünschten Empfänger wissen, was gesendet wurde, unerwünschte Teilnehmer jedoch nicht ermitteln können, was gesendet wurde. IPSec erzielt Vertraulichkeit mit Hilfe von Kapselung und Verschlüsselung. Das ursprüngliche IP-Datenpaket wird in einem IPSec-Datenpaket gekapselt. Der ursprüngliche IP-Kennsatz und die ursprünglichen IP-Nutzinformationen werden im Tunnelmodus, der gewöhnlich von Gateways verwendet wird, gekapselt.

Im Gegensatz dazu werden im Transportmodus, der gewöhnlich von Hosts verwendet wird, nur die ursprünglichen Nutzinformationen gekapselt. Im IPSec-Verschlüsselungsschema werden in der Regel DES (Data Encryption Standard) mit 56-Bit-Verschlüsselung, DES-3 (Triple Data Encryption Standard) mit 3x56-Bit-Verschlüsselung und CMDF (Commercial Data Masking Facility) mit 40-Bit-Verschlüsselung verwendet.

Eine *Sicherheitszuordnung* (SA - Security Association) ist eine Beziehung zwischen gegebenen Netzwerkverbindungen, die einen Satz gemeinsam benutzter Sicherheitsinformationen bilden. Sicherheitszuordnungen werden basierend auf geheimen Schlüsseln, Verschlüsselungsalgorithmen, Authentifizierungsalgorithmen und Kapselungsmodi vereinbart. Das Diffie-Hellman-Schlüsselvereinbarungsprotokoll (Gruppe 1: 768-Bit-Verschlüsselung, Gruppe 2: 1024-Bit-Verschlüsselung) wird von IKE verwendet, um einen geheimen Schlüssel für gemeinsame Benutzung zu generieren, d. h. einen Schlüssel zwischen den beiden IPSec-Definitionseinheiten. Beachten Sie, daß IKE früher als ISAKMP/Oakley (Internet Security Association and Key Management Protocol/Oakley Protocol) bekannt war. Die Dauer einer Sicherheitszuordnung wird durch die Lebensdauer (Dauer in Sekunden) bzw. die Datenmenge (Dauer in Kilobyte) angegeben.

Endpunkt-zu-Endpunkt-Tunnelung

Durch Endpunkt-zu-Endpunkt-IPSec-Tunnelung kann ein IP-Host an einem Ende des Netzwerks Daten sicher zu einem IP-Host am anderen Ende des Netzwerks übertragen. Dieses Modell ähnelt einem spezifischen Peer-zu-Peer-Modell, bei dem beide IP-Hosts IPSec-fähig sein müssen. Der IPSec-Tunnel setzt sich aus einem Schlüsselmanagementtunnel und einem Datenmanagementtunnel zwischen den beiden IP-Hosts zusammen.

Gateway-zu-Gateway-Tunnelung

Durch Gateway-zu-Gateway-IPSec-Tunnelung kann mindestens ein IP-Host an einem Ende des Netzwerks Daten sicher zu mindestens einem IP-Host am anderen Ende des Netzwerks übertragen. Dieses Modell ähnelt einem Any-to-Any-Modell, in dem die Gateways IPSec-fähig sein müssen, die IP-Hosts jedoch nicht. Der IPSec-Tunnel setzt sich aus einem Schlüsselmanagementtunnel und mindestens einem Datenmanagementtunnel zwischen den beiden Gateways zusammen. Die Gateways werden über ihre allgemein zugängliche Schnittstelle (Public Interface) verbunden und schützen mindestens eine private Schnittstelle hinter ihnen. Eine private Schnittstelle kann ein IP-Teilnetz-
werk, ein Bereich von IP-Adressen oder eine einzelne IP-Adresse sein.

Schlüsselmanagement

Ein IPSec-Schlüsselmanagementtunnel wird häufig als IKE-Tunnel (IKE - Internet Key Exchange) oder als IPSec-Phase-1-Tunnel bezeichnet und ist ein Steuertunnel für mindestens einen anschließenden IPSec-Phase-2-Benutzerdatentunnel. Der IPSec-Schlüsselmanagementtunnel wird im Hauptmodus vereinbart, bei dem sechs Nachrichten ausgetauscht werden, oder im Aggressivmodus, bei dem drei Nachrichten ausgetauscht werden.

Die Vereinbarung zieht die Authentifizierung der Definitionseinheiten, das Festlegen eines geheimen Schlüssels für gemeinsame Benutzung (Shared Secret) und das Festlegen von Parametern für die Sicherheitszuordnung nach sich. Nach dem erfolgreichen Abschluß der Vereinbarung verwendet der IPSec-Schlüsselmanagementtunnel eine einzelne bidirektionale Sicherheitszuordnung zur Kommunikation. Während der Lebensdauer eines gegebenen IPSec-Schlüsselmanagementtunnels kann die Sicherheitszuordnung ablaufen und eine neue erstellt werden.

Datenmanagement

Ein IPSec-Datenmanagementtunnel wird häufig als IPSec-Phase-2-Benutzerdatentunnel oder IPSec-Tunnel bezeichnet und wird zum sicheren Transportieren von IP-Daten verwendet. Der IPSec-Datenmanagementtunnel wird im Schnellmodus vereinbart, bei dem drei Nachrichten ausgetauscht werden. Die Vereinbarung zieht den Austausch der Identitäten, die Entscheidung, ob das Verhindern von Wiederholungen durchgesetzt werden soll oder nicht, das Generieren eines Schlüssels bei erforderlicher absoluter vorwärtsgerichteter Sicherheit, die Einigung hinsichtlich der zukünftigen Handhabung des Nichtfragmentierens von Bit und das Festlegen von Parametern für die Sicherheitszuordnung(en) nach sich. Die Sicherheitsparameter können aus AH- (AH - Authentication Header) und/oder ESP-Verarbeitungsattributen (ESP - Encapsulating Security Payload) bestehen. Paketintegrität und Datenursprungsauthentifizierung werden sowohl von AH als auch von ESP bereitgestellt, während die Verschlüsselung nur von ESP bereitgestellt wird. Die IPSec-Datenmanagementtunnel verwenden mindestens eine ankommende Sicherheitszuordnung und mindestens eine abgehende Sicherheitszuordnung. Während der Lebensdauer eines gegebenen IPSec-Datenmanagementtunnels können die Sicherheitszuordnungen ablaufen und neue erstellt werden.

Während dieser Umschaltungsperiode gibt es für jede ursprünglich ankommende Sicherheitszuordnung zwei Sicherheitszuordnungen (eine mit dem Status CURRENT und eine mit dem Status EXPIRING).

Leistungsspektrum der IPSec-Tunnelung

IPSec-Tunnelung kann Authentifizierung, Verschlüsselung und Integrität direkt bereitstellen.

Authentifizierung kann auf Tunnelbasis und wahlfrei auf Paketbasis ausgeführt werden. Tunnelauthentifizierung wird durch die IKE-Peers mit Hilfe eines vorab bekannten gemeinsamen Schlüssels (Pre-Shared Key) oder einer digitalen Unterschrift (Digital Signature) ausgeführt.

Paketauthentifizierung kann durch AH- oder ESP-Verarbeitung mit Hilfe des Algorithmus HMAC-MD5 oder HMAC-SHA erzielt werden. Verschlüsselung wird wahlfrei auf Paketbasis durch ESP-Verarbeitung ausgeführt. Paketverschlüsselung verwendet den Algorithmus DES, DES-3 oder CMDF. Integrität wird wahlfrei auf Paketbasis ausgeführt. Integrität kann durch AH- oder ESP-Verarbeitung erzielt werden und verwendet den Algorithmus HMAC-MD5 oder HMAC-SHA.

Policies

Eine Policy besteht aus einem Profil und einer Aktion. Das Profil definiert eine Gruppe von Attributen für die Quelle und die Zieladresse einer Verbindung.

Die Aktion ist tatsächlich eine Gruppe von Aktionen oder Sub-Policies, die für IPSec-Schlüsselmanagement, IPSec-Datenmanagement, serviceabhängige Policies und Aktionen sowie RSVP (Resource Preservation Protocol - Ressourcenreservierungsprotokoll) verwendet wird. Beim Herstellen einer Verbindung werden die definierten Policy-Profile nach einer Übereinstimmung durchsucht.

Wenn eine Profilübereinstimmung gefunden wird, werden Aktionsangebote ausgetauscht. Wird die Angebotsphase erfolgreich beendet, wird die Verbindung hergestellt und für die definierte Policy eine aktuelle Instanz erstellt. Aus einer einzelnen definierten Policy können mehrere Policy-Instanzen erstellt werden.

Beziehungen der Policy-Komponenten

Eine VPN-Policy muß eine Policy-Bedingung enthalten, die aus einer Gültigkeitsperiode und einem Datenverkehrsprofil sowie mindestens einer Policy-Aktion besteht. Die Definition der Komponente „Gültigkeitsperiode“ kann in mehreren Policies verwendet werden, da sie keine einheitenspezifischen Informationen enthält. Die Definition der Komponente „Datenverkehrsprofil“ ist für die Policy eindeutig, da sie einheitenspezifische Informationen zur IP-Adresse enthält. Die Definitionen der Komponenten „Schlüsselmanagementaktion“ und „Schlüsselmanagementangebot“ der IPSec-Aktion können in mehreren Policies verwendet werden, da sie keine einheitenspezifischen Informationen enthalten. Die Definition der Komponente „Datenmanagementaktion“ der IPSec-Aktion ist für die Policy eindeutig, da sie einheitenspezifische Informationen zur IP-Adresse enthält.

Die Definitionen der Komponenten „Datenmanagementaktion“, „Datenmanagementangebot“, „AH-Umsetzung“ (AH - Authentication Header) und „ESP-Umsetzung“ (ESP - Encapsulated Security Payload) der IPSec-Aktion können in mehreren Policies verwendet werden, da sie keine einheitenspezifischen Informationen enthalten. Die Definitionen der Komponenten „Serviceabhängige Maßnahme“ und „RSVP-Aktion“ können in mehreren Policies verwendet werden, da sie keine einheitenspezifischen Informationen enthalten. Die folgende Tabelle illustriert die Beziehungen der Komponenten einer VPN-Policy.

Policy-Komponente	Beziehung
Policy-Bedingungen (Policy Conditions)	Die Policy muß eine Gültigkeitsperiode und ein Datenverkehrsprofil enthalten.
Gültigkeitsperiode (Validity Period)	Kann von mehreren Policies gemeinsam benutzt werden.
Datenverkehrsprofil (Traffic Profile)	Eindeutig für die Policy mit Ausnahme des Gesamtdatenverkehrsprofils
Policy-Aktionen (Policy Actions)	Die Policy muß mindestens eine Aktion enthalten.
IPSec-Aktion (IPSec Action)	Muß eine Schlüsselmanagement- und eine Datenverwaltungsaktion enthalten.
Schlüsselmanagementaktion (Key Management (KM) Action)	Kann von mehreren Policies gemeinsam benutzt werden.
Schlüsselmanagementangebot (Key Management (KM) Proposal)	Kann von mehreren Schlüsselmanagementaktionen gemeinsam benutzt werden.
Datenmanagementaktion (Data Management (DM) Action)	Eindeutig für die Policy (enthält IP-Adreßinformationen)
Datenmanagementangebot (Data Management (DM) Proposal)	Kann von mehreren Datenmanagementaktionen gemeinsam benutzt werden.
AH-Umsetzung (AH Transform)	Kann von mehreren Datenmanagementangeboten gemeinsam benutzt werden.
ESP-Umsetzung (ESP Transform)	Kann von mehreren Datenmanagementangeboten gemeinsam benutzt werden.
Serviceabhängige Maßnahme (Differential Services Action)	Kann von mehreren Policies gemeinsam benutzt werden.
RSVP-Aktion (RSVP Action)	Kann von mehreren Policies gemeinsam benutzt werden.

LDAP

LDAP (Light Weight Directory Access Protocol) ist ein Internet-Verzeichnisstandard, der aus DAP (X.500 Directory Access Protocol) entstand und Client-Einheiten offenen Zugriff auf Verzeichnis-Server im Intranet/Internet verschaffen kann. Das Protokoll stellt diese Funktion durch das Übergeben von textgestützten Austauschvorgängen auf Grundlage eines Schemas zwischen einem Client und einem Server über TCP/IP bereit. Vom Client und Server können ein oder mehrere Schemata unterstützt werden, wobei jedes Schema zum Definieren einer Gruppe verwandter Objekte verwendet wird.

Die DEN-Initiative (DEN - Directory-Enabled Networking) hat LDAP in ihrer Spezifikation als den Mechanismus identifiziert, mit dem auf Informationen zugegriffen wird. DEN begann 1997 und wird momentan von einer Vielzahl von Lieferanten wie IBM, Microsoft, Cisco Systems und Netscape unterstützt. Das Ziel ist, eine Informationsmodellspezifikation für ein integriertes Verzeichnis zu liefern, das Informationen zu Menschen, Netzwerkeinheiten und Anwendungen speichert.

In der Netzwerkbetriebsindustrie wird DEN momentan als die Schlüsselkomponente zum Aufbauen intelligenter Netzwerke angesehen, in denen Produkte mehrerer Lieferanten die Topologie und Konfiguration zugehöriger Daten auf einem LDAP-Server speichern und von dort abrufen können.

Aus VPN-Sicht sind eine Policy-Konfigurationsanwendung und die VPN-Einheiten LDAP-Clients, die mit einem LDAP-Server kommunizieren. Die Policy-Konfigurationsanwendung wirkt mit dem LDAP-Server zusammen, um VPN-Policies zu erstellen, zu aktualisieren und zu löschen. Die VPN-Einheiten wirken mit dem LDAP-Server zusammen, um seine VPN-Policies abzurufen. Die Austauschvorgänge zwischen den LDAP-Clients und dem LDAP-Server basieren auf einem Policy-Schema, das die Objekte oder Daten definiert, durch die eine VPN-Policy dargestellt wird.

Einheiteninteraktionen

Die Policy-Konfigurationsanwendung wird zum Definieren von VPN-Policies für alle VPN-Einheiten verwendet. Die VPN-Policies werden auf einem LDAP-Server gespeichert und im Anschluß während der Initialisierung auf die VPN-Einheiten heruntergeladen. Dies geschieht aufgrund einer Anforderung von der Policy-Konfigurationsanwendung oder aufgrund einer Anforderung von einer VPN-Monitoranwendung.

VPN List Manager verwenden

Dieses Kapitel enthält die folgenden Abschnitte:

- Informationen zu **VPN List**
- Informationen zur Anzeige **VPN List Manager Information**
- Informationen zur Anzeige **VPN Device List**

Informationen zu "VPN List"

Mit Nways VPN List können Sie eine Liste von Einheiten anzeigen, die von einem Nways-Service namens VPN List Manager verwaltet werden. Dieser Service empfängt Einheiten von Benutzern dieser Anwendung und von den NetView- und OpenView-Datenbanken. Einheiten, die der NetView- oder OpenView-Liste hinzugefügt werden sollen, müssen zuerst einen Filtertest bestehen. Dieser Test prüft, ob die Einheit den von IBM implementierten virtuellen privaten Netzwerkbetrieb unterstützt. Mit dieser Anwendung können Sie der Liste über eine Benutzerliste von Einheiten, auf die alle VPN List Manager-Clients Zugriff haben, Einheiten hinzufügen. Dies ist hilfreich für Einheiten, die NetView und OpenView unbekannt sind oder die den in diesem Release von VPN List Manager implementierten Filtertest nicht bestehen.

Diese Anwendung ermöglicht die Benutzereingabesteuerung von VPN List Manager. Sie können die VPN List Manager-Liste zurücksetzen oder dieser Liste Einheiten hinzufügen, indem Sie auf Ihre manuell bearbeitete Liste zugreifen oder die NetView- bzw. OpenView-Datenbank auf neue Einheiten überprüfen, die eventuell geändert wurden. Die Fähigkeit einer Einheit, den Filtertest zu bestehen, kann sich aufgrund von Softwareerweiterungen seit dem ersten Test durch den Filter geändert haben.

Die Anwendung bietet Ihnen eine Liste mit Einheiten in Tabellenformat an, in der Sie blättern, suchen und sortieren können. Wenn Sie eine Einheit in der Liste anklicken, können Sie weitere Einzelangaben zur Einheit einsehen und VPN Monitor starten, um spezifische VPN-Informationen zu dieser Einheit aufzurufen.

Informationen zur Anzeige "VPN List Manager Information"

Diese Anzeige enthält die folgenden Abschnitte:

- Information
- Log File Settings
- Reset VPN Manager List
- Password
- Change Password

Sie ordnen einen Abschnitt im Anzeigebereich der Anzeige an, indem Sie den Namen des Abschnitts in der Auswahlliste links in der Anzeige einmal anklicken.

Aktionssteuerungsprioritäten

VPN List Manager führt in dieser Anzeige nur jeweils eine Aktion aus. Wenn in dieser Anzeige mehrere Änderungen angefordert werden, ermittelt VPN List Manager mit Hilfe der folgenden Hierarchie, welche der Aktionen ausgeführt werden sollen:

1. Kennwort ändern
2. Protokollstatus ändern
3. Liste zurücksetzen

Information

Dieser Abschnitt enthält folgende Felder:

VPN List Manager Host Name:
Der Host-Name des Systems, auf dem VPN List Manager ausgeführt wird

VPN List Manager IP Address:
Die IP-Adresse des Systems, auf dem VPN List Manager ausgeführt wird

VPN List Manager Version:
Die Version von VPN List Manager, die ausgeführt wird

VPN List Started on:
Die Uhrzeit und das Datum des Starts von VPN List Manager

Current Time on VPN List Manager:
Die aktuelle Uhrzeit und das aktuelle Datum auf dem System, auf dem VPN List Manager ausgeführt wird

Number of Devices:
Die aktuelle Anzahl der Einheiten in der Liste, die VPN List Manager verwaltet

Vergleichen Sie diese Zahl mit der Anzahl von Einheiten, die von diesem Client verwendet wird. Wenn die Zahlen von einander abweichen, klicken Sie den Knopf **Refresh** in der Anzeige **VPN Device List** an, um die Client-Liste von VPN List Manager zu aktualisieren.

Number of Clients:
Die Anzahl der Clients, die von VPN List Manager für den Empfang von Aktualisierungshinweisen bei Änderung der Liste registriert ist. Änderungen können durch andere Clients oder dadurch verursacht werden, daß VPN List Manager von OpenView bzw. Netview darüber benachrichtig wird, daß eine neue Einheit festgestellt oder hinzugefügt wurde.

This Client Notify Status:
Gibt an, ob dieser Client bei einer Änderung der Liste Aktualisierungen von VPN List Manager empfängt.

Clients werden für Aktualisierungen registriert, wenn VPN Manager initialisiert wird. Der Status muß *enabled* (aktiviert) sein.

Wenn der Status nicht *enabled* ist, weist dies auf ein Problem in der Verbindung zu VPN List Manager hin. Versuchen Sie, **VPN Device List** erneut anzuzeigen und zur Anzeige **VPN List Manager Control** zurückzukehren, um zu prüfen, ob sich der Status geändert hat.

Log File Settings

Dieser Abschnitt enthält folgende Felder:

Current Logging Status:

Gibt an, ob VPN List Manager seine Aktivitäten in einer Datei protokolliert. Wenn Benutzer diesen Status ändern wollen, müssen sie das aktuelle Kennwort eingeben und **Apply** anklicken, um die Änderung zu aktivieren.

Wird die Protokolldatei erstellt, wird sie vpnlist.log genannt und an die gleiche Position wie die anderen Nways Manager-Protokolldateien gestellt.

Reset List

Dieser Abschnitt enthält folgende Felder:

Current System Device Status:

Gibt an, ob VPN List Manager auf die NetView- oder OpenView-Systemdatenbank von Einheiten zugreifen konnte, die List Manager verwaltet.

Gültige Werte sind:

Failed to Load

Gibt an, daß VPN List Manager keinen Kontakt mit der Systemdatenbank aufnehmen konnte und daher die Einheitenliste nicht laden konnte.

Unknown Gibt an, daß VPN List Manager den Status der Systemdatenbank nicht kennt. Dies weist auf ein Problem mit VPN List Manager hin.

Loaded Der normale Status, der angibt, daß das System auf die Anforderung von VPN List Manager nach Einheiten geantwortet hat. Dies gibt an, daß VPN List Manager VPN-fähige Einheiten erfolgreich seiner Liste hinzugefügt hat.

Waiting for System to Respond

Gibt an, daß VPN List Manager noch keine Einheiten aus der Systemdatenbank hinzugefügt hat. Das System sammelt weiterhin Einheitendaten vom Netzwerk und übergibt sie nach Beendigung der Task an VPN List Manager.

Loading in progress...

Gibt an, daß das System momentan Informationen zu Einheiten an VPN List Manager übergibt.

Current User Device Status

Gibt den Status von Einheiten an, die Benutzer VPN List Manager manuell hinzugefügt haben.

Gültige Werte sind:

Failed to Load
Gibt an, daß VPN List Manager die angegebene Benutzerdatei nicht laden konnte. Dies weist auf ein Problem mit der Benutzerdatei hin.

Unknown Gibt an, daß VPN List Manager den Status der Benutzerdatei nicht kennt. Dies weist auf ein Problem mit VPN List Manager hin.

Loaded Die ist der normale Status, nachdem die Benutzerdatei von VPN List Manager gelesen wurde. Dies gibt an, daß VPN List Manager die Einheiten in der Benutzerdatei seiner Einheitenliste erfolgreich hinzugefügt hat.

Loading in progress...
Gibt an, daß VPN List Manager momentan die Benutzerdatei liest.

Reset List Ermöglicht das Hinzufügen zur aktuellen Liste der Einheiten bzw. das Aktualisieren dieser Liste. Wenn Sie die Liste zurücksetzen wollen, müssen Sie das aktuelle Kennwort eingeben. Klicken Sie **Apply** an, um die Liste mit der ausgewählten Grundstellungsart zurückzusetzen.

Password

Dieser Abschnitt enthält das folgende Feld:

Current Password:

Benutzer müssen ein gültiges Kennwort eingeben, bevor VPN List Manager Änderungen an den Einheitenlisten vornehmen kann. Änderungen an den VPN List Manager-Einheitenlisten wirken sich auf andere Clients aus, die diesen VPN List Manager verwenden, und sollten sorgfältig vorgenommen werden.

Das Standardkennwort ist **OK**.

Change Password

Dieser Abschnitt enthält das folgende Feld:

Change Password

Für diese Aktion ist die Eingabe des aktuellen Kennworts erforderlich. Sie müssen das neue Kennwort zweimal zur Bestätigung eingeben. Klicken Sie nach der Eingabe des neuen Kennworts **Apply** an, um das aktuelle Kennwort zu ändern.

Informationen zur Anzeige "VPN Device List"

Die Anzeige **VPN Device List** enthält die folgenden Abschnitte:

- Devices
- Details
- Print

Devices

Dieser Abschnitt enthält folgende Felder und Knöpfe:

Device Table

Die Einheitentabelle zeigt Informationen zu den Einheiten in der aktuellen Einheitenliste von VPN List Manager in einem Tabellenformat an. Damit können Sie nach Informationen suchen, in Informationen blättern und einzelne Einheiten auswählen.

Wenn sich der Zeiger über den Daten einer Zeile in der Tabelle befindet und Sie diese Zeile durch Anklicken auswählen, werden andere in der Anzeige dargestellten Informationen entsprechend aktualisiert.

Wählen Sie eine Spalte in der Tabelle aus, wird die Tabelle basierend auf den Daten in der ausgewählten Spalte in aufsteigender oder absteigender Reihenfolge sortiert.

Durch doppeltes Anklicken einer Zeile wird die gleiche Funktion ausgeführt wie beim Anklicken des Knopfs **Monitor**, d. h. VPN Monitor wird für die Einheit aufgerufen.

In der Tabelle werden die folgenden Spalten angezeigt:

Device Name Der Name, der der Einheit durch den Benutzer oder die Netzwerkmanagementplattform gegeben wurde

IP Address Die IP-Adresse der Einheit

Device Type Der Typ dieser Einheit

Search Fields

Die Suchfelder verwenden den Stern (*) als Platzhalterzeichen. Das Platzhalterzeichen kann am Anfang und/oder Ende eines Feldes verwendet werden. Das Platzhalterzeichen kann nicht innerhalb des Suchbegriffs verwendet werden. Sie können Einheiten nach Einheitenname und/oder IP-Adresse suchen.

Device Name

Der zu suchende Name

IP Address

Die zu suchende IP-Adresse

Knopf "Search"
Führt eine Suche unter Verwendung der Informationen aus der ersten Zeile der aktuellen Listensicht aus.

Knopf "Search Next"
Führt eine Suche unter Verwendung der Informationen aus der Zeile nach der momentan ausgewählten Zeile in der aktuellen Listensicht aus.

Details

Dieser Abschnitt enthält folgende Felder und Knöpfe:

Total Number of Devices in List:
Gibt die Gesamtzahl der Einheiten in der momentan angezeigten Liste an.

Device Name:
Der benutzerdefinierte Name der aktuellen Einheit

IP Address:
Die IP-Adresse der aktuellen Einheit

Read Community Name:
Der für Lesezugriff verwendete Name der SNMP-Benutzergemeinschaft für die aktuelle Einheit. Die Einheit kann über mehrere Zugriffsebenen zum Lesen und Schreiben verfügen. Dieser Name ist dem Lesezugriff zugeordnet.

Write Community Name:
Der für Schreibzugriff verwendete Name der SNMP-Benutzergemeinschaft für die aktuelle Einheit. Die Einheit kann über mehrere Zugriffsebenen zum Lesen und Schreiben verfügen. Dieser Name ist dem Schreib-/Lesezugriff zugeordnet.

Device Type:
Der Typ der aktuellen Einheit

Knopf "Add":
Wenn Sie diesen Knopf anklicken, werden der Liste unter Verwendung der eingegebenen Informationen neue Einheiten hinzugefügt.

Knopf "Change":
Ändert Attribute von Einheiten, die der Liste manuell hinzugefügt wurden. Mit der Systemmanagementplattform können Sie Änderungen an Einheiten vornehmen, die der Liste durch das System hinzugefügt wurden.

Knopf "Delete":
Löscht Einheiten, die der Liste manuell hinzugefügt wurden. Auf der Systemmanagementplattform können Sie durch das System hinzugefügte Einheiten löschen.

Knopf "Monitor":
Ruft VPN Monitor auf der aktuellen Einheit auf.

Print

Mit Hilfe der Funktionen in diesem Abschnitt können Sie die in der Liste angezeigten Informationen drucken. Sie können Kopfzeilen- und Fußzeilentext eingeben, der auf jeder gedruckten Seite ausgegeben wird.

Dieser Abschnitt enthält folgende Felder und Knöpfe:

Header: Geben Sie den Kopfzeilentext ein, der oben auf jeder Seite gedruckt werden soll.

Footer: Geben Sie den Fußzeilentext ein, der unten auf jeder Seite gedruckt werden soll.

Knopf "Print"

Wenn Sie diesen Knopf anklicken, wird eine Druckerauswahlliste angezeigt. Wählen Sie einen Drucker aus, um die Ausgabe für den richtigen Druckertyp zu formatieren.

Anmerkung: Wenn auf dem System kein Drucker definiert ist, kann die Druckfunktion die Einheitenliste nicht formatieren. Sie kehrt zur Anzeige **VPN Device List** zurück und gibt folgende Nachricht aus:

```
Print Cancelled
```

VPN Monitor

VPN Monitor bietet Ihnen Überwachung, Ereignisberichte, Fehlerbehebung, Betriebssteuerung und Anwendungsstartfunktionen für VPN-fähige Einheiten in Ihrem Netzwerk und für VPNs, die diese Einheiten verwenden.

Dieses Kapitel enthält Informationen zum Fenster **VPN Manager**. Es enthält die folgenden Abschnitte:

- Das Fenster **VPN Manager**
- Funktionen von VPN Monitor

Fenster "VPN Monitor"

Das Fenster **VPN Manager** setzt sich aus drei Teilen zusammen:

- Navigationsbaumstruktur
- Informationsanzeige
- Nachrichtenbereich

Navigationsbaumstrukturanzeige

Die Navigationsbaumstruktur ist eine hierarchische Struktur, mit der Sie den Bereich der Managementinformationen zur verwalteten Einheit anzeigen können.

Symbole

Die Navigationsbaumstruktur verwendet mehrere Symbole, um überwachte Ressourcen darzustellen:

Ordner Eine Ressource auf höherer Ebene, die mindestens ein abhängiges Objekt darstellt. Der Ordner oben in der Baumstruktur z. B. stellt in der Regel die Einheit selbst dar. Andere Ordner auf nachfolgenden Ebenen stellen möglicherweise Konfigurationsdaten oder Fehlerinformationen dar.

In jedem Ordner sind Objekte angeordnet, die einen Teil des Gesamtordners mit Informationen bilden. Der für einen Ordner angegebene Status wird aus den Status der unmittelbar abhängigen Objekte berechnet. Klicken Sie das Pluszeichen (+) neben einem Ordner an, um die Objekte im Ordner anzuzeigen und eine Aktion für diese auszuführen.

Seite Eine abhängige Ressource, die nur aus Informationen besteht, etwa Konfigurationsdaten. Diese Ressource ermöglicht eventuell Änderungen durch Benutzer. Dies hängt vom Objekt, von der verwalteten Einheit und von den Zugriffsrechten des Benutzers ab.

Navigieren

Erweitern Sie Ordner, indem Sie das Pluszeichen (+) neben dem Symbol anklicken. Hierdurch werden abhängige Objekte angezeigt.

Unterdrücken Sie Ordner, indem Sie das Minuszeichen (–) neben dem Symbol anklicken. Hierdurch werden abhängige Objekte verdeckt.

Informationsanzeige

In der Informationsanzeige werden Informationen zu der Funktion angezeigt, die in der Navigationsbaumstrukturanzeige ausgewählt ist. In dieser Anzeige können Sie alle Funktionen von VPN Monitor ausführen.

Nachrichtenbereich

Im Nachrichtenbereich werden Statusinformationen von VPN Monitor angezeigt.

Funktionen von VPN Monitor

VPN Monitor stellt die folgenden Funktionen bereit:

- Überwachung
- Ereignisberichte
- Betriebssteuerung
- Fehlerbehebung
- Anwendungen starten

Im verbleibenden Teil dieses Abschnitts wird beschrieben, wie Sie mit diesen Funktionen Ihr VPN und die Position der Funktionen in der Navigationsbaumstruktur verwalten können.

Überwachung

VPN Monitor zeigt Informationen zu mehrfachen Facetten Ihres Netzwerks an, wie Tunnel, Clients und Policies. Der „VPN Monitor-Ordner "Global Status"“ auf Seite 25 stellt Basisinformationen zum Status von Elementen in Ihrem VPN-Netzwerk bereit. Verwenden Sie den „VPN Monitor-Ordner "Tunnels"“ auf Seite 29, den „VPN Monitor-Ordner "Clients"“ auf Seite 43, den „VPN Monitor-Ordner "Policies"“ auf Seite 53 und den „VPN Monitor-Ordner "Quality of Service"“ auf Seite 47, um weitere Informationen anzuzeigen.

Diese Ordner liefern Ihnen wichtige Informationen zum Status von Elementen in Ihrem Netzwerk.

Ereignisberichte

VPN Monitor stellt Protokolle und Zähler für in Ihrem Netzwerk auftretende Ereignisse bereit, um zusätzliche Informationen zu Ihrem VPN zu liefern. Sie werden im „VPN Monitor-Ordner "Events"“ auf Seite 65 angezeigt.

Der Ordner **Events** zeigt Ereignisprotokolle und -zähler für erfolgreiche und erfolglose Layer-2-Tunnel und -Sitzungen sowie für erfolgreiche und erfolglose IPSec-Tunnel und -Verschlüsselungen an.

Betriebssteuerung

Mit VPN Monitor können Sie zudem Tunnel, Clients und Policies von Ihrer Management-Workstation steuern. Mit dem „VPN Monitor-Ordner "Operational"“ auf Seite 69 können Sie IPSec- und Layer-2-Tunnel aktivieren bzw. inaktivieren, Clients aktivieren und inaktivieren sowie Ihre Policies aktualisieren.

Fehlerbehebung

VPN Monitor stellt im „VPN Monitor-Ordner "Tests"“ auf Seite 75 eine Vielzahl von Tools zur Verfügung, mit denen Sie in Ihrem Netzwerk Konnektivitätsprobleme ausfindig machen können. Im einzelnen können Sie potentielle Konnektivität, die Auswirkungen von neuen Policies vor ihrer Implementierung in Ihrem Netzwerk und die Umlaufzeit für einen angegebenen Tunnel bzw. zu einem angegebenen Host testen.

Anwendungen starten

Mit VPN Monitor können Sie einige Anwendungen starten, die Sie bei der Verwaltung Ihres Netzwerks unterstützen, unter anderem:

- Telnet
- Die JMA der überwachten Einheit
- MIB-Browser
- Ihren Web-Browser

VPN Monitor-Ordner "General"

Der VPN Monitor-Ordner **General** liefert Informationen zu VPN-Einheiten in Ihrem Netzwerk. Er enthält zwei abhängige Objekte:

- Identification
- Administration

Identification

Die Anzeige **Identification** liefert Basisinformationen, die die ausgewählte VPN-Einheit beschreiben. Sie enthält die folgenden Felder, in denen Informationen angezeigt werden, die aus der Managementinformationsdatenbank (MIB - Management Information Base) der Einheit abgerufen wurden.

Description
Eine Beschreibung der Einheit

Device ID Die Systemobjektkennung (SYSOID) für die Einheit

Contact Die Kontaktinformationen aus der Managementinformationsdatenbank (MIB - Management Information Base) der Einheit. Berechtigte Benutzer können diese Informationen in der Anzeige **Identification** ändern.

Domain Name
Der von der Einheit verwendete IP-Domänenname. Berechtigte Benutzer können diese Informationen in der Anzeige **Identification** ändern.

Location Die Positionsinformationen für die Einheit. Berechtigte Benutzer können diese Informationen in der Anzeige **Identification** ändern.

Up Time Die Zeitdauer seit dem letzten Start bzw. Neustart der Einheit

System Services
Eine Nummer, die das Leistungsspektrum der Einheit darstellt

System Service Functions
Eine Textbeschreibung des Leistungsspektrums, das durch die Nummer für „System Services“ dargestellt wird

Administration

Die Anzeige **Administration** zeigt die SNMP-Parameter an, die VPN Monitor zur Kommunikation mit der Einheit verwendet. Berechtigte Benutzer können diese Informationen in der Anzeige **Administration** ändern.

Die Anzeige **Administration** enthält die folgenden Felder:

IP Address
Die für SNMP-Anforderungen verwendete IP-Adresse

Community Name (Read)
Der für Leseanforderungen verwendete SNMP-Benutzergemeinschaftsname

Community Name (Write)
Der für Schreibanforderungen verwendete SNMP-Benutzergemeinschaftsname

Remote Port
Der für SNMP-Anforderungen verwendete Anschluß der Einheit

Timeout (ms)
Der für SNMP-Anforderungen verwendete Zeitlimitüberschreitungswert in Millisekunden

Retries Die für SNMP-Anforderungen verwendete Anzahl von Wiederholungen

Polling Interval
Das für SNMP-Anforderungen verwendete Sendeaufrufintervall in Millisekunden

VPN Monitor-Ordner "Global Status"

Der VPN Monitor-Ordner **Global Status** bietet eine Anzeige der VPN-Verarbeitung auf der ausgewählten Einheit. Er enthält das folgende abhängige Objekt:

- At-A-Glance

At-A-Glance

Die Anzeige **At-A-Glance** liefert Übersichtsdaten zur VPN-Verarbeitung auf der ausgewählten Einheit. Sie enthält die folgenden Abschnitte:

- Levels
- Tunnels
- Clients
- Policy
- Events

Levels

Der Abschnitt **Levels** liefert Informationen zum Protokollcode und zu den Nachrichteninformationsblöcken (MIBs), die von der Einheit verwendet werden. Er enthält die folgenden Felder:

Layer-2 MIB Version
: Die Version der von der Einheit verwendeten Layer-2-Managementinformationsdatenbank (MIB - Management Information Base)

Layer-2 Protocol Version
: Die Version des von der Einheit verwendeten Layer-2-Protokollcodes

IPSec MIB Version
: Die Version der von der Einheit verwendeten IPSec-Managementinformationsdatenbank (MIB - Management Information Base)

Policy MIB Version
: Die Version der von der Einheit verwendeten Policy-Managementinformationsdatenbank (MIB - Management Information Base)

Tunnels

Der Abschnitt **Tunnels** liefert Informationen zur Anzahl der momentan aktiven Layer-2- und IPSec-Tunnel auf dieser Einheit.

Clients

Im Abschnitt **Clients** wird die Anzahl der momentan aktiven Layer-2-Sitzungen auf dieser Einheit angezeigt.

Policy

Der Abschnitt **Policy** liefert Informationen zur VPN-Policy, die momentan von der Einheit verwendet wird. Er enthält die folgenden Felder:

Policy Up Time
Die Zeit, in der der aktuelle Policy-Komponentencode aktiv war

Device Up Time
Die Zeit, in der die Einheit aktiv war

Device Current Time
Die aktuelle, von der Einheit verwendete Uhrzeit

Hours from UTC
Die Differenz zwischen der von der Einheit verwendeten Zeit und der aktuellen Westeuropäischen Zeit

Current Config Source
Die Quelle für die aktuelle Policy-Konfiguration

Policy Load Status
Die Ergebnisse des letzten Versuchs, eine Policy zu laden

Events

Der Abschnitt **Events** liefert Informationen zu Ereignissen, die von VPN Monitor für diese Einheit überwacht wurden. Er enthält die folgenden Felder:

Layer-2 Tunnel Successes
Die Anzahl der erfolgreich für diese Einheit aktivierten Layer-2-Tunnel

Layer-2 Tunnel Failures
Die Anzahl der Layer-2-Tunnel für diese Einheit, für die ein erfolgloser Aktivierungsversuch unternommen wurde

Layer-2 Session Successes
Die Anzahl der erfolgreich für diese Einheit aktivierten Layer-2-Sitzungen

Layer-2 Session Failures
Die Anzahl der erfolglosen Versuche, eine Layer-2-Sitzung für diese Einheit zu aktivieren

IPSec In Authentications
Die Anzahl der erfolgreichen ankommenden IPSec-Authentifizierungen

IPSec In Authentication Failures
Die Anzahl der fehlgeschlagenen ankommenden IPSec-Authentifizierungsversuche

IPSec In Decryptions
Die Anzahl der erfolgreich ausgeführten ankommenden IPSec-Entschlüsselungen

IPSec In Decryption Failures
Die Anzahl der fehlgeschlagenen ankommenden IPSec-Entschlüsselungsversuche

IPSec Out Authentications
Die Anzahl der erfolgreich abgehenden IPSec-Authentifizierungen

IPSec Out Authentication Failures
Die Anzahl der fehlgeschlagenen abgehenden IPSec-Authentifizierungsversuche

IPSec Out Encryptions
Die Anzahl der erfolgreich ausgeführten abgehenden IPSec-Entschlüsselungen

IPSec Out Encryption Failures
Die Anzahl der fehlgeschlagenen abgehenden IPSec-Entschlüsselungsversuche

VPN Monitor-Ordner "Tunnels"

Der VPN Monitor-Ordner **Tunnels** enthält Informationen zum Status von Layer-2- und IPSec-Tunneln, die von der ausgewählten Einheit verwendet werden. Dieser Ordner enthält die folgenden abhängigen Objekte:

- Ordner **Layer-2 Tunnels**
- Ordner **IPSec Tunnels**

Ordner "Layer-2 Tunnels"

Der Ordner **Layer-2 Tunnels** liefert Informationen zu aktiven und vorherigen Layer-2-Tunneln für die ausgewählte Einheit. Er enthält die folgenden abhängigen Objekte:

- Ordner **Active Tunnels**
- Ordner **Previous Tunnels**

Ordner "Active Tunnels"

Der Ordner **Active Tunnels** liefert Informationen zu allen aktiven Layer-2-Tunneln, die der ausgewählten Einheit zugeordnet sind. Er enthält die folgenden abhängigen Objekte:

- Anzeige **Status**
- Anzeige **Attributes**
- Anzeige **Statistics**
- Anzeige **End-Points**

Anzeige "Status"

Die Anzeige **Status** liefert Informationen zum Status von aktiven Layer-2-Tunneln, die der ausgewählten Einheit zugeordnet sind. Sie enthält die folgenden Felder:

Tunnel Die Indexnummer des Tunnels

Status Der Status des Tunnels: **active** (aktiv) oder **destroy** (löschen). Berechtigte Benutzer können diesen Wert in der Anzeige **Status** ändern.

Type Die Tunnelart: L2TP, L2F oder PPTP

Remote Host
Der Name des fernen Hosts, der diesem Tunnel zugeordnet ist

Active Time
Der Zeitraum, in dem der Tunnel aktiv war

Active Sessions
Die Anzahl der aktiven Sitzungen, die diesem Tunnel zugeordnet sind

Previous Sessions
Die Anzahl der zuvor aktiven Sitzungen, die diesem Tunnel zugeordnet sind

Destroy All Tunnels
Der Auslöser zum Löschen aller Layer-2-Tunnel. Berechtigte Benutzer können diesen Wert in der Anzeige **Status** ändern.

Anzeige "Attributes"

Die Anzeige **Attributes** liefert Informationen zu den Attributen eines ausgewählten Tunnels. Sie enthält die folgenden Felder:

Local Control ID
Die lokale Steuer-ID für den Tunnel

Peer Control ID
Die Peer-Steuer-ID für den Tunnel

Control State
Der Steuerstatus für den Tunnel

Control Timouts
Die Anzahl der für diesen Tunnel aufgezeichneten Steuerzeitlimitüberschreitungen

Remote Host
Der Name des fernen Hosts, der diesem Tunnel zugeordnet ist

Remote Vendor Name
Der Name des Lieferanten für den fernen Host

Remote Firmware Version
Die Version der auf dem fernen Host ausgeführten Firmware

Remote Protocol Version
Die vom fernen Host verwendete Protokollversion

Init Connect
Gibt an, ob der Tunnel vom lokalen Host generiert wurde

Local Receive Packet Window
Die Größe des Empfangspaketfensters, das vom lokalen Host verwendet wird

Remote Receive Packet Window
Die Größe des Empfangspaketfensters, das vom fernen Host verwendet wird

Next Send Sequence
Der Wert der nächsten Sendefolgenummer

Next Receive Sequence
Der Wert der nächsten Empfangsfolgenummer

Anzeige "Statistics"

Die Anzeige **Statistics** liefert Statistiken zum angegebenen Layer-2-Tunnel. Sie enthält die folgenden Felder:

In Bytes Die Anzahl der Byte, die über diesen Tunnel empfangen wurden

In Packets
Die Anzahl der Pakete, die über diesen Tunnel empfangen wurden

In Discarded Packets
Die Anzahl der Pakete, die während des Empfangs über diesen Tunnel gelöscht wurden

Out Bytes Die Anzahl der Byte, die durch den lokalen Host über diesen Tunnel gesendet wurden

Out Packets
Die Anzahl der Pakete, die durch den lokalen Host über diesen Tunnel gesendet wurden

Out Discarded Packets
Die Anzahl der Pakete, die während des Sendens über diesen Tunnel durch den lokalen Host gelöscht wurden

Anzeige "End Points"

Die Anzeige **End Points** liefert Informationen zum Endpunkt eines ausgewählten Tunnels. Sie enthält die folgenden Felder:

Remote IP Address
Die ferne IP-Adresse, die dem ausgewählten Tunnel zugeordnet ist

Local IP Address
Die lokale IP-Adresse des ausgewählten Tunnels

Source Port
Der Anschluß des lokalen Hosts, der diesem Tunnel zugeordnet ist

Destination Port
Der Anschluß des fernen Hosts, der diesem Tunnel zugeordnet ist

Ordner "Previous Tunnels"

Der Ordner **Previous Layer-2 Tunnels** liefert eine Zusammenfassung und Statistikinformationen zu angegebenen vorherigen Layer-2-Tunneln, die der ausgewählten Einheit zugeordnet sind. Die Anzahl der vorherigen Einträge, zu denen Informationen angezeigt wird, kann in der Anzeige **Summary** angegeben werden. Der Ordner **Previous Layer-2 Tunnels** enthält die folgenden abhängigen Objekte:

- Anzeige **Summary**
- Anzeige **Statistics**

Anzeige "Summary"

Die Anzeige **Summary** liefert Informationen zu einem ausgewählten zuvor aktiven Layer-2-Tunnel. Sie enthält die folgenden Felder:

Order Die Anordnung, in der der Tunnel beendet wurde

Tunnel Der Index des Tunnels

Type Die Tunnelart: L2TP, L2F, PPTP

Remote Host
Der Name des fernen Hosts, der dem Tunnel zugeordnet ist

Remote IP Address
Die ferne IP-Adresse, die dem Tunnel zugeordnet ist

Remote Port
Der ferne Anschluß, der dem Tunnel zugeordnet ist

Local IP Address
Die lokale IP-Adresse, die dem Tunnel zugeordnet ist

Local Port Der lokale Anschluß, der dem Tunnel zugeordnet ist

Total Sessions
Die Gesamtzahl der aktiven Sitzungen, die vom Tunnel verwendet werden

Tunnel Up Time
Der Zeitraum, in dem der Tunnel aktiv war

Anzeige "Statistics"

Die Anzeige **Statistics** liefert Informationen zur Verwendung eines vorherigen Tunnels. Sie enthält die folgenden Felder:

In Bytes Die Anzahl der Byte, die über diesen Tunnel von der überwachten Einheit empfangen wurden

In Packets
Die Anzahl der Pakete, die über diesen Tunnel von der überwachten Einheit empfangen wurden

In Discarded Packets
Die Anzahl der Pakete, die während des Empfangs über diesen Tunnel durch die überwachte Einheit gelöscht wurden

Out Bytes Die Anzahl der Byte, die durch die überwachte Einheit über diesen Tunnel gesendet wurden

Out Packets
Die Anzahl der Pakete, die durch die überwachte Einheit über diesen Tunnel gesendet wurden

Out Discarded Packets
Die Anzahl der Pakete, die während des Sendens über diesen Tunnel durch die überwachte Einheit gelöscht wurden

Ordner "IPSec Tunnels"

Der Ordner **IPSec Control Tunnels** liefert Informationen zu aktiven und vorherigen IPSec-Tunneln für die ausgewählte Einheit. Er enthält die folgenden abhängigen Objekte:

- Ordner **Active Tunnels**
- Ordner **Previous Tunnels**

Ordner "Active Tunnels"

Der Ordner **Active Tunnels** liefert Informationen zu aktiven IPSec-Steuertunneln und IPSec-Benutzerdatentunneln. Er enthält die folgenden abhängigen Objekte:

- Ordner **Active IPSec Control Tunnels**
- Ordner **Active IPSec User-Data Tunnels**

Ordner "Active IPSec Control Tunnels"

Der Ordner **Active IPSec Control Tunnels** liefert Informationen zu aktiven IPSec-Steuertunneln, die der ausgewählten Einheit zugeordnet sind. Er enthält die folgenden Anzeigen:

- Status
- Attributes
- Statistics
- Processing

Status: Die Anzeige **Status** liefert Informationen zum Status eines ausgewählten IPSec-Steuertunnels. Sie enthält die folgenden Felder:

Tunnel Die Indexnummer des ausgewählten Tunnels

Status Der Status des Tunnels: **active** (aktiv) oder **destroy** (löschen). Berechtigte Benutzer können diesen Wert in der Anzeige **Status** ändern.

ID Die ID des ausgewählten Tunnels

Remote Name
Der ferne Name des Tunnels

Remote Address
Die ferne IP-Adresse des Tunnels

Local Name
Der lokale Name des Tunnels

Local Address
Die lokale IP-Adresse des Tunnels

Up Time Der Zeitraum, in dem der Tunnel aktiv war

Destroy All Tunnels
Der Auslöser zum Löschen aller aktiven IPSec-Steuertunnel. Berechtigte Benutzer können diesen Wert in der Anzeige **Status** ändern.

Attributes: Die Anzeige **Attributes** liefert Informationen zu den Attributen des ausgewählten IPSec-Steuertunnels. Sie enthält die folgenden Felder:

Negotiation Mode
Der Modus, der vom ausgewählten IPSec-Steuertunnel verwendet wird, um neue Verbindungen mit fernen Hosts zu vereinbaren

SA Lifetime
Die Lebensdauer der Sicherheitszuordnung für den Tunnel in Sekunden

SA Refresh Threshold Percent
Der Schwellenprozentwert der Aktualisierung für die Sicherheitszuordnung

Total SA Refreshes
Die Anzahl der ausgeführten Aktualisierungen für die Sicherheitszuordnung

Statistics: Diese Anzeige liefert Statistiken zum ausgewählten IPSec-Steuertunnel. Sie enthält die folgenden Felder:

In Bytes Die Anzahl der Byte, die über diesen Tunnel von der überwachten Einheit empfangen wurden

In Packets
Die Anzahl der Pakete, die über diesen Tunnel von der überwachten Einheit empfangen wurden

In Dropped Packets
Die Anzahl der Pakete, die während des Empfangs über diesen Tunnel durch die überwachte Einheit gelöscht wurden

Out Bytes Die Anzahl der Byte, die durch die überwachte Einheit über diesen Tunnel gesendet wurden

Out Packets
Die Anzahl der Pakete, die durch die überwachte Einheit über diesen Tunnel gesendet wurden

Out Dropped Packets
Die Anzahl der Pakete, die während des Sendens über diesen Tunnel durch die überwachte Einheit gelöscht wurden

Processing: Diese Anzeige liefert Informationen zur Verarbeitung hinsichtlich des ausgewählten IPSec-Steuertunnels. Sie enthält die folgenden Felder:

In Notifys Die Anzahl der Hinweise, die über diesen Tunnel empfangen wurden

In Proposals
Die Anzahl der Angebote, die über diesen Tunnel empfangen wurden

In Invalid Proposals
Die Anzahl der Angebote, die über diesen Tunnel empfangen wurden, jedoch ungültig waren

In Rejected Proposals
Die Anzahl der Angebote, die über diesen Tunnel empfangen, jedoch zurückgewiesen wurden

In SA Deletes
Die Anzahl der Löschungen von Sicherheitszuordnungen, die über diesen Tunnel empfangen wurden

Out Notifys
Die Anzahl der Hinweise, die über diesen Tunnel gesendet wurden

Out Proposals
Die Anzahl der Angebote, die über diesen Tunnel gesendet wurden

Out Invalid Proposals
Die Anzahl der Angebote, die über diesen Tunnel gesendet wurden, jedoch ungültig waren

Out Rejected Proposals
Die Anzahl der Angebote, die über diesen Tunnel gesendet, jedoch zurückgewiesen wurden

Out SA Deletes
Die Anzahl der Löschungen von Sicherheitszuordnungen, die über diesen Tunnel gesendet wurden

Ordner "Active IPSec User-Data Tunnels"

Dieser Ordner liefert Informationen zu aktiven IPSec-Benutzerdatentunneln, die der ausgewählten Einheit zugeordnet sind. Er enthält die folgenden abhängigen Objekte:

- Anzeige **Status**
- Anzeige **Attributes**
- Anzeige **Statistics**
- Anzeige **End Points**
- Anzeige **Security Protection Indices**

Anzeige "Status": Diese Anzeige liefert Informationen zum Status des ausgewählten IPSec-Benutzerdatentunnels. Sie enthält die folgenden Felder:

Tunnel Die Indexnummer des ausgewählten Tunnels

Status Der Status des ausgewählten Tunnels: **active** (aktiv) oder **destroy** (löschen). Berechtigte Benutzer können diesen Wert in der Anzeige **Status** ändern.

Remote IP Address
Die ferne IP-Adresse des Tunnels

Local IP Address
Die lokale IP-Adresse des Tunnels

Up Time Der Zeitraum, in dem der Tunnel aktiv war

Total Security Association Refreshes
Die Gesamtzahl der ausgeführten Aktualisierungen für die Sicherheitszuordnung

Current Security Associations
Die Anzahl der aktuellen Sicherheitszuordnungen

Expired Security Associations
Die Anzahl der abgelaufenen Sicherheitszuordnungen

Destroy All Tunnels
Der Auslöser zum Löschen aller aktiven IPSec-Benutzerdatentunnel. Berechtigte Benutzer können diesen Wert in der Anzeige **Status** ändern.

Anzeige "Attributes": Diese Anzeige liefert Informationen zu den Attributen des ausgewählten IPSec-Benutzerdatentunnels. Sie enthält die folgenden Felder:

ID Die Indexnummer des Tunnels

Control Tunnel
Die Indexnummer des IPSec-Steuertunnels, der diesem IPSec-Benutzerdatentunnel zugeordnet ist

Key Type Der Schlüsseltyp des Tunnels

Encapsulation Mode
Der Kapselungsmodus des Tunnels

Security Association Lifetime
Die Lebensdauer der Sicherheitszuordnung für den Tunnel in Sekunden

Security Association Refresh Threshold Percent
Der Schwellenprozentwert der Aktualisierung für die Sicherheitszuordnung

In SA Encryption
Die für diesen Tunnel verwendete Art der Verschlüsselung für ankommende Sicherheitszuordnungen

In SA Authentication
Der für diesen Tunnel verwendete Algorithmus für die Authentifizierung ankommender Sicherheitszuordnungen

Out SA Encryption
Die für diesen Tunnel verwendete Art der Verschlüsselung für abgehende Sicherheitszuordnungen

Out SA Authentication
Der für diesen Tunnel verwendete Algorithmus für die Authentifizierung abgehender Sicherheitszuordnungen

Anzeige "Statistics": Diese Anzeige liefert Benutzungsstatistiken für den ausgewählten IPSec-Benutzerdatentunnel. Sie enthält die folgenden Felder:

In Bytes Die Anzahl der Byte, die über diesen Tunnel empfangen wurden

In Byte Counter Wraps
Die Anzahl der Umläufe des Zählers für ankommende Byte

In Decompressed Bytes
Die Anzahl der dekomprimierten Byte, die über diesen Tunnel empfangen wurden

In Decompressed Byte Wraps
Die Anzahl der Umläufe des Zählers für ankommende dekomprimierte Byte

In Packets
Die Anzahl der Pakete, die über diesen Tunnel empfangen wurden

In Dropped Packets
Die Anzahl der Pakete, die während des Empfangs über diesen Tunnel gelöscht wurden

In Authentications
Die Anzahl der für diesen Tunnel ausgeführten Authentifizierungen ankommender Daten

In Authentication Failures
Die Anzahl der für diesen Tunnel ausgeführten Authentifizierungen ankommender Daten, die erfolglos waren

In Decryptions
Die Anzahl der für diesen Tunnel ausgeführten Entschlüsselungen ankommender Daten

In Decryption Failures
Die Anzahl der für diesen Tunnel ausgeführten Entschlüsselungen ankommender Daten, die erfolglos waren

Out Bytes Die Anzahl der über diesen Tunnel gesendeten Byte

Out Byte Counter Wraps
Die Anzahl der Umläufe des Zählers für abgehende Byte

Out Decompressed Bytes
Die Anzahl der über diesen Tunnel gesendeten dekomprimierten Byte

Out Decompressed Byte Wraps
Die Anzahl der Umläufe des Zählers für abgehende dekomprimierte Byte

Out Packets
Die Anzahl der über diesen Tunnel gesendeten Pakete

Out Dropped Packets
Die Anzahl der Pakete, die während der Übertragung über diesen Tunnel gelöscht wurde

Out Authentications
Die Anzahl der für diesen Tunnel ausgeführten Authentifizierungen abgehender Daten

Out Authentication Failures
Die Anzahl der für diesen Tunnel ausgeführten Authentifizierungen abgehender Daten, die erfolglos waren

Out Encryptions
Die Anzahl der für diesen Tunnel ausgeführten Verschlüsselungen abgehender Daten

Out Encryption Failures
Die Anzahl der für diesen Tunnel ausgeführten Verschlüsselungen abgehender Daten, die erfolglos waren

Anzeige "End Points": Diese Anzeige liefert Informationen zu den Endpunkten des ausgewählten Tunnels. Sie enthält die folgenden Felder:

Local Name
Der lokale Name des Tunnels

Local Type
Die Art der lokalen Adressierung: **subnet** (Teilnetz) oder **range** (Bereich)

Local Protocol
Das lokale Protokoll des Tunnels

Local Subnet Mask
Die für den Tunnel verwendete lokale Teilnetzmaske

Local Low IP Address
Die lokale niedrige IP-Adresse für den Tunnel

Local High IP Address
Die lokale hohe IP-Adresse für den Tunnel

Local Port Der vom Tunnel verwendete lokale Anschluß

Remote Name
Der ferne Name des Tunnels

Remote Type
Die Art der fernen Adressierung: **subnet** (Teilnetz) oder **range** (Bereich)

Remote Protocol
Das ferne Protokoll des Tunnels

Remote Subnet Mask
Die für den Tunnel verwendete ferne Teilnetzmaske

Remote Low IP Address
Die ferne niedrige IP-Adresse für den Tunnel

Remote High IP Address
Die ferne hohe IP-Adresse für den Tunnel

Remote Port
Der vom Tunnel verwendete ferne Anschluß

Anzeige "Security Protection Indices": Diese Anzeige liefert Informationen zum Sicherheitsschutzindex (SPI - Security Protection Index), der vom Tunnel verwendet wird. Sie enthält die folgenden Felder:

SPI Der vom Tunnel verwendete Sicherheitsschutzindex

Direction Die Richtung des Datenverkehrs, in der der SPI angewendet wird: **in** (Eingang) oder **out** (Ausgang)

Value Der Wert des Sicherheitsschutzindex

Protocol Das vom Sicherheitsschutzindex verwendete Protokoll

Ordner "Previous Tunnels"

Dieser Ordner liefert Informationen zu IPSec-Benutzerdatentunneln, die nicht mehr aktiv sind. Er enthält die folgenden Anzeigen:

- Anzeige **Summary**
- Anzeige **Statistics**

Anzeige "Summary": Diese Anzeige liefert Übersichtsdaten zu vorherigen IPSec-Benutzerdatentunneln. Sie enthält die folgenden Felder:

Order Die Anordnung, in der der Tunnel beendet wurde

ID Die ID des Tunnels

Remote IP Address
Die vom Tunnel verwendete ferne IP-Adresse

Local IP Address
Die vom Tunnel verwendete lokale IP-Adresse

Up Time Der Zeitraum, in dem der Tunnel aktiv war

Total SA Refreshes
Die Anzahl der für diesen Tunnel ausgeführten Aktualisierungen der Sicherheitszuordnung

Total SAs Die Gesamtzahl der Sicherheitszuordnungen für diesen Tunnel

Anzeige "Statistics": Diese Anzeige liefert Benutzungsstatistiken für einen ausgewählten, zuvor aktiven IPSec-Benutzerdatentunnel. Sie enthält die folgenden Felder:

In Bytes Die Anzahl der Byte, die über diesen Tunnel empfangen wurden

In Byte Counter Wraps
Die Anzahl der Umläufe des Zählers für ankommende Byte

In Decompressed Bytes
Die Anzahl der dekomprimierten Byte, die über diesen Tunnel empfangen wurden

In Decompressed Byte Wraps
Die Anzahl der Umläufe des Zählers für ankommende dekomprimierte Byte

In Packets
Die Anzahl der Pakete, die über diesen Tunnel empfangen wurden

In Dropped Packets
Die Anzahl der Pakete, die während des Empfangs über diesen Tunnel gelöscht wurden

In Authentications
Die Anzahl der für diesen Tunnel ausgeführten Authentifizierungen ankommender Daten

In Authentication Failures
Die Anzahl der für diesen Tunnel ausgeführten Authentifizierungen ankommender Daten, die erfolglos waren

In Decryptions
Die Anzahl der für diesen Tunnel ausgeführten Entschlüsselungen ankommender Daten

In Decryption Failures
Die Anzahl der für diesen Tunnel ausgeführten Entschlüsselungen ankommender Daten, die erfolglos waren

Out Bytes Die Anzahl der über diesen Tunnel gesendeten Byte

Out Byte Counter Wraps
Die Anzahl der Umläufe des Zählers für abgehende Byte

Out Decompressed Bytes
Die Anzahl der über diesen Tunnel gesendeten dekomprimierten Byte

Out Decompressed Byte Wraps
Die Anzahl der Umläufe des Zählers für abgehende dekomprimierte Byte

Out Packets
Die Anzahl der über diesen Tunnel gesendeten Pakete

Out Dropped Packets
Die Anzahl der Pakete, die während der Übertragung über diesen Tunnel gelöscht wurden

Out Authentications
Die Anzahl der für diesen Tunnel ausgeführten Authentifizierungen abgehender Daten

Out Authentication Failures
Die Anzahl der für diesen Tunnel ausgeführten Authentifizierungen abgehender Daten, die erfolglos waren

Out Encryptions
Die Anzahl der für diesen Tunnel ausgeführten Verschlüsselungen abgehender Daten

Out Encryption Failures
Die Anzahl der für diesen Tunnel ausgeführten Verschlüsselungen abgehender Daten, die erfolglos waren

VPN Monitor-Ordner "Clients"

Der VPN Monitor-Ordner **Clients** liefert Informationen zu Layer-2-Sitzungen. Er enthält den folgenden Unterordner:

- Layer-2 Sessions

Ordner "Layer-2 Sessions"

Dieser Ordner liefert Informationen zu Layer-2-Sitzungen für die ausgewählte Einheit. Er enthält die folgenden Unterordner:

- Active Sessions
- Previous Layer-2 Sessions

Ordner "Active Sessions"

Dieser Ordner liefert Informationen zu aktiven Layer-2-Sitzungen für die ausgewählte Einheit. Er enthält die folgenden Ordner:

- Status
- Statistics

Ordner "Status"

Dieser Ordner liefert Statusinformationen zu einer ausgewählten Layer-2-Sitzung. Er enthält die folgenden Anzeigen:

- Status
- Attributes
- Statistics

Anzeige "Status": Diese Anzeige liefert Informationen zum Status einer ausgewählten Layer-2-Sitzung. Sie enthält die folgenden Felder:

Tunnel Der Index des Tunnels, der von der ausgewählten Sitzung verwendet wird

Session Der Index der Sitzung

Status Der Status der Sitzung: **active** (aktiv) oder **destroy** (löschen). Berechtigte Benutzer können diesen Wert in der Anzeige **Status** ändern.

Session Up Time
Der Zeitraum, in dem die Sitzung aktiv war

Connect BPS
Die Geschwindigkeit der Verbindung in Bit pro Sekunde

Authentication Method
Die von dieser Sitzung verwendete Authentifizierungsmethode

Encryption/Decryption
Der Verschlüsselungs-/Entschlüsselungsanzeiger für diese Sitzung. **True** gibt an, daß für die Sitzung Verschlüsselung und Entschlüsselung verwendet werden. **False** gibt an, daß sie nicht verwendet werden.

Destroy All Sessions
Der Auslöser zum Löschen aller Layer-2-Sitzungen. Berechtigte Benutzer können diesen Wert in der Anzeige **Status** ändern.

Anzeige "Attributes": In dieser Anzeige werden die Attribute der ausgewählten Sitzung aufgelistet. Sie enthält die folgenden Felder:

Remote Name
Der ferne Name der Sitzung

Line State Der Leitungsstatus der Sitzung

Local ID Die lokale ID der Sitzung

Remote ID
Die ferne ID der Sitzung

Device Number
Die von der Sitzung verwendete Einheitennummer

Serial Number
Die von der Sitzung verwendete Seriennummer der Einheit

Bearer Type
Der von der Sitzung verwendete Trägertyp: **digital** oder **analog**

Framing Type
Die von der Sitzung verwendete Rahmenart: **synchronous** (synchron) oder **asynchronous** (asynchron)

Local Packet Window
Die Größe des lokalen Paketfensters

Remote Packet Window
Die Größe des fernen Paketfensters

Timeouts Die Anzahl der während dieser Sitzung aufgetretenen Zeitlimitüberschreitungen

Next Send Sequence
Der Wert der nächsten Sendefolgenummer

Next Receive Sequence
Der Wert der nächsten Empfangsfolgenummer

Remote PPD
Die Länge der Verarbeitungsverzögerung für das ferne Paket

Anzeige "Statistics": Diese Anzeige liefert statistische Informationen zur ausgewählten Layer-2-Sitzung. Sie enthält die folgenden Felder:

In Bytes Die Anzahl der empfangenen Byte

In Uncompressed Bytes
Die Anzahl der empfangenen unkomprimierten Byte

In Packets
Die Anzahl der empfangenen Pakete

In Discarded Packets
Die Anzahl der während des Empfangs gelöschten Pakete

Out Bytes Die Anzahl der gesendeten Byte

Out Uncompressed Bytes
Die Anzahl der gesendeten unkomprimierten Byte

Out Packets
Die Anzahl der gesendeten Pakete

Out Discarded Packets
Die Anzahl der während des Sendens gelöschten Pakete

Ordner "Previous Layer-2 Sessions"

Dieser Ordner liefert Informationen zu vorherigen Layer-2-Sitzungen für die ausgewählte Einheit. Er enthält die folgenden abhängigen Objekte:

- Anzeige **Summary**
- Anzeige **Statistics**

Anzeige "Summary": Diese Anzeige liefert Übersichtsdaten zu einer ausgewählten Layer-2-Sitzung auf der ausgewählten Einheit. Sie enthält die folgenden Felder:

Order Die Anordnung, in der die Sitzung beendet wurde

Tunnel Der Index des von der Sitzung verwendeten Tunnels

Session Der Index der zuvor aktiven Sitzung

Authentication Method
Die von der Sitzung verwendete Authentifizierungsmethode

Encryption/Decryption
Der Verschlüsselungs-/Entschlüsselungsanzeiger für die Sitzung. **True** gibt an, daß für die Sitzung Verschlüsselung/Entschlüsselung verwendet wird. **False** gibt an, daß sie nicht verwendet wird.

Up Time Der Zeitraum, in dem die Sitzung aktiv war

Anzeige "Statistics": Diese Anzeige liefert statistische Informationen zu einer zuvor aktiven Layer-2-Sitzung auf der ausgewählten Einheit. Sie enthält die folgenden Felder:

In Bytes Die Anzahl der empfangenen Byte

In Uncompressed Bytes
Die Anzahl der empfangenen unkomprimierten Byte

In Packets
Die Anzahl der empfangenen Pakete

In Discarded Packets
Die Anzahl der während des Empfangs gelöschten Pakete

Out Bytes Die Anzahl der gesendeten Byte

Out Uncompressed Bytes
Die Anzahl der gesendeten unkomprimierten Byte

Out Packets
Die Anzahl der gesendeten Pakete

Out Discarded Packets
Die Anzahl der während des Sendens gelöschten Pakete

VPN Monitor-Ordner "Quality of Service"

Dieser Ordner liefert Informationen zur Servicequalität für eine ausgewählte Sitzung unter Verwendung des Ressourcenreservierungsprotokolls (RSVP - Resource Reservation Protocol). Er enthält das folgende abhängige Objekt:

- RSVP

Ordner "RSVP"

Dieser Ordner enthält Informationen zum Ressourcenreservierungsprotokoll (RSVP), das für eine ausgewählte Sitzung verwendet wird. Er enthält die folgenden Anzeigen:

- Sessions
- Sender PATH Messages
- Upstream RESV Messages

Anzeige "Sessions"

Diese Anzeige liefert RSVP-Informationen zu einer ausgewählten Sitzung. Sie enthält die folgenden Felder:

Session Index
Der Sitzungsindex

Session Type
Die Sitzungsart

IP Protocol
Das von der Sitzung verwendete IP-Protokoll

Destination Address
Die Zieladresse der Sitzung

Destination Port
Der Zielanschluß der Sitzung

Number of Senders
Die Anzahl der Sender in der Sitzung

Number of RSVP Requests Received
Die Anzahl der von der ausgewählten Einheit empfangenen RSVP-Anforderungen

Number of RSVP Requests Sent
Die Anzahl der von der ausgewählten Einheit gesendeten RSVP-Anforderungen

Anzeige "Sender PATH Messages"

Diese Anzeige enthält Informationen zur ausgewählten Sitzung. Sie enthält die folgenden Felder:

Session Index
Der Index der Sitzung

Sender Index
Der Index des Senders, der dieser Sitzung zugeordnet ist

Session Type
Die Sitzungsart

IP Protocol
Das IP-Protokoll der Sitzung

Destination Address
Die dieser Sitzung zugeordnete Zieladresse

Destination Port
Der dieser Sitzung zugeordnete Zielanschluß

Source Address
Die dieser Sitzung zugeordnete Quellenadresse

Source Port
Der dieser Sitzung zugeordnete Quellenanschluß

IPv6 Flow Identifier
Die IPv6-Ablaufkennung für diese Sitzung

Previous Hop Address
Die IP-Adresse des vorherigen Hops

Previous Hop Logical Interface Handle
Die logische Schnittstellenkennung des vorherigen Hops

Last Interface Index
Der letzte Schnittstellenindex

Average BPS
Die durchschnittliche Verbindungsgeschwindigkeit dieser Sitzung in Bit pro Sekunde

Peak BPS Die Spitzenverbindungsgeschwindigkeit dieser Sitzung in Bit pro Sekunde

Maximum Expected Bytes
Die maximale Anzahl der über diese Verbindung erwarteten Byte

Minimum Message Size
Die minimale Nachrichtengröße, die für diese Sitzung verwendet wird

Maximum Message Size
Die maximale Nachrichtengröße, die für diese Sitzung verwendet wird

Refresh Message Interval
Das Intervall, in dem Aktualisierungsnachrichten für diese Sitzung gesendet werden

Previous Hop Is RSVP
Gibt an, ob der vorherige Hop ein RSVP-Hop war

Path Message Last Change
Der Zeitpunkt, an dem die Pfadnachricht zuletzt geändert wurde

Policy Die diesem Sender zugeordnete Policy

Last TTL Value
Der letzte für diese Sitzung verwendete TTL-Wert (Time to Live)

Non-IS Hop Detected
Gibt an, ob ein Nicht-IS-Hop für diese Sitzung festgestellt wurde

Hop Count
Die Hop-Anzahl für diese Sitzung

Path Bandwidth
Die Pfadbandbreite

Minimum Path Latency
Die minimale Pfadlatenzzeit

Maximum Transmission Unit
Die Größe der maximalen Übertragungseinheit (MTU) für diese Sitzung

Guaranteed Service
Gibt an, ob der Service für diese Sitzung garantiert ist

Break In Service
Gibt an, ob der Service in dieser Sitzung unterbrochen wurde

Hop Count Override
Die Überschreibung der Hop-Anzahl für diese Sitzung

Path Bandwidth Override
Die Überschreibung der Pfadbandbreite für diese Sitzung

Minimum Path Latency Override
Die Überschreibung der minimalen Pfadlatenzzeit für diese Sitzung

Maximum Transmission Unit Override
Die Überschreibung der maximalen Übertragungseinheit für diese Sitzung

Anzeige "Upstream RESV Messages"

Diese Anzeige liefert Informationen zu übergeordneten RESV-Nachrichten für die ausgewählte Sitzung. Sie enthält die folgenden Felder:

Session Index
Der Index der Sitzung

Request Index
Der Index der Anforderung

Session Type
Die Sitzungsart

IP Protocol
Das für diese Sitzung verwendete IP-Protokoll

Destination Address
Die dieser Sitzung zugeordnete Zieladresse

Destination Port
Der dieser Sitzung zugeordnete Zielanschluß

Source Address
Die dieser Sitzung zugeordnete Quellenadresse

Source Port
Der dieser Sitzung zugeordnete Quellenanschluß

Previous Hop Address
Die IP-Adresse des vorherigen Hops

Previous Hop Logical Interface Handle
Die logische Schnittstellenkennung des vorherigen Hops

Last Interface Index
Der letzte Schnittstellenindex

Quality of Service
Die Qualität der für diese Sitzung angeforderte Serviceklassifikation

Average BPS
Die durchschnittliche Geschwindigkeit dieser Verbindung in Bit pro Sekunde

Peak BPS Die Spitzengeschwindigkeit dieser Verbindung in Bit pro Sekunde

Maximum Expected Bytes
Die maximale Anzahl der über diese Verbindung erwarteten Byte

Minimum Message Size
Die minimale Nachrichtengröße, die für diese Verbindung verwendet wird

Maximum Message Size
Die maximale Nachrichtengröße, die für diese Verbindung verwendet wird

Refresh Message Interval
Das Nachrichtenaktualisierungsintervall für diese Verbindung

Scope Der Wert des Bereichsobjekts

Shared Reservation
Der Anzeiger für gemeinsame Reservierung

Explicit Senders
Der Anzeiger für explizite Sender

Next Hop Is RSVP Hop
Gibt an, ob der nächste Hop ein RSVP-Hop ist

Last Change
Der Zeitpunkt der letzten Änderung

Policy Die dieser Anforderung zugeordnete Policy

Last TTL Value
Der letzte empfangene TTL-Wert (Time To Live)

IPv6 Flow Identifier
Die IPv6-Ablaufkennung

VPN Monitor-Ordner "Policies"

Dieser Ordner enthält Informationen zu Policies, mit denen VPN-Verbindungen gesteuert werden. Er enthält die folgenden abhängigen Objekte:

- Ordner **Device**
- Ordner **Conditions**
- Ordner **Actions**

Ordner "Device"

Der Ordner **Device** liefert Informationen zu den Policies, die für eine ausgewählte Einheit erstellt wurden. Er enthält die folgenden Anzeigen:

- Policies
- Filter Rules
- Policy to Rule

Der Ordner **Device** stellt für alle drei Anzeigen der Policy-Informationen die gleichen Felder bereit:

Policy Name
Der Name der Policy

Status Der Status der Policy: **enable** (aktivieren) oder **disable** (inaktivieren). Berechtigte Benutzer können diesen Wert in der Anzeige **Policies** ändern.

Priority Die Priorität der Policy

Validity Der Gültigkeitsanzeiger für die Policy

IPSec Manual ID
Die ID des manuell konfigurierten IPSec-Tunnels

Matches Die Anzahl Übereinstimmungen für diese Policy

Validity Period
Der Name der Gültigkeitsperiode für diese Policy

Traffic Profile
Der Name des Datenverkehrsprofils für diese Policy

Key Management Action
Der Name der Schlüsselmanagementaktion für diese Policy

Data Management Action
Der Name der Datenmanagementaktion für diese Policy

Differential Services Action
Der Name der serviceabhängigen Maßnahme für diese Policy

RSVP Action
Der Name der RSVP-Aktion für diese Policy

Ordner "Conditions"

Der Ordner **Conditions** liefert Informationen zu Gültigkeitsperioden und Policy-Aktionen für eine ausgewählte Policy. Er enthält die folgenden abhängigen Objekte:

- Anzeige **Validity Periods**
- Ordner **Traffic Profiles**

Anzeige "Validity Periods"

Die Anzeige **Validity Periods** listet alle Definitionen von Gültigkeitsperioden auf. Sie enthält die folgenden Felder:

Validity Period Name
Der Name der Gültigkeitsperiode

Start Date and Time
Das Startdatum und die Startzeit für die Gültigkeitsperiode

End Date and Time
Das Enddatum und die Endzeit für die Gültigkeitsperiode

Month Mask
Die zum Festlegen der Monate für die Gültigkeitsperiode verwendete Maske

Days Mask
Die zum Festlegen der Tage für die Gültigkeitsperiode verwendete Maske

Start Time of Day
Die Startzeit des Tags für die Gültigkeitsperiode

End Time of Day
Die Endzeit des Tags für die Gültigkeitsperiode

Ordner "Traffic Profiles"

Der Ordner **Traffic Profiles** liefert Informationen zu den Datenverkehrsprofilen, die einer Policy zugeordnet sind. Er enthält die folgenden Anzeigen:

- Base Profiles
- Ingress/Egress Profiles
- Remote ID Profiles

Anzeige "Base Profiles": Die Anzeige **Base Profiles** liefert Informationen zu den Basisprofilen, die einer Policy zugeordnet sind. Sie enthält die folgenden Felder:

Traffic Profile Name
Der Name des Datenverkehrsprofils

Low Protocol
Die niedrige Protokollnummer

High Protocol
Die hohe Protokollnummer

Source Low IP Address
Die niedrige Quellen-IP-Adresse, die diesem Profil zugeordnet ist

Source High IP Address
Die hohe Quellen-IP-Adresse, die diesem Profil zugeordnet ist

Source High Port
Der diesem Profil zugeordnete hohe Anschluß

Source Low Port
Der diesem Profil zugeordnete niedrige Anschluß

Destination of Low IP Address
Die niedrige Ziel-IP-Adresse

Destination of High IP Address
Die hohe Ziel-IP-Adresse

Destination Low Port
Die niedrige Zielanschlußnummer

Destination High Port
Die hohe Zielanschlußnummer

Type-of-Service Byte Mask
Die TOS-Bytemaske (Type of Service)

Type-of-Service Byte Match
Die TOS-Byteanpassungswert (Type of Service)

Local ID Type
Die Art der lokalen ID

Local ID Value
Der Wert der lokalen ID

Remote ID Group Name
Der Name der fernen ID-Gruppe

Ingress/Egress Profiles: Diese Anzeige liefert Informationen zu Ingress/Egress-Profilen. Sie enthält die folgenden Felder:

Traffic Profile Name
Der Name des Datenverkehrsprofils

Traffic Profile Ingress/Egress Index
Der Index des Schnittstellenpaars

Ingress IP Address
Die IP-Adresse des ankommenden Datenverkehrs

Egress IP Address
Die IP-Adresse des abgehenden Datenverkehrs

Anzeige "Remote ID Profiles": Diese Anzeige liefert Informationen zu den fernen IDs, die einem Datenverkehrsprofil zugeordnet sind. Sie enthält die folgenden Felder:

Traffic Profile Name
Der Name des Datenverkehrsprofils

Traffic Profile Remote Group
Der Name der fernen Gruppe

Index Der Index der fernen ID

Type Die Art der fernen ID

Value Der Wert der fernen ID

Authentication Mode
Der für diese ferne ID verwendete Authentifizierungsmodus

Ordner "Actions"

Dieser Ordner liefert Informationen zum IPSec-Schlüsselmanagement, zum IPSec-Datenmanagement, zu serviceabhängigen Policies und zum Ressourcenreservierungsprotokoll (RSVP). Er enthält die folgenden abhängigen Objekte:

- Ordner **IPSec**
- Anzeige **Differential Services**
- Anzeige **RSVP**

Ordner "IPSec": Der Ordner **IPSec** liefert Informationen zum IPSec-Schlüsselmanagement und zum IPSec-Datenmanagement. Er enthält die folgenden abhängigen Objekte:

- Ordner **Key Management**
- Ordner **Data Management**

Ordner "Key Management": Der Ordner **Key Management** liefert Informationen zum IPSec-Schlüsselmanagement. Er enthält die folgenden Anzeigen:

- Actions
- Proposals
- Actions-to-Proposals
- Active Instances

Anzeige "Actions": Die Anzeige **Actions** liefert Informationen zu Schlüsselmanagementaktionen. Sie enthält die folgenden Felder:

Key Management Action Name
Der Name der Schlüsselmanagementaktion

Exchange Mode
Der Austauschmodus

Connection SA Lifetime
Die Lebensdauer der Sicherheitszuordnung für die Verbindung in Sekunden

Connection SA Lifesize
Die Datenmenge der Sicherheitszuordnung für die Verbindung in Kilobyte

Policy Role
Die Policy-Berechtigungsklasse

Minimum Percent Refresh
Der minimale Aktualisierungsprozentsatz der Sicherheitszuordnung

Auto Start Der Anzeiger für automatisches Starten: **true** (wahr) oder **false** (falsch)

Matches Die Anzahl Übereinstimmungen für diese Aktion

Anzeige "Proposals": Diese Anzeige liefert Informationen zu Schlüsselmanagementangeboten. Sie enthält die folgenden Felder:

Key Management Proposal Name
Der Name des Schlüsselmanagementangebots

Authentication Method
Die für dieses Angebot verwendete Authentifizierungsmethode

Hash Algorithm
Der Name des Hash-Algorithmus, der für dieses Angebot verwendetet wird

Cipher Algorithm
Der Name des Cipher-Algorithmus, der für dieses Angebot verwendetet wird

Diffie Hellman Group ID
Die Diffie-Hellman-Gruppen-ID dieses Angebots

SA Lifetime
Die Lebensdauer der Sicherheitszuordnung in Sekunden

SA Lifesize
Die Datenmenge der Sicherheitszuordnung in Kilobyte

Anzeige "Actions-To-Proposals": Diese Anzeige liefert Informationen zu Schlüsselaktionen und Schlüsselangeboten. Sie enthält die folgenden Felder:

Key Management Action Name
Der Name der Schlüsselmanagementaktion

Proposal Name
Der Name des Schlüsselmanagementangebots

Proposal Order
Die Anordnung des Schlüsselmanagementangebots

Action Details
Eine Zusammenfassung der Informationen in der Anzeige **Actions**. Weitere Informationen finden Sie in „Anzeige "Actions"“ auf Seite 56.

Proposal Details
Eine Zusammenfassung der Informationen in der Anzeige **Proposals**. Weitere Informationen finden Sie in „Anzeige "Proposals"“ auf Seite 57.

Anzeige "Active Instances": Diese Anzeige liefert Informationen zu aktiven Schlüsselmanagementinstanzen. Sie enthält die folgenden Felder:

Action Name
Der Name der Schlüsselmanagementaktion

Create Order
Die Anordnung, in der diese Aktion erstellt wurde

KM Tunnel ID
Die Tunnel-ID des Schlüsselmanagements

KM Tunnel Index
Der Tunnelindex des Schlüsselmanagements

Action Details
Eine Zusammenfassung der Informationen in der Anzeige **Actions**. Weitere Informationen finden Sie in „Anzeige "Actions"“ auf Seite 56.

Status Der Status des aktiven Tunnels: **active** (aktiv) oder **destroy** (löschen). Berechtigte Benutzer können diesen Wert in der Anzeige **Active Instances** ändern.

Ordner "IPSec Data Management": Dieser Ordner liefert Informationen zum IPSec-Datenmanagement. Er enthält die folgenden abhängigen Objekte:

- Anzeige **Actions**
- Anzeige **Proposals**
- Anzeige **Active Instances**
- Ordner **Transforms**
- Ordner **Correlations**

Anzeige "Actions": Diese Anzeige liefert Informationen zu IPSec-Datenmanagementaktionen. Sie enthält die folgenden Felder:

Data Management Action Name
Der Name der Datenmanagementaktion

Type Die Art der Aktion: **permit** (zulassen) oder **deny** (verweigern)

Tunnel Start IP Address
Die Start-IP-Adresse des Tunnels

Tunnel End IP Address
Die End-IP-Adresse des Tunnels

Local Proxy Type
Die Art des lokalen Proxy

Local Proxy Value
Der Wert des lokalen Proxy

Local Proxy Protocol
Das Protokoll des lokalen Proxy

Local Proxy Source Port
Die Anschlußnummer der lokalen Proxy-Quelle

Remote Proxy Type
Die Art des fernen Proxy

Remote Proxy Value
Der Wert des fernen Proxy

Remote Proxy Protocol
Das Protokoll des fernen Proxy

Remote Proxy Source Port
Die Anschlußnummer der fernen Proxy-Quelle

SA Refresh Threshold Percent
Der Aktualisierungsschwellenwert der Sicherheitszuordnung

Minimum SA Refresh Threshold Percent
Der minimale Aktualisierungsschwellenwert der Sicherheitszuordnung

Tunnel-In-Tunnel
Der Tunnel-in-Tunnel-Anzeiger

Auto Start Die Einstellung für automatisches Starten: **enable** (aktivieren) oder **disable** (inaktivieren)

Don't Fragment Bit Handling
Der Anzeiger für das Nichtfragmentieren von Bit

Replay Prevention
Die Einstellung für das Verhindern von Wiederholungen

Matches Die Anzahl Übereinstimmungen für diese Aktion

Anzeige "Proposals": Diese Anzeige liefert Informationen zu Datenmanagementangeboten. Sie enthält die folgenden Felder:

Name Der Name der Datenmanagementaktion

Perfect-Forward-Secrecy
Die Einstellung für absolute vorwärtsgerichtete Sicherheit: **enable** (aktivieren) oder **disable** (inaktivieren)

Diffie Hellman Group ID
Die Diffie-Hellman-Gruppen-ID

Anzeige "Active Instances": Diese Anzeige liefert Informationen zu Datenmanagementinstanzen. Sie enthält die folgenden Felder:

Data Management Action
Der Name der Datenmanagementaktion

Creation Order
Die Anordnung, in der die Datenmanagementaktion erstellt wurde

Key Management Tunnel ID
Die Tunnel-ID des Schlüsselmanagements

Data Management Tunnel Index
Der Tunnelindex des Datenmanagements

Data Management Action Details
Eine Zusammenfassung der Anzeige **Data Management Action**. Weitere Informationen finden Sie in „Anzeige "Actions"“ auf Seite 58.

Key Management Action Details
Eine Zusammenfassung der Anzeige **Key Management Action**. Weitere Informationen finden Sie in „Anzeige "Actions"“ auf Seite 56.

Ordner "Transforms": Dieser Ordner liefert Informationen zu Datenmanagementumsetzungen. Er enthält die folgenden Anzeigen:

- AH Transforms
- ESP Transforms
- IPCOMP Transforms

Anzeige "AH Transforms": Diese Anzeige liefert Informationen zu AH-Umsetzungen (AH - Authentication Header). Sie enthält die folgenden Felder:

AH Transform Name
Der Name für die AH-Umsetzung

Encapsulation Algorithm
Der von der AH-Umsetzung verwendete Kapselungsalgorithmus

Integrity Algorithm
Der von der AH-Umsetzung verwendete Integritätsalgorithmus

SA Lifetime
Die Lebensdauer der Sicherheitszuordnung in Sekunden

SA Lifesize
Die Datenmenge der Sicherheitszuordnung in Kilobyte

Anzeige "ESP Transforms": Diese Anzeige liefert Informationen zu ESP-Umsetzungen (ESP - Encapsulating Security Payload). Sie enthält die folgenden Felder:

ESP Transform Name
Der Name der ESP-Umsetzung

Encapsulation Algorithm
Der von der ESP-Umsetzung verwendete Kapselungsalgorithmus

Integrity Algorithm
Der von der ESP-Umsetzung verwendete Integritätsalgorithmus

SA Lifetime
Die Lebensdauer der Sicherheitszuordnung in Sekunden

SA Lifesize
Die Datenmenge der Sicherheitszuordnung in Kilobyte

Anzeige "IPCOMP Transforms": Diese Anzeige liefert Informationen zu IPCOMP-Umsetzungen. Sie enthält die folgenden Felder:

Name Der Name der IPCOMP-Umsetzung

IPCOMP Algorithm
Der Name des Komprimierungsalgorithmus

IPCOMP Vendor Algorithm
Der Name des Lieferantenalgorithmus

SA Lifetime
Die Lebensdauer der Sicherheitszuordnung in Sekunden

SA Lifesize
Die Datenmenge der Sicherheitszuordnung in Kilobyte

Ordner "Correlation": Dieser Ordner liefert Informationen zur Korrelation zwischen IPSec-Datenmanagementangeboten und aktiven Umsetzungen. Er enthält die folgenden Anzeigen:

- Data Management Proposal Correlation
- AH Correlation
- ESP Correlation
- IPCOMP Correlation

Anzeige "Data Management Proposal Correlation": Diese Anzeige liefert Informationen zu Korrelationen von Datenmanagementangeboten. Sie enthält die folgenden Felder:

Action Name
Der Name der Datenmanagementaktion

Proposal Name
Der Name des Datenmanagementangebots

Proposal Order
Die Anordnung des Datenmanagementangebots

Data Management Action Details
Eine Zusammenfassung der Anzeige **Data Management Actions**. Weitere Informationen finden Sie in „Anzeige "Actions"“ auf Seite 58.

Data Management Proposal Details
Eine Zusammenfassung der Anzeige **Data Management Proposal**. Weitere Informationen finden Sie in „Anzeige "Proposals"“ auf Seite 59.

Anzeige "AH Correlation": Diese Anzeige liefert Informationen zu AH-Korrelationen (AH - Authentication Header). Sie enthält die folgenden Felder:

Proposal Name
Der Name des Datenmanagementangebots

AH Transform Name
Der Name der AH-Umsetzung

AH Transform Order
Die Anordnung der AH-Umsetzung

Data Management Action Details
Eine Zusammenfassung der Anzeige **Data Management Actions**. Weitere Informationen finden Sie in „Anzeige "Actions"“ auf Seite 58.

AH Transform Details
Eine Zusammenfassung der Anzeige **AH Transform**. Siehe „Anzeige "AH Transforms"“ auf Seite 60.

Anzeige "ESP Correlation": Diese Anzeige liefert Informationen zu ESP-Korrelationen (ESP - Encapsulating Security Payload). Sie enthält die folgenden Felder:

Proposal Name
Der Name des Datenmanagementangebots

ESP Transform Name
Der Name der ESP-Umsetzung

ESP Transform Order
Die Anordnung der ESP-Umsetzung

Data Management Action Details
Eine Zusammenfassung der Anzeige **Data Management Actions**. Weitere Informationen finden Sie in „Anzeige "Actions"“ auf Seite 58.

ESP Transform Details
Eine Zusammenfassung der Anzeige **ESP Transform**. Siehe „Anzeige "ESP Transforms"“ auf Seite 61.

Anzeige "IPCOMP Correlation": Diese Anzeige liefert Informationen zu IPCOMP-Korrelationen. Sie enthält die folgenden Felder:

Proposal Name
Der Name des Datenmanagementangebots

IPCOMP Transform Name
Der Name der IPCOMP-Umsetzung

IPCOMP Transform Order
Die Anordnung der IPCOMP-Umsetzung

Data Management Action Details
Eine Zusammenfassung der Anzeige **Data Management Actions**. Weitere Informationen finden Sie in „Anzeige "Actions"“ auf Seite 58.

IPCOMP Transform Details
Eine Zusammenfassung der Anzeige **IPCOMP Transform**. Siehe „Anzeige "IPCOMP Transforms"“ auf Seite 61.

Anzeige "Differential Services Actions": Diese Anzeige listet alle Definitionen von serviceabhängigen Maßnahmen auf. Sie enthält die folgenden Felder:

Differential Services Action Name
Der Name der serviceabhängigen Maßnahme

Permission
Der Berechtigungswert der Aktion: **permit** (zulassen) oder **deny** (verweigern)

Queue Priority
Die Warteschlangenpriorität der Aktion

Bandwidth Type
Die Bandbreitenart der Aktion

Bandwidth Share
Die gemeinsame Benutzung der Bandbreite für die Aktion

TOS Mask Die TOS-Bytemaske (Type of Service)

TOS Match
Die TOS-Byte-Übereinstimmung (Type of Service)

Matches Die Anzahl Übereinstimmungen für diese Aktion

RSVP Actions: Diese Anzeige listet alle Definitionen von RSVP-Aktionen auf. Sie enthält die folgenden Felder:

Name Der Name der RSVP-Aktion

Permission
Der Berechtigungswert der Aktion: **permit** (zulassen) oder **deny** (verweigern)

Max Rate/Flow
Die maximale Geschwindigkeit pro Ablauf in Kilobyte

Max Token-Bucket/Flow
Der maximale Token-Protokollbereich pro Ablauf

Max Flow Duration
Die Dauer des maximalen Ablaufs in Sekunden

Min Delay Die minimale Verzögerung in Sekunden

Differential Services Action
Der Name der serviceabhängigen Maßnahme

Differential Services Action Details
Eine Zusammenfassung der Anzeige **Differential Services Action**. Weitere Informationen finden Sie in „Anzeige "Differential Services Actions"“ auf Seite 63.

VPN Monitor-Ordner "Events"

Der VPN Monitor-Ordner **Events** liefert Informationen zu Ereignisberichten, die von VPN Monitor ausgeführt wurden. Er enthält die folgenden abhängigen Objekte:

- Ordner **Layer-2 Authentication**
- Ordner **IPSec Authentication/Encryption**

Ordner "Layer-2 Authentication"

Dieser Ordner liefert Informationen zu Layer-2-Authentifizierungen, die von der überwachten Einheit ausgeführt wurden. Er enthält die folgenden Anzeigen:

- Statistics
- Tunnel Failure Log
- Session Failure Log

Anzeige "Statistics"

Diese Anzeige liefert Statistiken zu Layer-2-Authentifizierungen, die von der überwachten Einheit ausgeführt wurden. Sie enthält die folgenden Felder:

Tunnel Successes
Die Anzahl der aktivierten Layer-2-Tunnel

Tunnel Failures
Die Anzahl der aufgrund mangelnder Authentifizierung nicht aktivierten Layer-2-Tunnel

Session Successes
Die Anzahl der aktivierten Layer-2-Sitzungen

Session Failures
Die Anzahl der aufgrund mangelnder Authentifizierung nicht aktivierten Layer-2-Sitzungen

Anzeige "Tunnel Failure Log"

Diese Anzeige liefert Informationen zu Layer-2-Tunneln, die nicht authentifiziert und daher nicht geöffnet werden konnten. Sie enthält die folgenden Felder:

Failure Number
Die Fehlernummer

Host Der Host für den fehlgeschlagenen Tunnel

IP Address
Die IP-Adresse für den fehlgeschlagenen Tunnel

Time Der Zeitpunkt, an dem der Fehler auftrat

Anzeige "Session Failure Log"

Diese Anzeige liefert Informationen zu Layer-2-Sitzungen, die nicht authentifiziert und daher nicht geöffnet werden konnten. Sie enthält die folgenden Felder:

Failure Number
Die Fehlernummer

User ID Die dem fehlgeschlagenen Tunnel zugeordnete Benutzer-ID

Time Der Zeitpunkt, an dem der Fehler auftrat

Ordner "IPSec Authentication/Encryption"

Dieser Ordner liefert Informationen zu IPSec-Authentifizierungen und -Verschlüsselungen, die von der überwachten Einheit ausgeführt wurden. Er enthält die folgenden Anzeigen:

- Statistics
- IPSec Failure Log

Anzeige "Statistics"

Diese Anzeige liefert Statistiken für IPSec-Authentifizierungen und -Verschlüsselungen, die von der überwachten Einheit ausgeführt wurden. Sie enthält die folgenden Felder:

In Authentications
Die Anzahl der ausgeführten IPSec-Authentifizierungen ankommender Daten

In Authentication Failures
Die Anzahl der fehlgeschlagenen IPSec-Authentifizierungen ankommender Daten

In Decryptions
Die Anzahl der ausgeführten IPSec-Entschlüsselungen ankommender Daten

In Decryption Failures
Die Anzahl der fehlgeschlagenen IPSec-Entschlüsselungen ankommender Daten

Out Authentications
Die Anzahl der ausgeführten IPSec-Authentifizierungen abgehender Daten

Out Authentication Failures
Die Anzahl der fehlgeschlagenen IPSec-Authentifizierungen abgehender Daten

Out Encryptions
Die Anzahl der ausgeführten IPSec-Entschlüsselungen abgehender Daten

Out Encryptions Failures
Die Anzahl der fehlgeschlagenen IPSec-Entschlüsselungen abgehender Daten

Anzeige "IPSec Failure Log"

Diese Anzeige liefert Informationen zu IPSec-Authentifizierungs- und -Verschlüsselungsfehlern. Sie enthält die folgenden Felder:

Failure Number
Die Fehlernummer

Reason Die Ursache für den Fehler

Time Der Zeitpunkt, an dem der Fehler auftrat

Tunnel ID Die Tunnel-ID des Fehlers

SA SPI Der Sicherheitsschutzindex für die Sicherheitszuordnung des Fehlers

Source IP Address
Die Quellen-IP-Adresse des Fehlers

Destination IP Address
Die Ziel-IP-Adresse des Fehlers

VPN Monitor-Ordner "Operational"

Dieser Ordner liefert Informationen zum Betrieb der überwachten Einheit. Er enthält die folgenden abhängigen Objekte:

- Ordner **Tunnels**
- Ordner **Clients**
- Ordner **Policies**
- Ordner **LDAP**
- Ordner **Traps**

Ordner "Tunnels"

Dieser Ordner stellt das Anzeige- und Betriebsleistungsspektrum für die Größe von Layer-2-Protokolltabellen, aktive Layer-2-Tunnel, aktive IPSec-Steuertunnel und aktive IPSec-Benutzertunnel bereit. Er enthält die folgenden Anzeigen:

- Table Size
- Inactivate Layer-2 Tunnels
- Inactivate IPSec Control Tunnels
- Inactivate IPSec User Tunnels

Anzeige "Table Size"

Diese Anzeige liefert Informationen zur Größe von Layer-2-Protokolltabellen. Sie enthält die folgenden Felder:

Layer-2 History Tables
Die Anzahl der Einträge, die für vorherige Layer-2-Tunnel und -Sitzungen aufbewahrt werden sollen. Berechtigte Benutzer können diesen Wert in der Anzeige **Table Size** ändern.

Layer-2 Authentication Failure Tables
Die Anzahl der Einträge, die in der Tabelle für Layer-2-Authentifizierungsfehler aufbewahrt werden sollen. Berechtigte Benutzer können diesen Wert in der Anzeige **Table Size** ändern.

Anzeige "Inactivate Layer-2 Tunnels"

In dieser Anzeige können berechtigte Benutzer Layer-2-Tunnel inaktivieren. Sie enthält die folgenden Felder:

Active Layer-2 Tunnels Details
Eine Zusammenfassung der Anzeige **Active Layer-2 Tunnels**

Status Der Auslöser zum Löschen eines einzelnen Tunnels. Berechtigte Benutzer können diesen Wert in der Anzeige **Inactivate Layer-2 Tunnels** ändern.

Destroy All Tunnels
Der Auslöser zum Löschen aller Tunnel. Berechtigte Benutzer können diesen Wert in der Anzeige **Inactivate Layer-2 Tunnels** ändern.

Anzeige "Inactivate IPSec Control Tunnels"

In dieser Anzeige können berechtigte Benutzer IPSec-Steuertunnel inaktivieren. Sie enthält die folgenden Felder:

Active IPSec Control Tunnel Details
Eine Zusammenfassung der Anzeige **Active IPSec Control Tunnels**

Status Der Auslöser zum Löschen eines einzelnen Tunnels. Berechtigte Benutzer können diesen Wert in der Anzeige **Inactivate IPSec Control Tunnels** ändern.

Destroy All Tunnels
Der Auslöser zum Löschen aller Tunnel. Berechtigte Benutzer können diesen Wert in der Anzeige **Inactivate IPSec Control Tunnels** ändern.

Anzeige "Inactivate IPSec User Tunnels"

In dieser Anzeige können berechtigte Benutzer IPSec-Benutzertunnel inaktivieren. Sie enthält die folgenden Felder:

Active IPSec User Tunnel Details
Eine Zusammenfassung der Anzeige **Active IPSec User Tunnels**

Status Der Auslöser zum Löschen eines einzelnen Tunnels. Berechtigte Benutzer können diesen Wert in der Anzeige **Inactivate IPSec User Tunnels** ändern.

Destroy All Tunnels
Der Auslöser zum Löschen aller Tunnel. Berechtigte Benutzer können diesen Wert in der Anzeige **Inactivate IPSec User Tunnels** ändern.

Ordner "Clients"

Dieser Ordner stellt das Anzeige- und Steuerleistungsspektrum für Layer-2-Sitzungen bereit. Er enthält die folgende Anzeige:

- Inactivate Layer-2 Sessions

Anzeige "Inactivate Layer-2 Sessions"

In dieser Anzeige können berechtigte Benutzer Layer-2-Sitzungen inaktivieren. Sie enthält die folgenden Felder:

Active Layer-2 Sessions Details
Eine Zusammenfassung der Anzeige **Active Layer-2 Sessions**

Status Der Auslöser zum Löschen einer Einzelsitzung. Berechtigte Benutzer können diesen Wert in der Anzeige **Inactivate Layer-2 Sessions** ändern.

Destroy All sessions
Der Auslöser zum Löschen aller Sitzungen. Berechtigte Benutzer können diesen Wert in der Anzeige **Inactivate Layer-2 Sessions** ändern.

Ordner "Policies"

Dieser Ordner stellt das Anzeige- und Steuerleistungsspektrum für VPN-Einheiten-Policies bereit. Er enthält die folgenden Anzeigen:

- Enable/Disable Policies
- Reload Device Policies

Anzeige "Enable/Disable Policies"

In dieser Anzeige können Benutzer eine ausgewählte Einheiten-Policy aktivieren bzw. inaktivieren. Sie enthält die folgenden Felder:

Policy Details
Eine Zusammenfassung der Anzeige **Policies**

Status Der Auslöser zum Aktivieren bzw. Inaktivieren einer Policy. Berechtigte Benutzer können diesen Wert in dieser Anzeige ändern.

Anzeige "Reload Device Policies"

In dieser Anzeige können Benutzer die für eine überwachte Einheit verwendeten Policies erneut laden. Sie enthält die folgenden Felder:

Administrative Definition Details
Eine Zusammenfassung der LDAP-Definitionen (LDAP - Lightweight Directory Access Protocol). Weitere Informationen finden Sie in „Anzeige "Administrative Parameters"“ auf Seite 72.

Operational Definition Details
Eine Zusammenfassung der LDAP-Betriebsdefinitionen. Weitere Informationen finden Sie in „Anzeige "Operational Parameters"“ auf Seite 71.

Reload Policies
Der Auslöser zum erneuten Laden von Policies. Berechtigte Benutzer können in dieser Anzeige Policies erneut laden.

Ordner "LDAP"

Dieser Ordner stellt das Anzeige- und Steuerleistungsspektrum für die LDAP-Parameter (LDAP - Lightweight Directory Access Protocol) bereit. Er enthält die folgenden Anzeigen:

- Operational Parameters
- Administrative Parameters

Anzeige "Operational Parameters"

Diese Anzeige liefert Informationen zu LDAP-Verarbeitungsparametern. Sie enthält die folgenden Felder:

Status Der Status der Definition: **enable** (aktivieren) oder **disable** (inaktivieren)

Primary LDAP Server IP Address
Die IP-Adresse des primären LDAP-Servers

Secondary LDAP Server IP Address
Die IP-Adresse des sekundären LDAP-Servers

LDAP Server Level
Die Ebene des LDAP-Servers

Policy Base Name
Der Name des Policy-Basisobjekts für die Einheit

Port Die vom LDAP-Server verwendete Anschlußnummer

Timeout Der vom LDAP-Server verwendete Zeitlimitüberschreitungswert

Retry Interval
Das vom LDAP-Server verwendete Wiederholungsintervall

User ID Die Benutzer-ID des LDAP-Servers

Anzeige "Administrative Parameters"

Mit dieser Anzeige können die LDAP-Parameter gesteuert werden. Sie enthält die gleichen Felder wie die Anzeige **Operational Parameters**. Jedoch können berechtigte Benutzer den Wert eines beliebigen Parameters in dieser Anzeige ändern.

Ordner "Traps"

Dieser Ordner stellt das Anzeige- und Steuerleistungsspektrum für VPN-Alarmnachrichten bereit. Er enthält die folgenden Anzeigen:

- Layer-2 Trap Control
- IPSec Trap Control

Anzeige "Layer-2 Trap Control"

Diese Anzeige liefert Informationen zu Layer-2-Alarmnachrichten für die ausgewählte Einheit und ermöglicht die Steuerung dieser Nachrichten. Berechtigte Benutzer können die Werte aller Felder in dieser Anzeige ändern. Die Anzeige **Layer-2 Trap Control** enthält die folgenden Felder:

Tunnel Start Traps
Der Status der Verarbeitung von Alarmnachrichten, die beim Tunnelstart ausgegeben werden: **enable** (aktivieren) oder **disable** (inaktivieren)

Tunnel Stop Traps
Der Status der Verarbeitung von Alarmnachrichten die beim Tunnelstopp ausgegeben werden: **enable** (aktivieren) oder **disable** (inaktivieren)

Tunnel Authentication Failure Traps
Der Status der Verarbeitung von Alarmnachrichten, die bei Tunnelauthentifizierungsfehlern ausgegeben werden: **enable** (aktivieren) oder **disable** (inaktivieren)

User Authentication Failure Traps
Der Status der Verarbeitung von Alarmnachrichten, die bei Benutzerauthentifizierungsfehlern ausgegeben werden: **enable** (aktivieren) oder **disable** (inaktivieren)

Anzeige "IPSec Trap Control"

Diese Anzeige liefert Informationen zu IPSec-Alarmnachrichten für die ausgewählte Einheit und ermöglicht die Steuerung dieser Nachrichten. Berechtigte Benutzer können die Werte aller Felder in dieser Anzeige ändern. Die Anzeige **IPSec Trap Control** enthält die folgenden Felder:

Control Tunnel Start Traps
Der Status der Verarbeitung von Alarmnachrichten, die beim Steuertunnelstart ausgegeben werden: **enable** (aktivieren) oder **disable** (inaktivieren)

Control Tunnel Stop Traps
Der Status der Verarbeitung von Alarmnachrichten, die beim Steuertunnelstopp ausgegeben werden: **enable** (aktivieren) oder **disable** (inaktivieren)

User-Data Tunnel Start Traps
Der Status der Verarbeitung von Alarmnachrichten, die beim Benutzerdatentunnelstart ausgegeben werden: **enable** (aktivieren) oder **disable** (inaktivieren)

User-Data Tunnel Stop Traps
Der Status der Verarbeitung von Alarmnachrichten, die beim Benutzerdatentunnelstopp ausgegeben werden: **enable** (aktivieren) oder **disable** (inaktivieren)

Authentication Failure Traps
Der Status der Verarbeitung von Alarmnachrichten, die bei Authentifizierungsfehlern ausgegeben werden: **enable** (aktivieren) oder **disable** (inaktivieren)

Decryption Failure Traps
Der Status der Verarbeitung von Alarmnachrichten, die bei Entschlüsselungsfehlern ausgegeben werden: **enable** (aktivieren) oder **disable** (inaktivieren)

VPN Monitor-Ordner "Tests"

Mit diesem Ordner können Benutzer die Policies, Konnektivität und Antwortzeit zu und von Hosts testen. Er enthält die folgenden abhängigen Objekte:

- Anzeige **Policy Test**
- Ordner **Layer-2 Tests**
- Anzeige **Remote Ping**

Anzeige "Policy Test"

In dieser Anzeige können Sie Policy-Tests ausführen und die Ergebnisse prüfen. Beim Start eines Tests können Sie die Quellen- und Zieladressen, Quellen- und Zielanschlüsse, das zu verwendende Protokoll und die Art des angeforderten Services angeben. Nach dem Testende werden die ausgewählten Policies und Aktionen angezeigt. Die Anzeige **Policy Test** enthält die folgenden Felder:

Test Index
Der Index des Tests

Result Das Ergebnis des Tests

Status Der Status des Testeintrags

Source IP Address
Die im Test zu verwendende Quellen-IP-Adresse. Sie können diesen Wert hier ändern.

Source Port
Der im Test zu verwendende Quellenanschluß. Sie können diesen Wert hier ändern.

Destination IP Address
Die im Test zu verwendende Ziel-IP-Adresse. Sie können diesen Wert hier ändern.

Destination Port
Der im Test zu verwendende Zielanschluß. Sie können diesen Wert hier ändern.

Protocol Das im Test zu verwendende Protokoll. Sie können diesen Wert hier ändern.

TOS Byte Das im Test zu verwendende TOS-Byte (Type Of Service). Sie können diesen Wert hier ändern.

Key Management Policy
Die ausgewählte Schlüsselmanagement-Policy

Key Management Action
Die ausgewählte Schlüsselmanagementaktion

Data Management Policy
Die ausgewählte Datenmanagement-Policy

Data Management Action
Die ausgewählte Datenmanagementaktion

Diff Services Policy
Die ausgewählte serviceabhängige Policy

Diff Services Action
Die ausgewählte serviceabhängige Maßnahme

RSVP Policy
Die ausgewählte RSVP-Policy

RSVP Action
Die ausgewählte RSVP-Aktion

Ordner "Layer-2 Tests"

Mit diesem Ordner können Sie die Konnektivität und Antwortzeit für Layer-2-Tunnel testen. Er enthält die folgenden Anzeigen:

- Layer-2 Connection Test
- Layer-2 Response Time Test

Anzeige "Layer-2 Connection Test"

In dieser Anzeige können Sie die potentielle Layer-2-Konnektivität zu einem Host testen. Wählen Sie den Namen eines potentiellen Hosts aus, um den Test zu starten. Nach dem Testende wird die Verfügbarkeit der Verbindung angezeigt. Diese Anzeige enthält die folgenden Felder:

Test Index
Der Index des Tests

Host Der Host, dessen Konnektivität getestet werden soll. Sie können diesen Wert hier ändern.

Result Das Ergebnis des Tests

Tunnel Type
Die für den Test verwendete Tunnelart

Anzeige "Layer-2 Response Time Test"

In dieser Anzeige können Sie die Antwortzeit eines aktiven Hosts testen. Wählen Sie den Namen eines aktiven Hosts aus, um den Test zu starten. Nach dem Testende wird die Umlaufzeit eines Pakets zum ausgewählten Host angezeigt. Diese Anzeige enthält die folgenden Felder:

Test Index
Der Index des Tests

Host Der Host, dessen Konnektivität getestet werden soll. Sie können diesen Wert hier ändern.

Result Das Ergebnis des Tests

Round Trip Time
Die Umlaufzeit des Testpakets

Anzeige "Remote Ping"

In dieser Anzeige können Sie die Antwortzeit von der aktuellen VPN-Einheit zu einer anderen Einheit testen. Geben Sie die IP-Adresse des fernen Hosts, die Paketgröße und den Zeitlimitüberschreitungswert an, die für den Test verwendet werden sollen, um Ping zu starten. Nach dem Testende wird die Umlaufzeit eines Pakets zum Host angezeigt. Diese Anzeige enthält die folgenden Felder:

IP Address
Die mit Ping zu überprüfende IP-Adresse. Sie können diesen Wert hier ändern.

Packet Size
Die für Ping zu verwendende Paketgröße. Sie können diesen Wert hier ändern.

Timeout Value
Der für Ping zu verwendende Zeitlimitüberschreitungswert. Sie können diesen Wert hier ändern.

Result Das Ping-Ergebnis

Ping Time Die Umlaufzeit des Tests

Anhang A. Bemerkungen

Die vorliegenden Informationen wurden für Produkte und Services entwickelt, die auf dem deutschen Markt angeboten werden. Möglicherweise bietet IBM die in dieser Dokumentation beschriebenen Produkte, Services oder Funktionen in anderen Ländern nicht an. Informationen über die gegenwärtig im jeweiligen Land verfügbaren Produkte und Services sind beim IBM Ansprechpartner erhältlich.

Hinweise auf IBM Produkte, Programme oder Dienstleistungen in dieser Veröffentlichung bedeuten nicht, daß IBM diese in allen Ländern, in denen IBM vertreten ist, anbietet. Hinweise auf IBM Lizenzprogramme oder andere IBM Produkte bedeuten nicht, daß nur Programme, Produkte oder Dienstleistungen von IBM verwendet werden können. Anstelle der IBM Produkte, Programme oder Dienstleistungen können auch andere ihnen äquivalente Produkte, Programme oder Dienstleistungen verwendet werden, solange diese keine gewerblichen Schutzrechte der IBM verletzen. Die Verantwortung für den Betrieb der Produkte in Verbindung mit Fremdprodukten liegt beim Kunden, soweit solche Verbindungen nicht ausdrücklich von IBM bestätigt sind.

Für in diesem Handbuch beschriebene Erzeugnisse und Verfahren kann es IBM Patente oder Patentanmeldungen geben. Mit der Auslieferung dieses Handbuchs ist keine Lizenzierung dieser Patente verbunden. Lizenzanfragen sind schriftlich an IBM Europe, Director of Licensing, 92066 Paris La Defense Cedex, France, zu richten. Anfragen an obige Adresse müssen auf englisch formuliert werden.

Trotz sorgfältiger Bearbeitung können technische Ungenauigkeiten oder Druckfehler in dieser Veröffentlichung nicht ausgeschlossen werden. Die Angaben in diesem Handbuch werden in regelmäßigen Zeitabständen aktualisiert. Die Änderungen werden in Überarbeitungen oder in Technical News Letters (TNLs) bekanntgegeben. IBM kann jederzeit ohne Vorankündigung Verbesserungen und/oder Änderungen an den in dieser Veröffentlichung beschriebenen Produkten und/oder Programmen vornehmen.

Verweise in dieser Veröffentlichung auf Web-Sites anderer Anbieter dienen lediglich als Benutzerinformationen und stellen keinerlei Billigung des Inhalts dieser Web-Sites dar. Das über diese Web-Sites verfügbare Material ist nicht Bestandteil des Materials für dieses IBM Produkt. Die Verwendung dieser Web-Sites geschieht auf eigene Verantwortung.

Marken

Folgende Namen sind in gewissen Ländern Marken der IBM Corporation:

DB2	IBM
Nways	DB2 Universal Database

Java und alle auf Java basierenden Marken und Logos sind in gewissen Ländern Marken oder eingetragene Marken von Sun Microsystems, Inc.

Microsoft, Windows, Windows NT und die Logos von Windows 95 und Windows 98 sind Marken der Microsoft Corporation.

Pentium ist in gewissen Ländern eine eingetragene Marke der Intel Corporation.

Netfinity ist in gewissen Ländern eine Marke der IBM Corporation.

UNIX ist eine eingetragene Marke und wird ausschließlich von der X/Open Company Limited lizenziert.

Freelance Graphics ist in gewissen Ländern eine Marke der Lotus Development Corporation.

Andere Namen von Unternehmen, Produkten oder Dienstleistungen können Marken anderer Unternehmen sein.

Antwort

Nways VPB Manager
Benutzerhandbuch

IBM Form GA12-4785-00

Anregungen zur Verbesserung und Ergänzung dieser Veröffentlichung nehmen wir gerne entgegen.
Bitte informieren Sie uns über Fehler, ungenaue Darstellungen oder andere Mängel.

Senden Sie Ihre Anregungen bitte an die angegebene Adresse.

IBM Deutschland
Informationssysteme GmbH
SW NLS Center

70548 Stuttgart

Kommentare:

Zu Ihrer weiteren Information:

Zur Klärung technischer Fragen sowie zu Liefermöglichkeiten und Preisen wenden Sie sich bitte entweder an Ihre *IBM Geschäftsstelle*, Ihren *IBM Geschäftspartner* oder Ihren *Händler*. Unsere Telefonauskunft **„Hallo IBM“** (Telefonnr.: 0180 3/31 32 33) steht Ihnen ebenfalls zur Klärung allgemeiner Fragen zur Verfügung.

GA12-4795-00