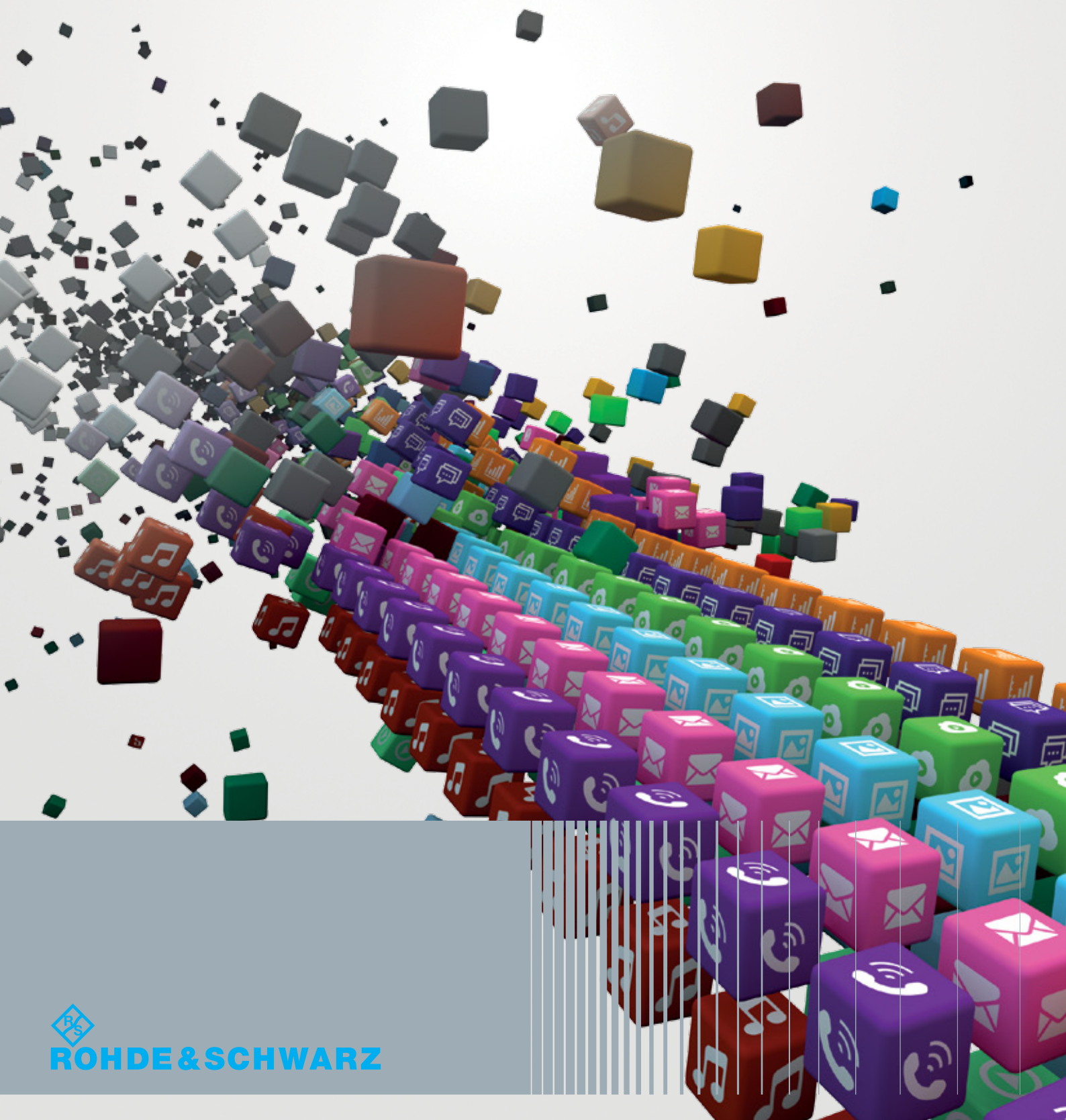


R&S®PACE 2

ソリューション・ガイド



目次

1.概要	3
R&S®PACE 2 の主要な特徴	3
2.OEM ソリューションとしての R&S®PACE 2	4
2.1 組み込み	4
2.2 パフォーマンス	4
3.構成の概要	5
3.1 パケットの準備	5
3.2 パケットの並べ替え	6
3.3 パケットの分類	6
3.4 パケットの復調	6
3.5 タイムアウト処理	6
4.プロトコルおよびアプリケーションの分類	7
5.分類確度の保証	9
6.暗号化の処理	10
7.メタデータの抽出	11
7.1 パフォーマンス・メタデータ	11
7.2 プロトコルおよびアプリケーション・メタデータ	12
8.コンテンツ復調	13
9.追加機能	14
9.1 動的なアップグレード	14
9.2 OS 検出	14
9.3 NAT/テザリング検出	14
9.4 クライアント・サーバ表示	14
9.5 一方向トラフィックのサポート	14
9.6 カスタマイズ	14
9.7 高速パス	14
10.パフォーマンス・テスト	15
10.1 テスト・データ	15
10.2 シングル・スレッド・テスト	15
11.サービスとサポート	16
11.1 製品評価	16
11.2 保守	16
11.3 顧客ポータル	16
11.4 トレーニング	16
12.ユース・ケース	17
12.1 ネットワークとトラフィックの管理 (QoS/QoE)	17
12.2 ポリシー制御と課金	17
12.3 ネットワーク・セキュリティ (ファイアウォール、IPS/IDS、SIEM、UTM)	18
12.4 ネットワークとサブスクリバの解析	18
12.5 モバイル・データ・オフロード	18
12.6 WAN の最適化	19
12.7 SDN/NFV 環境	19

1.概要

ネットワーク・インフラストラクチャ／セキュリティ・ベンダは、アプリケーションとIPネットワーク・トラフィックの理解を深める必要性が高まっています。モバイル・アプリ、クラウド・コンピューティング、ビデオ・トラフィックの高度成長と相まって、LTEモバイル・ネットワークへの移行にはこのネットワークの可視性が重要です。ベンダは、パフォーマンス管理、エンド・ユーザ・エクスペリエンス、および端末間のアプリケーションのセキュリティを改善するために、ソリューションにリアルタイム・アプリケーション認識を組み込んでいます。

ベンダが R&S®PACE 2 ソリューションを組み込むことで、製品に最先端のプロトコルおよびアプリケーション認識機能を搭載することができます。

R&S®PACE 2 は、ディープ・パケット・インスペクション、振る舞い解析、ヒューリスティック解析、統計的解析などのさまざまな技術を使用するソフトウェア・ライブラリです。ネットワーク・プロトコルおよびアプリケーションを確実に検出し、リアルタイムでメタデータを抽出することができます。R&S®PACE 2 は、高度な難読化技術や暗号化技術が使用されている場合でも、ネットワーク・プロトコルおよびアプリケーションを正確に検出することができます。ネットワーク設備／セキュリティ・ベンダが R&S®PACE 2 を組み込むことで、製品に最先端のプロトコルおよびアプリケーション認識機能を搭載することができます。R&S®PACE 2 は、第 7 層のプロトコルとアプリケーションの認識に関する長年の経験に基づいて設計されました。ネットワーク・セキュリティ (IDS/IPS、次世代ファイアウォール、SIEM、UTM)、ネットワーク・モニタリングとトラフィックの管理、ポリシーと課金、アプリケーションの配信と最適化、解析、およびモバイル・データ・オフロードを含む多様なユース・ケースに展開することができます。

R&S®PACE 2 の主要な特徴

- 製品化までの時間とコスト削減 - 更新と保守を含めた R&S®PACE ソフトウェアのライセンスを受けることで、開発期間、CapEx、および OpEx が削減されます。
- 容易で時間のかからない組み込み - 非常に柔軟な組み込み用 API、プラットフォーム非依存、外部依存関係なし。
- 高速パフォーマンス - 1 コアあたり 4Gbps の平均スループット。
- 非常に効率的 - 市場で最も効率的なメモリ消費。
- 確度と信頼性 - ネットワーク・トラフィックの 95% 以上を分類 (偽陽性なし)。
- 有効範囲 - 多様なオペレーティング・システム、アプリケーション・バージョン、サービス・タイプにわたる何千ものプロトコルおよびアプリケーションをサポート。
- メタデータ抽出 - アプリケーション属性のより深い洞察 (例: ネットワーク・パフォーマンスの QoS/QoE KPI、VoIP やビデオなどのアプリケーション)。
- 常に最新の状態を維持 - 分類ライブラリへの追加を含めたシグネチャの頻繁な更新。
- OEM としてグローバルに展開 - アプリケーションの可視性と検出率を向上するグローバル・モバイル・ネットワークで展開されます。

2.OEM ソリュー ションとしての R&S® PACE 2

2.1 組み込み

R&S®PACE 2 ソフトウェアは、プラットフォーム (ハードウェア/ソフトウェア) に依存せず、Linux、Mac、Solaris、および Windows の任意の環境で動作し、C インタフェースを用いてアクセスできます。ソフトウェアは ipoque の技術者が社内で開発したもので、コード・サンプルを含めて完全にドキュメント化された API が搭載されています。ソフトウェア・キットには ipoque の強力なネットワーク・トラフィック・テスト・ツールが付属しています。このツールを使用すると、組み込みの妥当性をダブルチェックし、ユース・ケースをより詳細に理解することができます。

2.2 パフォーマンス

R&S®PACE 2 は、ハイエンド・マルチコア技術に最適化されたコードを含めて、高パフォーマンスを実現するために全体が C で開発されています。マルチスレッド化により、マルチコア・システム上でほぼ線形のスケーラビリティが提供されます。また、何百万もの同時接続をサポートする高度に最適化されたフロー追跡も組み込まれています。

API はコード・サンプルを含めて完全にドキュメント化されており、容易に組み込むことができます。

PACE の概要	
CPU 構成	基本的に制限なし、Intel x86 に最適化
オペレーティング・システム	基本的に制限なし、Linux に最適化
パフォーマンス	1 コアあたり平均 4 Gbps
メタデータ抽出	対応
フル・コンテンツ復調	対応
サービス	専門サービス、設計、構築、実行
プロトコル/アプリケーション対象範囲	2,000 +、約 95% を認識
プロトコル/アプリケーションの更新	頻繁に動的なシグネチャ更新、少なくとも月 1 回
メモリ使用量	ライブラリ: 初期化メモリなし、サブスクリバあたり: 900 B 未満、フローあたり: 400 B 未満
APIs	C

3.構成の概要

R&S®PACE 2では、検出、復調、および関連するパケット処理コンポーネントを統一ライブラリに集約しています。パケット処理とメタデータ抽出にはポーリング API が使用されます。これによってコールバックの必要がなくなり、組み込みが容易になります。フローとサブスクリバの追跡は、ライブラリ内で処理することも、外部で処理することもできます。各段階は、コードを変更せずにパケットの並べ替えやデフラグなどの機能を有効または無効にできるように構成可能です。「パケットの分類」、「パケットの復調」、「タイムアウト処理」の各段階の後、処理のためのメタデータ・イベントのリストが提供されます。「パケットの復調」段階は完全にオプションであり、高度なメタデータ・オプションが不要な場合には呼び出す必要がありません。R&S®PACE 2 のフローは複数の段階に分割されており、順次呼び出されます。各段階は以下の順序で使用されます。

- 1.パケットの準備
- 2.パケットの並べ替え
- 3.パケットの分類
- 4.パケットの復調
- 5.タイムアウト処理

3.1 パケットの準備

パケットの準備はパケットごとの処理で、フレーム・スタックの構築、プロトコルのカプセル化解除、および IP デフラグを行います。出力されるのは、以降の各段階で処理可能な単一のパケットです。

プロトコルのカプセル化解除

R&S®PACE 2 は IP パケットにアクセスする必要があります。以下のコンポーネントが必要となります。

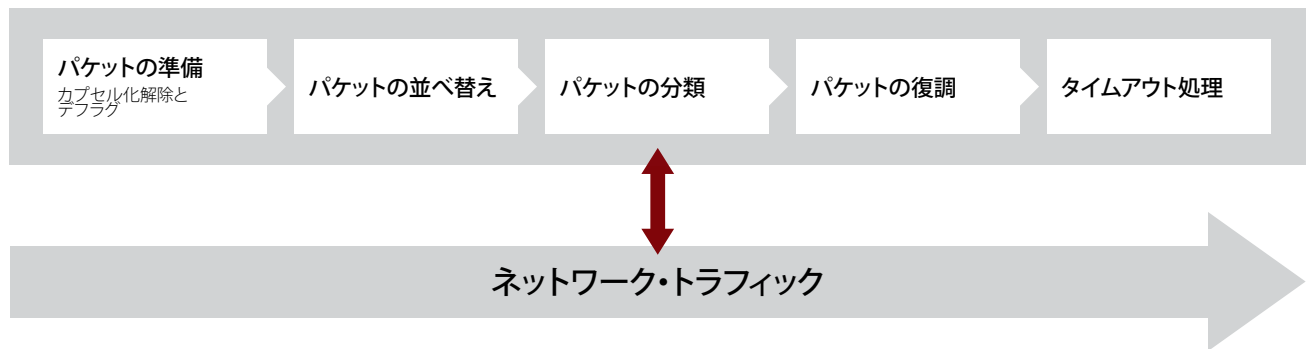
- IP ヘッダへのポインタ
- IP ヘッダから始まるパケットのアクセス可能な長さ
- パケットのタイムスタンプ

IP デフラグ

IP デフラグ・エンジンは、第 3 層から第 7 層への断片化した IP パケットを再構築するために使用されます。パケットの分類では、IP トラフィックのすべてのプロトコルおよびアプリケーションを確実に分類するために、断片化した IP パケットがないことを想定しています。IP デフラグ・エンジンは、検出結果を改善するために重要な IP フローの変換に役立ちます。

R&S®PACE 2 は検出結果の改善に重要な IP パケットを必要に応じて再構築します。

R&S®PACE 2 – IP の分類とメタデータ抽出



3.構成の概要

3.2 パケットの並べ替え

パケット並べ替えエンジンを使用すると、必要に応じてTCPパケットを並べ替えることができます。このエンジンは、欠落したパケットが到着するか一定のタイムアウトが発生するまで、順序逆転パケットをバッファに格納します。パケットの並べ替えによって検出分類率が向上します。

フロー／サブスクライバ追跡

並べ替えが機能するには、この段階を呼び出す前にフロー追跡を実行する必要があります。すべてのTCP/UDPフローの状態が内部の値とともに保持されます。フロー情報を取得するプロセスは以下の3つの段階に分かれます。

1. 第1段階では、一意な5つのタプルを作成する必要があります。
2. 第2段階では、これを接続追跡テーブルに挿入します。
3. 挿入によって新しいエントリが作成された場合、第3段階で0に設定する必要があります。

サブスクライバごとに同様な状態バッファを保持します。ほとんどの場合、サブスクライバは内部IPアドレスで識別されます。

3.3 パケットの分類

パケットの分類の段階では、ネットワーク・パフォーマンス・メタデータに加えて、プロトコルおよびアプリケーション検出結果が得られます。パケットの分類はライブラリのコア・インテリジェンスであり、多数の異なるプロトコルおよびアプリケーション検出が含まれています。

3.4 パケットの復調

パケットの復調では、内容の復調に加えて、詳細なメタデータも得られます。R&S®PACE 2の復調段階を使用する場合は、電子メール全文や圧縮されたHTTPペイロード・コンテンツなど、より詳細なメタデータをリアルタイムで抽出することができます。ICQボディ名、グループ・アクティビティ、送信メッセージなど、ソーシャル・ネットワーク・コンテンツを復調することもできます。

3.5 タイムアウト処理

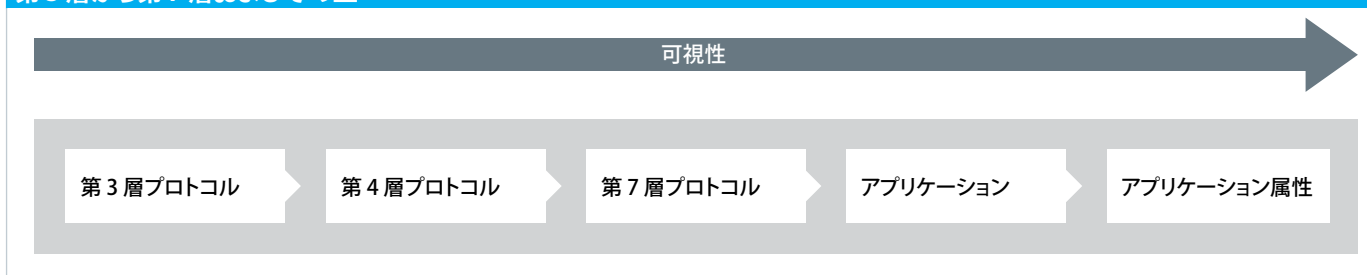
この段階では、主にデコーダからのタイムアウト・イベントを実行します。現在のパケットがパケットの並べ替えの段階でバッファに格納された場合でも呼び出す必要があります。内部のフローまたはサブスクライバ追跡が使用されている場合も、この段階でこれらのタイムアウト・イベントが返されます。

R&S®PACE 2はネットワーク・データをリアルタイムで解析し、今日最も一般的なアプリケーションの正確な検出機能を提供します。

4. プロトコルおよびアプリケーションの分類

R&S®PACE 2 ソフトウェア・エンジンは、ネットワーク・データをリアルタイムで検査および解析し、ネットワーク・トラフィックからメタデータとアプリケーション属性を抽出する機能を持った今日最も一般的なアプリケーションの正確な検出機能を提供します。ディープ・パケット・インスペクション (DPI)、振る舞い解析、ヒューリスティック解析、統計的解析などのさまざまな技術を使用して IP パケットを解析し、プロトコル、アプリケーション、およびその他のアプリケーション・ベースのトラフィック属性を判断します。

第 3 層から第 7 層およびその上へ



R&S®PACE 2 はソフトウェア開発者キット (SDK) として提供され、ネットワーク・インフラストラクチャとセキュリティ・プラットフォームに容易に組み込めるように設計された高度なプロトコルおよびアプリケーション分類機能を搭載しています。

R&S®PACE 2 はネットワーク・データをリアルタイムで解析し、今日最も一般的なアプリケーションの正確な検出機能を提供します。

R&S®PACE 2 は、第 7 層プロトコル (例: Skype、Facebook、Twitter、Dropbox) に基づいてアプリケーションを正確に検出することができます。また、音声、ビデオ、ファイル転送などのアプリケーション・クライアント・サービス機能を検出してより深く洞察することもできます。R&S®PACE 2 は何千ものネットワーク・プロトコルおよびアプリケーションをサポートしています。

正しいものを正しく検出する

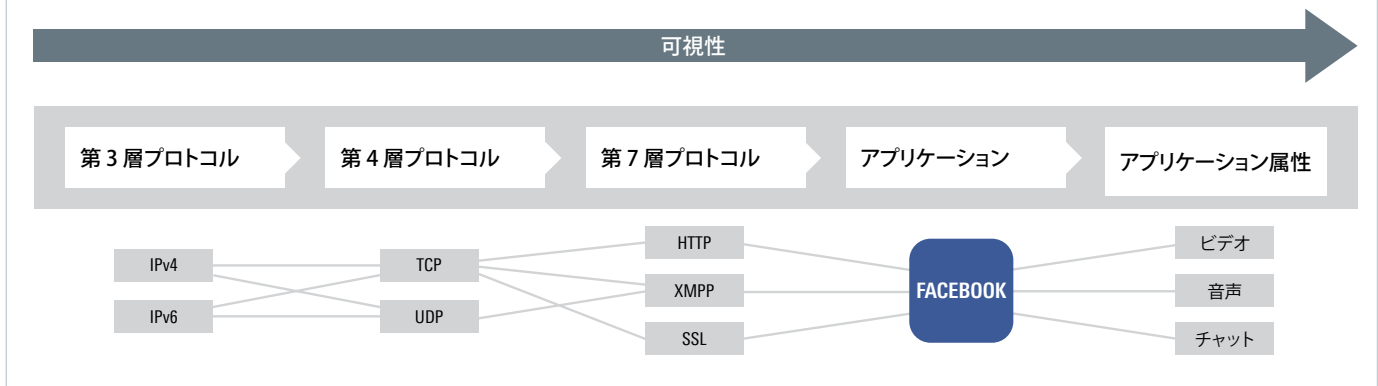
第 7 層プロトコル	第 7 層プロトコルは、OSI 第 7 層 (アプリケーション層) に位置し、アプリケーションと直接対話するネットワーク・プロトコルです。第 7 層ネットワーク・プロトコルは、標準化または暗号化されている場合も独自仕様のものである場合もあります。そのため、ネットワーク・プロトコル情報はほとんど、あるいはまったく参照できません。 <ul style="list-style-type: none">■ 標準 (例: HTTP、FTP、SIP、IAX、IMAP)■ 暗号化 (例: SSL、SSH、IPsec、OpenVPN)■ 独自仕様 (例: MSN、OSCAR (Icq)、Skype、UltraSurf、eDonkey)
アプリケーション	アプリケーションは、コンピュータまたはモバイル・デバイスに幅広い用途で有用なタスクを実行させる特定のソフトウェアです。「アプリケーション検出」は、Facebook、Twitter、Dropbox、Skype などの第 7 層プロトコルを使用するコンピュータ・プログラムを識別します。
アプリケーション属性	アプリケーション属性は、VoIP アプリケーション (例: Skype) 用の音声とビデオのフローや、インスタント・メッセージング・プロトコル (例: ICQ) のチャットとファイル転送など、アプリケーションをより詳細に分類するために使用されます。

4. プロトコルおよびアプリケーションの分類

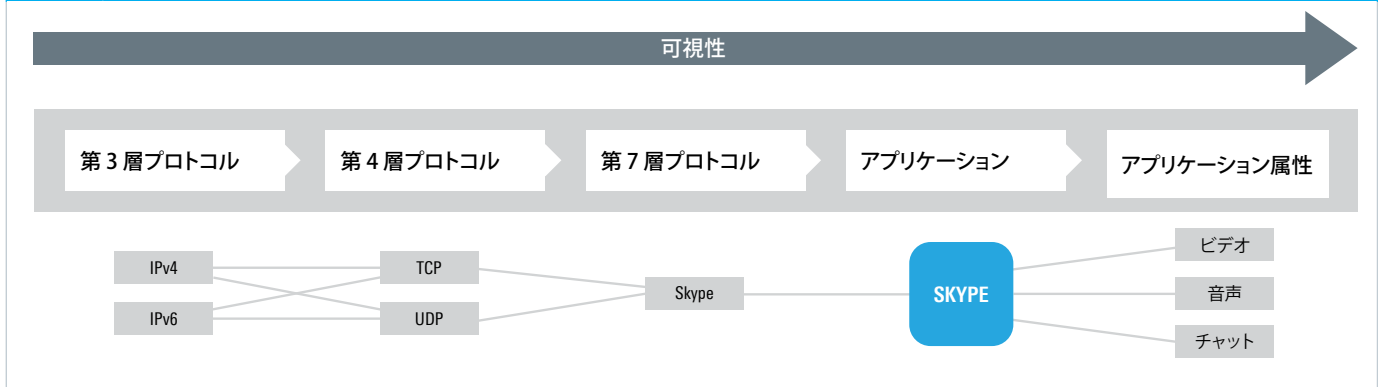
プロトコルとアプリケーション・バージョンが頻繁に更新されるため、継続的に信頼性の高い検出が保証されます。

アプリケーションは、ビデオ、ピアツーピア、VoIP、インスタント・メッセージングなどのサービス・タイプに分類できるため、解析が容易で、インテリジェントなトラフィック判断が可能になります。R&S[®]PACE 2 は分類結果を柔軟に提供でき、さまざまなユース・ケースをサポートします。

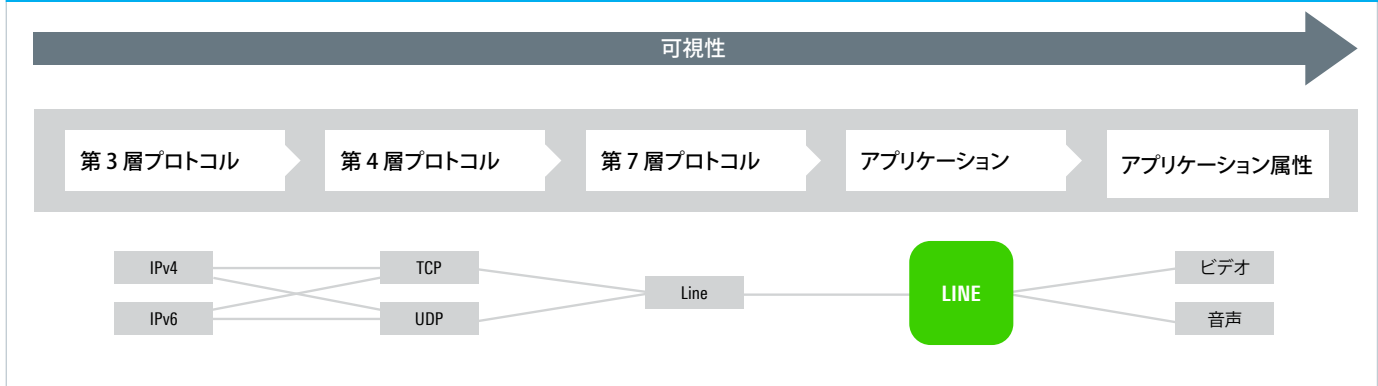
例 1: Facebook



例 2: Skype



例 3: Line



5.分類確度の保証

R&S®PACE 2 は、パターン・マッチング、振る舞い解析、ヒューリスティック解析、統計的解析など、業界をリードするさまざまな分類技術を使用してネットワーク・トラフィックを認識します。そのため、高度な難読化技術や暗号化技術が使用されている場合でも、R&S®PACE 2 はネットワーク・プロトコルを確実に検出することができます。R&S®PACE 2 は偽陽性（アプリケーションを誤って識別する）の検出率が最小限になるように設計されています。例えば請求書作成の分野では、実際の収益に悪影響を与え、事業者のブランド・イメージを傷付けるおそれがあるため、偽陽性を避けることは不可欠です。R&S®PACE 2 は、非常に低い偽陰性率（アプリケーションの分類率が低い）が要求されるトラフィック管理にも適しています。実際のトラフィック・データでのパフォーマンス・テストによると、R&S®PACE 2 はネットワーク・トラフィックの約 95% を正確に識別できます。

R&S®PACE 2 は業界をリードする分類技術を使用し、ネットワーク・トラフィックの約 95% を正確に識別できます。

ipoque は非常に正確なアプリケーション識別を保証するために、頻繁にシグネチャを更新しています。プロトコルとアプリケーションのわずかな変更でも分類に問題が生じる可能性があります。ほとんどのアプリケーションの変更の詳細は公表されることがないため、絶えず注意を払う必要があります。ipoque にはアプリケーション・プロトコルの専門家チームがあり、24 時間体制でパターンおよび動作を監視し解析しています。継続的なパフォーマンスと信頼性のテストの結果、ソフトウェアを定期的に改善し、すべてのアプリケーションを確実に検出することが可能になります。

ipoque のデータベースには、サポートされるすべてのプロトコルおよびアプリケーションについて、何千もの異なるトレースが格納されています。データベースには、2005 年以降の ipoque のトレースに加えて、さまざまな顧客、市場、地域からの匿名化されたテスト・データが格納されています。ipoque はよく知られたアプリケーション、特に、頻繁に変更されるモバイル・アプリケーションについて、毎週変更をチェックします。

6.暗号化の処理

Skype、WhatsApp、BitTorrent、Facebook、Twitter、Drop box、Gmail、Office365、Instagram など、暗号化されるプロトコルおよびアプリケーションはますます増加しています。加えて、eDonkey、Freenet およびその他の P2P アプリ、Ultrasurf、YourFreedom など一部のプロトコルは、特定のプロトコルのトラフィックが制限またはブロックされているような場合にファイアウォールや DPI 検出を迂回するように改変することができます。R&S®PACE 2 は、フロー追跡、バイト・パターン・マッチング、振る舞い解析などのさまざまな検出技術を使用しているため、この課題に対応することができます。

1.パターン・マッチング

- IP パケット内で繰り返される文字列および数の単純なチェックです。

2.振る舞い解析

- サブスクリバおよびホストの情報を追跡しながら、IP フロー内のパケット・サイズ、さまざまなパケット・サイズの順序をチェックします。

3.統計的／ヒューリスティック解析

- IP フロー内で繰り返されるバイト・オーダまたはメタデータのような共通する状況の解析。
- ほとんどの場合、分類結果の信頼性を保証するために多数のチェックが行われます。

4.有限状態機械

- 分類結果について特定の要件のセットが満たされる必要があります。

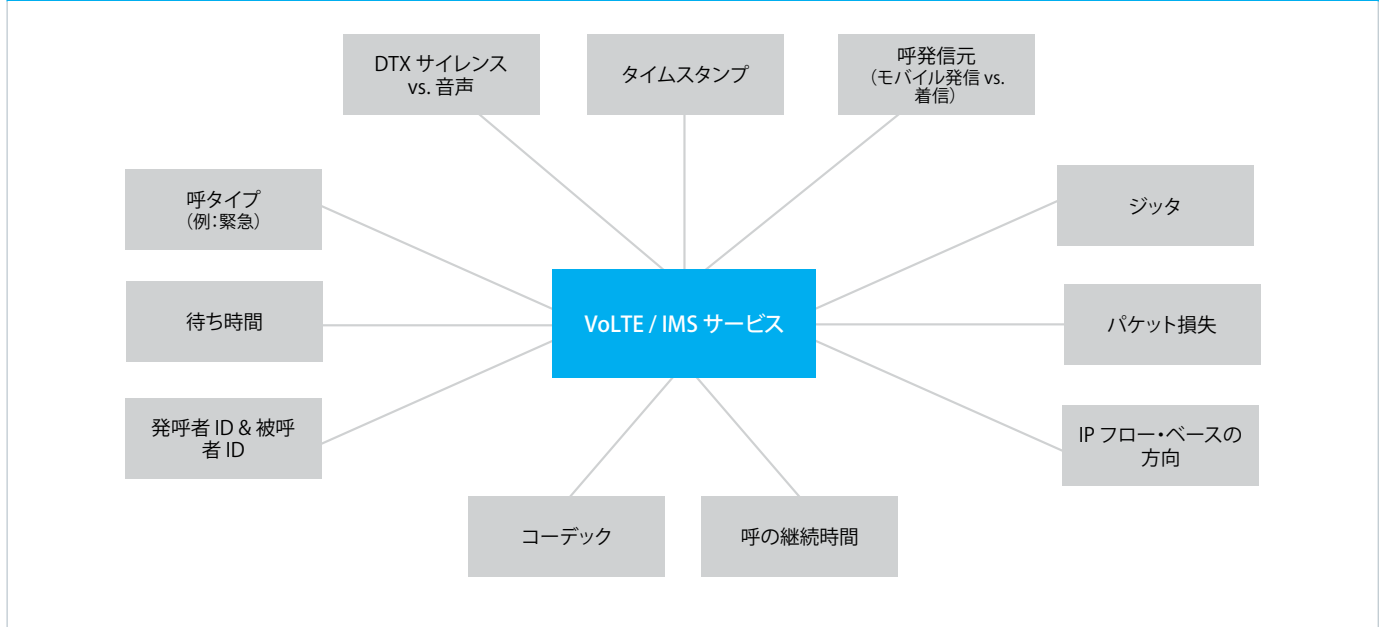
R&S®PACE 2 は、これらの技術をすべて組み合わせることで、偽陰性率が非常に低く、偽陽性がほぼない状態で暗号化されたプロトコルを確実に検出することができます。

7.メタデータの抽出

7.1 パフォーマンス・メタデータ

R&S®PACE 2 は、SYN-SYN/ACK パケット間および SYN/ACK-ACK パケット間のラウンドトリップ時間などの TCP パフォーマンスを測定する機能を搭載しています。これらは、待ち時間やジッタなどのアプリケーション・パフォーマンス・インジケータとして、ネットワークのトラブルシューティングに役立ちます。また、VoIP およびビデオ・アプリケーションの品質に関する情報を取得する機能も搭載しています。これらのパフォーマンス測定は、TCP/IP ベースの QoS/QoE ユース・ケースにおいて重要となります。

重要業績評価指標を含むメタデータの抽出



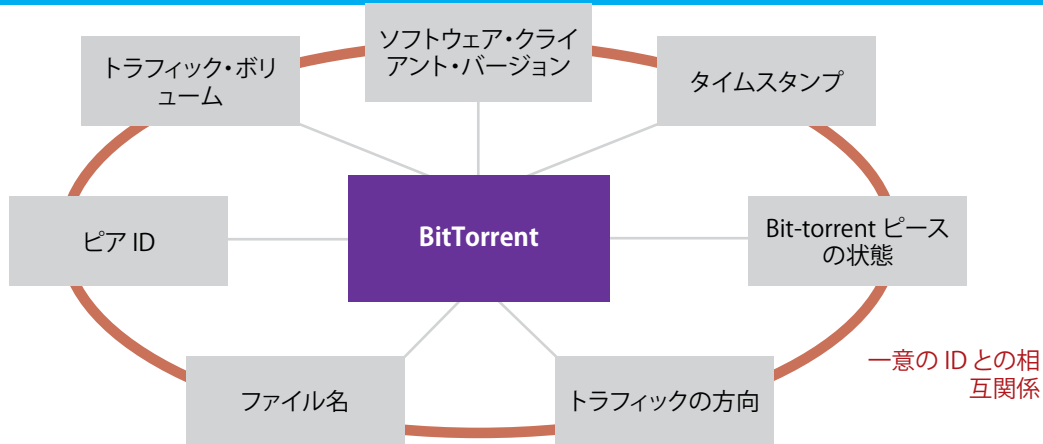
7.メタデータの抽出

7.2 プロトコルおよびアプリケーション・メタデータ

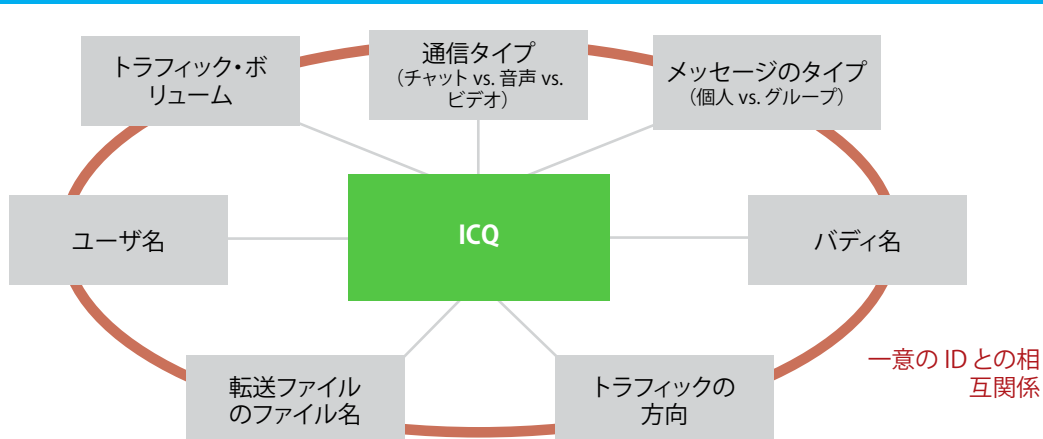
R&S®PACE 2 には、第 3 層から第 7 層へのプロトコルおよびアプリケーション・ベースのメタデータを IP トラフィックから抽出する機能が搭載されています。メタデータの抽出はリアルタイムで実行され、ユーザの行動やアプリケーションの使用状況を洞察することができます。プロトコルおよびアプリケーション・メタデータの抽出を推進する R&S®PACE 2 の機能によって、ネットワークのトランザクションおよび振る舞いをより詳細に理解することができます。この洞察力は、カスタマ・エクスペリエンス管理、ネットワーク計画、ポリシー管理、ネットワーク・セキュリティなどの幅広い用途に役立ちます。IP トラフィックからは以下のようなメタデータを抽出できます。

- ▶ ボリューム：アプリケーションごと、ユーザごと、プロトコルごとのトラフィックのボリューム。
- ▶ 識別子：強力なセキュリティ規則の実装に使用できる電子メールの送信者／受信者のアドレスまたはその他の ID。
- ▶ ファイル：ビデオ・オン・デマンド・アプリケーションで使用されるコーデックをセキュリティ・アプリケーションや QoS/QoE アプリケーションなどに使用できます。
- ▶ 使用状況：HTTP URL または使用されるクライアント・ソフトウェアをインテリジェント・トラフィック判断およびカスタマ・エクスペリエンス管理に使用できます。

例 1: BitTorrent



例 2: ICQ



8.コンテンツ復調

R&S®PACE 2 の復調結果には現在の接続に関する詳細情報が含まれています。R&S®PACE 2 は詳細レベルを設定可能な多数のネットワーク分類結果からすべての重要な関連メタデータを抽出し、さまざまなユース・ケースに適応させることができます。例えば、HTTP ペイロードを伸張し、インターネット・サイトのすべての画像またはビデオを再構築することができます。実際に必要なデータだけが得られるように、必要な情報の深度を柔軟に調整することができます。内部アグリゲータが特定のデコーダから復調情報を収集し、クラスにまとめます。例えば、電子メールの接続に長時間かかる場合でも、全セッションの復調情報によって 1 カ所ですべてのデータが提供されます。

R&S®PACE 2 の復調機能は、VoIP 呼、Web サイト、およびチャット・セッションの再生、または各種ドキュメントのアップロード／ダウンロード統計の収集など、ネットワーク・セキュリティ・アプリケーションで特に有用です。次世代ファイアウォールは、R&S®PACE 2 の復調結果に基づいて、データ漏洩防止、詳細なセキュリティ・スキャン、およびネットワーク・アクセス制御を有効にすることができます。トラフィック管理およびポリシー制御ソリューションも、帯域幅管理およびサービス品質 (QoS) / 経験品質 (QoE) の規則に関して最適な決定を行うことができるように、アプリケーション・コンテンツの詳細な洞察に頼っています。アプリケーション・レベルに基づいた個別課金も可能です。

9.追加機能

9.1 動的なアップグレード

R&S®PACE 2 は実行中に中断せずに更新できるため、稼働中のシステムでも検出を改善することができます。この更新にはよく知られたプロトコルのシグネチャ更新および検出ロジックの更新が含まれ、新しくサポートされるプロトコルの検出がシームレスに追加される場合もあります。検出ロジックの更新は、パフォーマンスと検出結果を改善するためのものです。

9.2 OS 検出

OS 検出では、フローの特定の属性を解析して対応するオペレーティング・システムを検出します。プロトコル検出と同様に、OS 検出では OS が検出されたかどうかを示す結果がフローごとに返されます。

9.3 NAT/テザリング検出

R&S®PACE 2 にはサブスライバ・ベースの NAT およびテザリング検出が搭載されています。OS 検出を使用して単一のサブスライバについて複数のオペレーティング・システムが使用されているかどうかを判断し、その結果に応じてサブスライバにフラグを設定します。サブスライバごとに、検出されたメイン OS と検出された NAT 状態を参照できます。

9.4 クライアント・サーバ表示

R&S®PACE 2 は、主にクライアントとして使用されるホストと主にサーバとして使用されるホストを識別できます。この機能を使用すると、内部ネットワーク内のサーバを検出したり、ネットワークのどちら側が実際に内部ネットワークなのか事前に判断していない場合に内部ネットワークを判断したりすることができます。この機能は、各フローがクライアントからサーバへのフローか、サーバからクライアントへのフローか、さらには P2P ネットワークにおけるクライアントからクライアントへのフローであるのかも識別できます。純粋なサーバ通信においては、サーバからサーバへのフローも識別できます。

9.5 一方向トラフィックのサポート

ネットワークの設定に応じて、特定のネットワーク・リンクが両方の方向にパケットを運ぶことも（双方向の場合）、1つの方向だけにパケットを運ぶことも（一方向の場合）あります。この一方向のルーティングは、当該リンクのすべてのパケットに適用することも、特定のサブスライバ・グループのみなど、パケットの一部だけに適用することもできます。一方向構成の典型的な例は、ケーブル・ダウンリンクと衛星アップリンクによるインターネット接続です。R&S®PACE 2 は双方向のトラフィックも一方向のトラフィックも検出できます。

9.6 カスタマイズ

R&S®PACE 2 は、新しいライブラリを追加しなくても、カスタム定義されたプロトコル (CDP) を追加して検出を拡張することができます。これらの CDP は顧客が追加でき、以下のような機能があります。

- 規則ベースのアプローチ (HTTP ホスト照合、ポート照合など) または C コード (あるいはその両方) により、最大限の柔軟性を確保できます。
- サポートされるプロトコルの数は事実上無制限です。
- ライブラリ初期化中に設定可能です。

9.7 高速パス

高速パス・メカニズムは、既に識別済みで、追加処理の必要がないフローの処理を高速化するために使用されます。R&S®PACE 2 にはこの高速パスのステータスを照会する API 機能が搭載されているので、追加処理の必要がないフローを完全にスキップすることができます。

10. パフォーマンス・テスト

ipoque は、R&S®PACE 2 が正常に展開されたさまざまな顧客製品の IP キャプチャ・ファイルを使用して R&S®PACE 2 のパフォーマンスを評価するテストを実施しました。

テストはすべて以下の機能を有効にして実施しました。

- フロー追跡
- サブスクライバ追跡
- IP デフラグ
- 検出

このテスト・データの背後にある考え方は、顧客のユース・ケースの幅広い選択に基づいてパフォーマンスを示すことです。

検出には TCP / UDP 接続の内部フロー・データ構造への有効なポイントが必要ですが、組み込みハッシュ・テーブルを使用してこの情報を格納できます。フロー追跡では、ハッシュ・テーブルは接続情報として 5 つのタプル (IP アドレス、TCP/UDP ポート、および IP プロトコル) を使用します。サブスクライバ追跡は接続の追跡によく似ています。IP デフラグは、R&S®PACE 2 に渡される前に断片化した IP パケットを再構築するために使用されます。R&S®PACE 2 デフラグ・エンジンの基本的な考え方は、パケット全体の再構築が可能になるまですべての断片を格納するというものです。ネットワークのパケットの流れの

中でほぼすべてのアプリケーションを検出するソフトウェア・ライブラリである R&S®PACE 2 は、検出自体を主要な目的としています。R&S®PACE 2 では、パターン・マッチング、ヒューリスティック解析、振る舞い解析など、幅広い IP 分類技術が使用されます。R&S®PACE 2 は、これらの技術を組み合わせることで、偽陰性率が非常に低く、偽陽性がほぼない状態で暗号化されたプロトコルを確実に検出することができます。

10.1 テスト・データ

リストのユース・ケースはすべて、R&S®PACE 2 が正常に展開されたさまざまな顧客製品の IP キャプチャ・ファイルです。各ファイルは特化されたユース・ケースであり、一連のアプリケーション・シナリオの選択を表します。この表の背後にある考え方は、顧客のユース・ケースの幅広い選択に従ってパフォーマンスを示すことです。

10.2 シングル・スレッド・テスト

このテストでは、パケットあたりの CPU サイクルに焦点を合わせます。以下の市販のシステム上ですべての測定を実行します。

テスト環境仕様	
筐体	Dell PowerEdge R210 II
CPU タイプ	Intel Core i3-2100 CPU @ 3.10GHz
内部メモリ	8GB DDR3-1333 SDRAM
イーサネット・インタフェース	Broadcom NetXtreme II BCM5716 ギガビット・イーサネット
ストレージ	2x Seagate ST31000340NS (1TB)、RAID0
オペレーティング・システム	Ubuntu 10.04 LTS

ユース・ケース	一般的な情報	一般的な情報
1 ネットワーク事業者	パケットの数: 33.1M 平均パケット・サイズ: 569 最大同時接続数: 418720 平均スループット: 3.4 Gbit/s	HTTP、FLASH、BITTORRENT、MPEG、SKYPE、DIRECT DOWNLOAD LINK、PPSTREAM、SSL、GNUTELLA、QUICK-TIME、MSN、SHOUTCAST、MMS、DNS、RTP、YAHOO、POP、RTSP、OGG、WINDOWS MEDIA、SSH、H323
2.次世代 ファイアウォール・ベンダ	パケットの数: 6.1M 平均パケット・サイズ: 523 最大同時接続数: 71191 平均スループット: 5.6 Gbit/s	HTTP、SSL、RTP、FLASH、OPENVPN、IPSEC、BITTORRENT、RTP、H323、QUICKTIME
3.エンタープライズ (中位展開)	パケットの数: 203.5M 平均パケット・サイズ: 396 最大同時接続数: 18128 平均スループット: 9.9 Gbit/s	HTTP、FLASH、QUICKTIME、RTP、SIP、SSL、BITTORRENT、EDONKEY、YAHOO、DIRECT DOWNLOAD LINK、SKYPE、H323、TEAM VIEWER、OPENVPN、IPSEC
4.エンタープライズ (小型展開)	パケットの数: 1M 平均パケット・サイズ: 786 最大同時接続数: 5702 平均スループット: 20.2 Gbit/s	BITTORRENT、HTTP、SSL

11. サービスとサポート

11.1 製品評価

限定された顧客がライブラリを評価するために、R&S®PACE 2 ソフトウェアのデモ版を提供できます。この段階では、顧客の組み込みプロセスを容易にし、ソリューションの評価とカスタマイズを効率的に行えるように、ipoque によるリモート・サポートまたは現地サポートを行います。

11.2 保守

高パフォーマンス IP 分類および復調ソフトウェアには定期的なファームウェアの更新が不可欠です。ipoque は、新しいプロトコル・シグネチャの分類アルゴリズムを開発して、プロトコルおよびアプリケーション検出の有効性を絶えず監視しています。サポートされるすべてのシグネチャが絶えずテストされ、ネットワーク・アプリケーションの進化に合わせて更新されます。シグネチャの更新は少なくとも月に 1 回の頻度で提供されます。更新がある場合、顧客は通知の電子メールを受信し、ipoque の顧客ポータルを通して更新にアクセスできます。

11.3 顧客ポータル

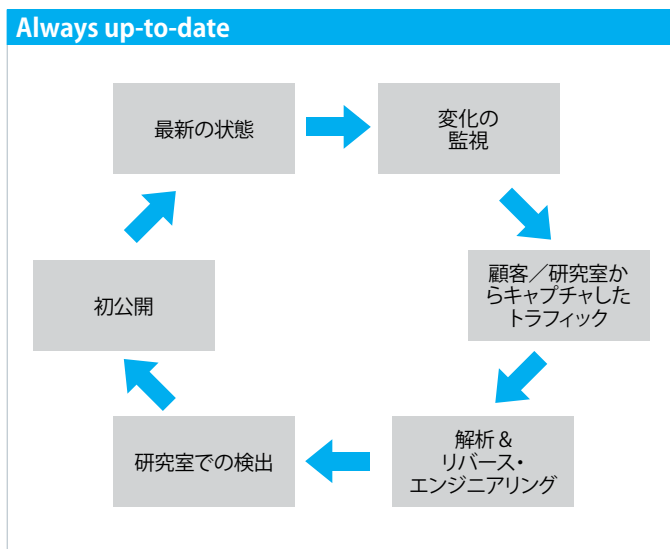
ipoque は R&S®PACE 2 の顧客向けに Web ベースのポータルを管理しており、顧客の技術スタッフが以下の用途に使用できます。

- ▮ トラブルシューティングの議題の作成／管理
- ▮ チケットの優先度の処理
- ▮ 双方向でのドキュメントおよび添付ファイルの共有 (PCAP、パッチなど)
- ▮ 利用可能なファームウェア・リリースに関する情報の受信

顧客には顧客ポータルの専用ログイン・アカウントが付与されます。システム上に個人用アカウントを作成するために複数のログイン・アカウントを提供することもできます。

11.4 トレーニング

ipoque は顧客およびパートナー向けに高品質なトレーニングを行っています。ipoque の総合的なトレーニングは、製品に関連する学習の要件をすべて満たすように設計されています。トレーニング・チームは ipoque 製品について並ぶものがない知識を持っており、PACE ソフトウェアを正しく実装して顧客のソリューションに組み込むために必要な知識を伝えることができます。トレーニングは ipoque の施設で行うことも顧客の施設で行うこともできます。製品トレーニングは ipoque が提供するオプションのサービスです。開発者向けの技術トレーニングから、管理職およびプロダクト・マネージャ向けの上位レベルの製品機能トレーニングまで、さまざまなトレーニング・モジュールを利用できます。



12.ユース・ケース

R&S®PACE 2 は、ネットワーク・セキュリティ (IDS/IPS、ファイアウォール、SIEM、UTM)、ネットワーク・モニタリング (QoS/QoE)、ポリシーと課金、OSS/BSS、WAN の最適化とアプリケーション配信、モバイル・データ・オフロード、およびネットワークとサブスクリバの解析など、さまざまなネットワーク・ソリューションに展開することができます。

R&S®PACE 2 を組み込むことで、ベンダは製品にアプリケーション検出機能を導入し、プロトコルとアプリケーションのダイナミックな変化に対応することができます。

12.1 ネットワークとトラフィックの管理 (QoS/QoE)

トラフィック管理ベンダは、モバイル・ネットワーク事業者などの最終顧客に、サブスクリバのアプリケーション使用状況とパフォーマンス、重要業績評価指標 (KPI) モニタリング、トレンド解析、およびサービス品質とサブスクリバの経験品質について正確なリアルタイムの情報を提供する必要があります。これらのソリューションには、キャリア VoIP とビデオ、YouTube、Netflix などのプロトコルおよびアプリケーション使用状況の詳細で信頼性の高い情報と、遅延、パケット待ち時間、ジッタ、VoLTE またはビデオの呼完了などのアプリケーション・メタデータを抽出する機能が必要です。R&S®PACE 2 はアプリケーションから第 7 層を正確に識別し、ネットワークとアプリケーションのパフォーマンスをリアルタイムで管理する機能を提供します。R&S®PACE 2 を組み込むことで、ベンダはプロトコルとアプリケーションのダイナミックな変化に対応し、トラフィック管理のための高い検出率を維持することができます。

12.2 ポリシー制御と課金

ネットワーク事業者は、ネットワーク帯域幅の需要と、新しいサービスおよびアプリケーションの収益を上げる必要性のバランスを取る必要があります。事業者は帯域幅の保証、優先度、および制限を規定し、追加料金による QoS を提供し、さらに重大なことに、リアルタイム課金と請求サポートを可能にしようとするため、ポリシー制御と課金は LTE ネットワークの主要コンポーネントとなります。ポリシー制御および課金ベンダは、きめ細かい QoS をサポートし、アプリケーション・サーバが提供するサービスの QoS と課金要件を動的に制御できるようにする必要があります。R&S®PACE 2 ソフトウェアはネットワーク・トラフィックの 95% 以上を識別でき、シグネチャが頻繁に更新されるため、ポリシーと請求のための高い検出率と正確なアプリケーション識別が保証されます。

12.ユース・ケース

12.3 ネットワーク・セキュリティ (ファイアウォール、IPS/IDS、SIEM、UTM)

Web プロトコルを使用する IP ネットワーク・トラフィックが大きく成長したため、セキュリティ・ベンダはアプリケーションを識別してトラフィックを区別する必要があります。次世代ファイアウォール (NGFW) はアプリケーションを認識します。通常の Web ポートから受信するトラフィックをすべて許可する代わりに、Hulu と Salesforce.com などの特定のアプリケーションを区別し、ビジネス規則に基づいたポリシーを適用することができます。ipoque R&S®PACE 2 を組み込むだけでセキュリティ・ベンダはアプリケーションの正確な認識と制御が可能になり、セキュリティの脅威に対応してネットワーク攻撃を防止することができます。R&S®PACE 2 のすぐに使用可能なソフトウェア・ライブラリとシグネチャ・データベースを使用することで、非常に複雑な技術を社内で開発および維持することに伴うコストとリスクを軽減できます。最新のアプリケーションおよびプロトコルに対応してソフトウェアを継続的に更新することは、これを社内で行うセキュリティ・ベンダにとっては難題です。そのため、セキュリティ製品は脅威およびマルウェアへの対応に効果的です。

R&S®PACE 2 のすぐに使用可能なソフトウェア・ライブラリを使用することで、非常に複雑な技術を社内で開発および維持することに伴うコストとリスクを軽減できます。

12.4 ネットワークとサブスクリイバの解析

サブスクリイバのアプリケーション使用状況と行動の理解を深めることの価値を事業者が認識するとともに、ネットワークとサブスクリイバのデータからビジネス・インテリジェンスを取得するという分野が急速に成長しています。これは次に、マーケティング部門がデータ・パッケージを強化するため、さらにはネットワークの計画と最適化により投資を計画しアプリケーションあたりの QoE を改善するために使用されています。R&S®PACE 2 は、サブスクリイバが使用しているアプリケーションの高性能で正確な識別機能を解析ベンダに提供します。また、パワー・ユーザや、サブスクリイバ区分または地域で最も使用されるアプリケーションなど、使用時間やコンテンツのタイプに関する豊富なデータも提供します。これによってベンダの報告機能が強化され、製品化までの時間が短縮されます。また、アプリケーション認識はそれ自体が中核的な専門技術であるため、ベンダは最新のアプリおよびプロトコルを追跡および分類するために社内リソースを利用する必要はありません。通常の組み込みでは、このアプリケーション使用状況データは、サブスクリイバのモバイル・データ消費に関するレポートとダッシュボードを提供するサードパーティの解析システムに直接リンクされます。

12.5 モバイル・データ・オフロード

ネットワーク事業者は、モバイル・データ・オフロード・ソリューションを使用して、ネットワークを停滞させるトラフィックのうち、収益が少なく優先度の低いトラフィックの負荷を軽減し、総合的なサービス品質を向上しています。モバイル・データ・オフロード・ソリューションは、通常、関連アプリケーションまたは使用されるデバイスを区別せず、すべてのトラフィック・フローを平等に扱います。ただし、LTE 展開では、事業者は使用されるアプリケーションに基づいてトラフィック・フローを選択

12.ユース・ケース

的に操縦しようとしています。R&S®PACE 2 ソフトウェアを使用すると、ベンダは確実にアプリケーションを検出し、フロー全体を認識して洗練されたオフロード戦略を実装できます。Intel は、モバイル・インターネット・アクセス・ゲートウェイとして小型セルで使用される「Smart Pipe」サーバに R&S®PACE 2 技術を組み込みました。ネットワーク事業者がこのソリューションを使用することで、アプリケーション・レベルでインターネット・トラフィックを分類し、モバイル Voice over IP (VoIP) 呼およびビデオ・ストリーミングの QoE を改善できます。

R&S®PACE ソフトウェアを使用すると、ベンダはフロー全体を認識して洗練されたオフロード戦略を実装できます。

12.6 WAN の最適化

クラウド・コンピューティングとモバイル作業の成長が相まって、広域ネットワーク上でビジネスに不可欠なアプリケーションのパフォーマンスを保証し、帯域幅効率を確保することはますます困難になりました。より効率的に重要なビジネス・トラフィックの優先順位を付け、帯域幅が過密にならないようにするために、ベンダはリアルタイム・アプリケーション認識を組み込み、広域ネットワーク上で実行されるアプリケーションの理解を深める必要があります。R&S®PACE 2 は何千ものアプリケーションを IP フローごとにリアルタイムで識別できます。WAN 最適化ベンダは、ネットワーク上で実行されるアプリケーションとユーザの行動を正確に認識し、先行投資費用、製品化までの時間の遅延、および社内開発に関連するビジネス・リスクを回避することができます。異なるサーバから数種類のマルチメディア・コンテンツ（ビデオ、画像、VoIP など）を集約する複雑なアプリケーションが登場したことで、WAN 最適化ソリューションはプロトコルおよびアプリケーションの完全な可視性が要求されます。

12.7 SDN/NFV 環境

電気通信事業者のハードウェアからソフトウェア・ベースの仮想化ネットワーク環境への移行は、既製の市販ハードウェアに基づいて一定の速度で進行しています。事業者は、独自仕様のハードウェアを減らし、ネットワーク費用を削減し、拡張性のある IP ベースのネットワークでアプリケーションをより柔軟に管理できるようにすることに専念しています。SDN / NFV によって、R&S®PACE 2 などの IP アプリケーション分類ソフトウェアは、多くのネットワーク・アプライアンスに組み込まれたものから、標準サーバ上でホストされた共有機能に移行することができます。R&S®PACE 2 には外部依存関係がなく、標準的なサーバと OS 上で動作します。また、物理的環境が仮想化環境に関わらず、さらには SDN 構成でも、すべての環境で使用できます。

ipoque について

ローデ・シュワルツ・グループ企業の ipoque GmbH は、ネットワーク事業者およびインフラストラクチャ・ベンダ向けのネットワーク・トラフィック解析と IP 分類ソリューションで世界をリードしています。ネットワーク効率を最大化し、サブスクリバの経験品質を向上し、将来のインテリジェントな通信ネットワークを開発するために、全世界 60 カ国以上で 200 を超える顧客が ipoque に頼っています。

ローデ・シュワルツについて

ローデ・シュワルツ・グループは、エレクトロニクス分野に特化し、電子計測、放送・メディア、サイバー・セキュリティ、無線通信の監視・探知および高品質な通信システムなどで世界をリードしています。80 年以上前に創業、世界 70 カ国以上で販売と保守・修理を展開している会社です。本社はドイツのミュンヘンにあります。

Certified Quality Management
ISO 9001

ipoque GmbH

www.ipoque.com

Rohde & Schwarz GmbH & Co. KG

www.rohde-schwarz.com

R&S® は、ドイツ Rohde & Schwarz 社の商標または登録商標です。
PD 3607.2332.36 | Version 01.00 | April 2016
R&S®PACE 2 ソリューション・ガイド
掲載されている記事・図表などの無断転載を禁止します。
おことわりなしに掲載内容の一部を変更させていただくことがあります。
あらかじめご了承ください。
© 2016 Rohde & Schwarz GmbH & Co. KG | 81671 Munich, Germany
© 2016 ipoque GmbH | 04109 Leipzig, Germany



3607.2332.36