Cisco ASR 1000 シリーズ ルータのネットワーク セキュリティ機能

このデータ シートでは、Cisco® ASR 1000 シリーズ アグリゲーション サービス ルータに搭載されたネットワーク セキュリティ機能の概要を説明します。

製品の概要

今日のビジネス アプリケーションの導入ペースは、5 年前に比べて大幅に迅速化されています。ビジネスにおける要求が強まり、テクノロジーが進歩するにつれて、ネットワークは基礎的な接続ユーティリティからサービスを提供するプラットフォームへと進化を遂げました。

企業の本社は、急速に変化する環境において、セキュリティやパフォーマンス、ネットワーク アップタイムを危険にさらすことなく、WAN および Metropolitan Area Network（MAN; メトロポリタン エリア ネットワーク）サービスをグローバルに拡張する必要が増しています。現在の課題は、運用上の複雑さとコストを最小限に抑えながらこれらのニーズを満たすことです。この課題への対応に役立つのが統合型アーキテクチャ アプローチです。

現在のトレンドに対処するために、シスコの統合型ルータ セキュリティは包括的なセキュリティ サービス、インテリジェントに組み込まれたルーティングおよびセキュリティ機能を提供し、高速でスケーラブルなミッションクリティカル ビジネス アプリケーションを実現します。

Cisco ASR 1000 シリーズ ルータはセキュリティを統合し、リモート サイトやビジネス パートナー、在宅勤務者、モバイル ワーカーへのビジネス リソースのセキュアな拡張を促進する、費用対効果に優れたスケーラブルな WAN および MAN サービスの集約を提供します。図 1 に Cisco ASR 1000 シリーズ ルータの製品ポートフォリオを示します。

図 1　Cisco ASR 1000 シリーズ ルータ ポートフォリオ

Cisco ASR 1000 シリーズ ルータは、個別のサービス ブレードを必要とせずに、組み込み型のハードウェア アクセラレーションを、VPN、ファイアウォール、Network Based Application Recognition（NBAR）、NetFlow、Quality of Service（QoS; サービス品質）、IP マルチキャスト、Access Control List（ACL; アクセス コントロール リスト）、Reverse Path Forwarding（RPF）、Policy-Based Routing（PBR; ポリシーベース ルーティング）などの Cisco IOS® ソフトウェア サービスに提供する、業界初の高度にスケーラブルな WAN およびインターネット エッジ ルータ プラットフォームです。さらに、冗長ルート プロセッサやエンベデッド サービス プロセッサ、ソフトウェアベースの冗長性を装備し、ビジネスクラスの復元力を実現します。

All contents are Copyright © 1992–2011 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Cisco ASR 1000 シリーズ ルータは、ルーティング性能、IP Security（IPsec）VPN、およびサービスが有効にされた従来のミッドレンジ アグリゲーション ルータの最大 20 倍の速度を実現したファイアウォールを備えており、既存のネットワーク設計と運用上のベスト プラクティスを活用しながら、最新のサービス集約要件を満たす費用対効果に優れたアプローチを提供します。

業界初のスケーラブルかつプログラマブルなアプリケーション認識ネットワーク プロセッサの Cisco QuantumFlow Processor を搭載した Cisco ASR 1000 シリーズ ルータは、WAN および MAN サービス集約をネットワーク セキュリティ機能と組み合わせ、お客様に次のようなメリットをお届けします。

- 高度な QoS および IP マルチキャスト統合を実現した拡張性の高いサイトツーサイトおよびリモートアクセス VPN 集約機能
- 高度な境界セキュリティ、アプリケーションの可視性、高速ロギング
- 企業のサーバおよびその他リソースにおける Distributed-Denial-of-Service（DDoS; 分散型サービス拒否）攻撃の検出と対応
- コントロール プレーンの分離およびエッジ ルータに内蔵された防御機能による高度な復元力で、攻撃されても稼働性を維持
- 将来のバージョンと互換性のあるアーキテクチャで、プラットフォーム シャーシなどのコンポーネントを置き換えることなく、さらなるスループットとサービスの成長に対応
- 単一プラットフォームにマルチサービスを集約して運用を簡素化し、トレーニング コストを削減

用途のシナリオ

スケーラブルでセキュアにマルチサービスを集約

本社の集約サイトに設置する Cisco ASR 1000 シリーズは、Cisco 7200 および 7301 ルータと、Cisco 7600 シリーズ ルータおよび Cisco Catalyst® 6500 シリーズ スイッチの間としての位置づけとなります。Cisco 7200 および 7301 ルータも組み込み型のサービス集約に基づいており、小規模から中規模のネットワーク向けに費用対効果の高い WAN 集約を促進しますが、パフォーマンスとスケーラビリティはサービス実行中の OC-3 の速度に限定されます。Cisco 7600 シリーズ ルータおよび Cisco Catalyst 6500 シリーズ スイッチは、パフォーマンスを毎秒 4 億パケットまで拡張でき、アーキテクチャは、アドオン サービス ブレードに基づいて高速化されます。このため追加費用がかかりますが、大企業向けに極めて高度な拡張性を持つ WAN および MAN 集約を実現できます。

従来、高性能のセキュリティ サービスはハードウェア（ルータあるいはスイッチ内に設置されるサービス ブレード、アプライアンス）を追加する必要がありました。革新的な Cisco QuantumFlow Processor によって、Cisco ASR シリーズ ルータはハードウェアまたはサービス ブレードを追加することなく最大毎秒 2000 万パケットの能力を実現し、高性能サービスを提供します。このパフォーマンス レベルは Cisco 7200 および 7301 の最大パフォーマンスの 20 倍で、同時にネットワークサービス統合によって複雑さの軽減と費用削減を達成します。

マルチサービス集約型の展開における重要な特徴は次のとおりです。

- 組み込みの型サービス アーキテクチャは、暗号化やファイアウォール、QoS などのネットワークおよびセキュリティ機能のために、サービス ブレードを追加する必要はありません。このアーキテクチャにより、将来の費用対効果が高く、高度な柔軟性を持ったスケーラブルなマルチサービス集約が可能となり、IT スタッフは変化し続ける WAN 要件に迅速に対応できるようになります。

All contents are Copyright © 1992–2011 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

- 将来のバージョンに互換性を持つアーキテクチャにより、Cisco ASR 1000 シリーズ エンベデッド サービス プロセッサ（ESP）を交換するだけで、残りのシャーシおよびコンポーネントはそのままに、暗号化などのサービスのための帯域幅拡張を実現します。
- マルチサービス集約型の展開は、スケーラブルで最適化された QoS および VPN との IP マルチキャスト統合向けに設計されており、大規模な音声およびビデオの統合を可能にします。
- このソリューションは最大 4000 のサイトツーサイト トンネルと 7 Gbps の暗号化（20-Gbps ESP [ESP20]）で、高度な拡張性とパフォーマンスを提供します。
- このソリューションは、ハードウェアの冗長性（Cisco ASR 1000 シリーズ ルート プロセッサ 1 [RP1]、ルート プロセッサ 2 [RP2]、および ESP）と、Cisco IOS ソフトウェアの冗長性によりハイアベイラビリティを提供します。

次世代ブランチ オフィスおよびマネージド CPE

シスコ統合型ルータの製品ポートフォリオは、リモート ブランチ オフィス向けに、業界をリードするサービス統合を実現する Cisco 1800、2800、3800 シリーズ サービス統合型ルータを揃えています。Cisco ASR 1002 ルータは、大規模なブランチ オフィスと各地区のオフィス向けにネットワークとサービスの統合を拡張し、パフォーマンスとスケーラビリティをより高いレベルへと導きます。

ブランチ オフィスおよびマネージド Customer-Premises-Equipment（CPE; 顧客宅内機器）展開の重要な特徴は次のとおりです。

- このソリューションは DS-0 から OC-192 まで、実質的にすべてのインターフェイスをサポートします。
- さまざまなタイプのイーサネット サービス レベル契約（SLA）を使用して、正しくルーティングできるようにブランチ オフィスを支援します。
- サービス プロバイダーのネットワーク停止を迂回して、ミッションクリティカルなアプリケーションの実行を保証するための WAN 最適化を実行します。
- 小型フォーム ファクタ（2 ラック ユニット [2RU]）を用意しています。Cisco IOS ソフトウェアの冗長性とモジュール性で堅牢性を強化し、Cisco IOS ソフトウェアがダウンしていてもデバイスを管理し続けることができます。
- このソリューションは最大 5 Gbps または 10 Gbps のファイアウォールと Network Address Translation（NAT; ネットワーク アドレス変換）および 4 Gbps IPsec を搭載、さらに WAN 最適化と高性能な音声およびビデオの統合を実現し、画期的な価格パフォーマンスを提供します。

製品アーキテクチャ

Cisco ASR 1000 シリーズ ルータのハードウェア アーキテクチャは、管理プレーン、コントロール プレーン、フォワーディング プレーンが単一の CPU に組み込まれています。従来のミッドレンジ ルータ アーキテクチャでは、費用対効果が高いながらも複数のサービス処理においては拡張性が限定されていましたが、そこからの大きな転換を実現しています。

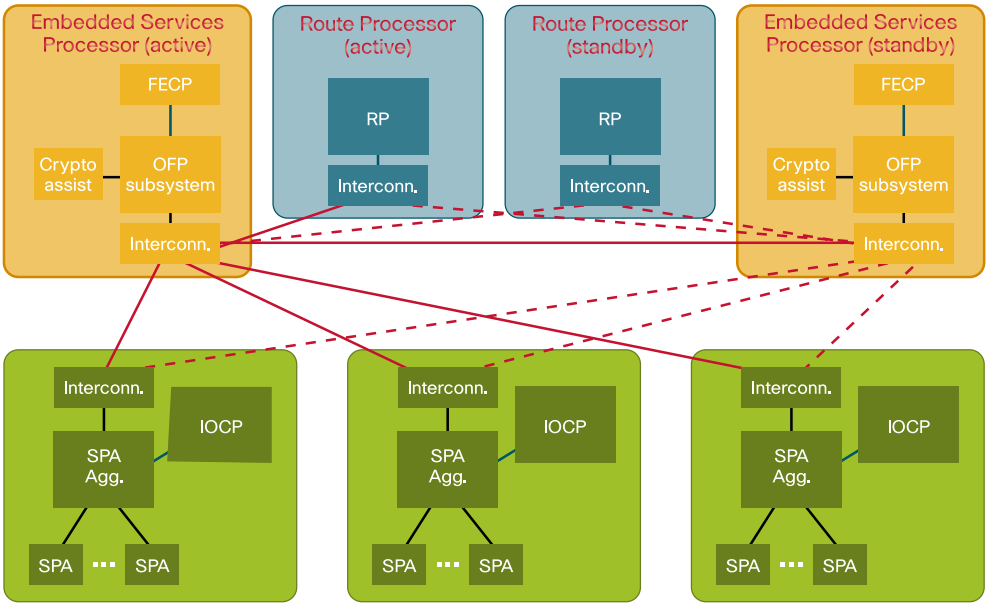
Cisco ASR 1000 シリーズ ルータでは、ハードウェアが機能ごとに個別のプロセッサに分離されています。

- ルート プロセッサはコントロール プレーンのトラフィックを処理して IP ルーティング プロトコルを実行し、システムを管理します。
- ESP はフォワーディング プレーンのトラフィックを処理して、ファイアウォール インスペクション、ACL、暗号化、QoS などのパケット処理機能を実行します。
- Shared Port Adaptor（SPA; 共有ポート アダプタ）キャリア カードには、インターフェイス（I/O）接続を提供する SPA が格納されています。

All contents are Copyright © 1992–2011 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

- 図 2 に冗長ルート プロセッサと ESP を備えた Cisco ASR 1006 ルータのアーキテクチャを示します。Cisco ASR 1004 および 1002 ルータでは、単一のルート プロセッサと ESP を備え、冗長性はソフトウェアで提供されています。

図 2　Cisco ASR 1000 シリーズ ルータのハードウェア アーキテクチャ



分散型コントロール プレーン

Cisco ASR 1000 シリーズ ルータは分散型コントロール プレーンを搭載しています。分散型コントロール プレーンでは、ルート プロセッサ、ESP、または I/O を問わず各プロセッサがさまざまなコンポーネントを実行し、必要なハウスキーピング処理を実行するための CPU をそれぞれ持っているため、ルート プロセッサはフォワーディングや I/O 操作を管理する必要がありません。

- ルータ宛ての Interior Gateway Protocol（IGP）トラフィック、管理ポートからのトラフィックなどのコントロール プレーンの実行は、ルータ プロセッサに搭載された CPU で処理されます。
- ESP 内では、Forwarding Engine Control Processor（FECP; フォワーディング エンジン コントロール プロセッサ）と呼ばれるコントロール プロセッサが、QuantumFlow Processor と暗号化チップ（Cavium Networks により構築されたソフトウェアを含む）を、障害発生時の再起動を含めブートストラップします。
- 各 SPA キャリア カードは SPA Online Insertion and Removal（OIR; 活性挿抜）と SPA ドライバを実行するそれぞれの I/O コントロール プロセッサ（IOCP）を備えています。

中央集中型フォワーディング アーキテクチャ

Cisco ASR 1000 シリーズ ルータは中央集中型フォワーディング アーキテクチャを採用しており、トラフィックはすべて中央集中型の ESP を通過し、パケット処理（ファイアウォール、ACL、暗号化、QoS など）が実行されます。この構成では、管理者は Cisco 7200 シリーズ ルータと同じように機能を設定することができます。たとえば、暗号化マップ、保護機能などはまったく同じで、ハードウェア固有のコマンドは必要ありません。

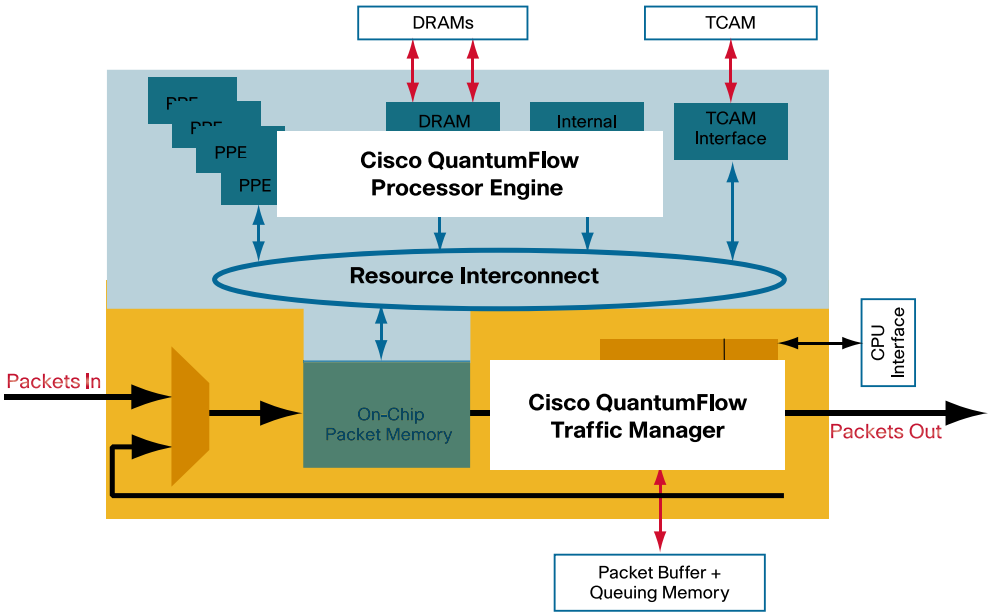
ただし、フォワーディング プロセッサ内では複数の機能が並行して実行され、大きな拡張とパフォーマンスが実現します。

All contents are Copyright © 1992–2011 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Cisco QuantumFlow Processor

ネットワーク フォワーディング プロセッサの中核を成しているのが、分類、サービス統合、トラフィック管理に真の大量並列処理と柔軟なフロー処理を実現する次世代ネットワーク プロセッサ テクノロジーの、次世代 Cisco QuantumFlow Processor です。図 3 に Cisco QuantumFlow Processor のブロック図を示します。

図 3 Cisco QuantumFlow Processor の主要ブロック図



Cisco QuantumFlow Processor は、単なるチップまたはハードウェアによるソリューションではありません。これは、シスコの将来の製品にわたって使用される次世代のハードウェアおよびソフトウェア アーキテクチャを実現するものです。Cisco ASR 1000 シリーズ ルータでの現行の実装では、次の 2 つの主要なシリコン部品が組み込まれています。

- Cisco QuantumFlow Processor Engine：このエンジンは 900 MHz ～ 1.2 GHz で動作する 40 の強力なパケット処理エンジン（コア）の集合体です。大量の並列処理能力によって、ペイロード全体およびフレーム ヘッダーの処理が可能です。このチップは基本的にファイアウォール、NBAR、NetFlow など Cisco IOS ソフトウェアの機能を集中的に高速化して、ルータ内に外部サービス ブレードを設置する必要性を低減します。
- Cisco QuantumFlow Traffic Manager：数百のカスタマイズされたネットワーク プロセッサ リソースを備えるハードウェア キューイング エンジンであり、それぞれのリソースは数々のアプリケーションを、柔軟なフローによってネットワーク内のあらゆる場所の 100,000 を超えるキューへと処理します。このチップにより、高速でスケーラビリティの高い QoS が実現し、性能低下を最小限に抑えたシェーピング、ポリシングなどの機能が展開できます。

また、ESP のオンチップおよびオフチップのリソースによって QuantumFlow Processor に搭載された次の機能が高速化されます。

- 暗号化エンジンは複数のパケット処理コアを搭載し、暗号化機能を高速化して最大 7 Gbps の IPsec スループットを実現します。このエンジンは Packet Processing Elements（PPE）からアクセスされます。PPE によってパケットがトラフィック マネージャに送信され、バッファおよびキューされた後、暗号化エンジンにスケジュールされます。暗号化操作が完了すると、パケットは PPE に戻され、さらにパケット処理が行われます。

All contents are Copyright © 1992–2011 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

- スケーラブルな IP マルチキャスト暗号化：暗号化エンジンの複数のコア、暗号化エンジンと QuantumFlow Processor 間のフルサークル バックプレッシャー メカニズム、そして大規模な暗号化エンジン バッファの 3 つのメカニズムすべてが、スケーラビリティの高い IP マルチキャスト暗号化を可能にするために設計されており、暗号化エンジン宛ての複製されたパケットでバーストが発生した場合にパケット ドロップを回避します。
- マルチギガビット パフォーマンス ファイアウォール：20 Gbps の ESP（ESP20）を搭載する強力なマルチコア QuantumFlow Processor では、Cisco IOS ファイアウォールおよび NAT をスループット最大 20 Gbps で提供します。このパフォーマンスはルーティング、QoS、NetFlow などの重要な機能が有効にされていても維持可能です。
- その他のリソースは、パケットの処理時の高度分類化およびハードウェア機能の高速化におけるネットワーク アドレスのルックアップ、ネットワーク プレフィクスのルックアップ、ハッシュのルックアップ、Weighted Random Early Detection（WRED; 重み付けランダム早期検出）、トラフィック ポリシング、範囲ルックアップ、および高度な分類と ACL 高速化のための Ternary Content Addressable Memory（TCAM）などで、QuantumFlow Processor を支援します。

ソフトウェア アーキテクチャ：ソフトウェアの冗長性

6 ラックユニット（6RU）Cisco ASR 1006 は冗長ルート プロセッサおよび ESP を搭載しています。各ルート プロセッサはそれぞれ Cisco IOS ソフトウェアのコピーを実行することができ、相互に In Service Software Upgrade（ISSU）を設定できるため、システムは障害から迅速に回復できます。2RU Cisco ASR 1002 および 4RU Cisco ASR 1004 には、単一のルート プロセッサと単一の ESP が搭載されているため、ハードウェアでは冗長性を実現できません。代わりに、ハイ アベイラビリティはソフトウェアで提供されています。

- Cisco IOS ソフトウェア 2 つを単一のルート プロセッサ上で実行し、相互に Nonstop Forwarding with Stateful Switchover（NSF SSO; ステートフル スイッチーバーでのノンストップ フォワーディング）を実行できます。たとえば、アクティブな Cisco IOS ソフトウェアで Open Shortest Path First（OSPF）の隣接関係を構築して OSPF データベースにデータを追加している間、スタンバイの Cisco IOS ソフトウェアでは、プロセス間通信メッセージを通して最新の状態が維持されます。これにより、アクティブな Cisco IOS ソフトウェアに障害が発生し、スタンバイの Cisco IOS ソフトウェアが引き継ぐ場合、データベースのもう 1 つのコピーがいつでも利用可能な状態にあることになり、OSPF データベースは隣接関係を失うことなく維持されます。
- ISSU は Cisco IOS ソフトウェアおよび SPA ドライバに対してサポートされており、サービスを中断することなくシステムを更新できます。
- ハードウェアで実行される Control-Plane Protection（CoPP; コントロール プレーン保護）メカニズムによって最大の保護と復元力が提供され、大規模の DDoS 攻撃が発生しても、システムは運用可能かつ管理者がアクセスできる状態に維持されます。

Cisco Self Defending Network（SDN; 自己防衛型ネットワーク）

Cisco ASR 1000 シリーズ ルータは Cisco Self-Defending Network（SDN; 自己防衛型ネットワーク）を構成するコンポーネントです。SDN は、組織がネットワークのセキュリティ脅威に対して識別、防御、適応することを可能にするアーキテクチャ フレームワークです。SDN は、Network Foundation Protection を基礎として、シスコ統合型セキュリティ システム、シスコ コラボレーション セキュリティ システム、シスコ適応型防御システムに基づいて構築されています。

シスコ統合型セキュリティは、ルータやスイッチ、アプライアンス、エンドポイントなどのネットワーク要素すべてを防御ポイントとすることで、ネットワーク セキュリティに進化をもたらしています。ルータをネットワーク保護の重要なデバイスとするシスコ統合型セキュリティの中核的な要素には、セキュアな接続、統合型脅威防御、信頼性、識別などがあります。

All contents are Copyright © 1992–2011 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

- セキュアな接続：この機能は、複数のタイプのトラフィックに対応するセキュアでスケーラブルなネットワーク接続を提供します。対応するトラフィックには、IPsec VPN、Dynamic Multipoint VPN（DMVPN）、Enhanced Easy VPN などが含まれます。
- 統合型脅威防御：この機能はネットワーク サービスを利用したネットワーク上の攻撃および脅威を防御し、対処します。防御機能には、Cisco IOS ファイアウォール、NetFlow、そして Flexible Packet Matching（FPM）などが含まれます。
- 信頼性と識別：この機能では、Authentication, Authorization, and Accounting（AAA; 認証、許可、アカウンティング）や Public Key Infrastructure（PKI; 公開鍵インフラストラクチャ）などのテクノロジーを使用して、ネットワークがインテリジェントにエンドポイントを保護します。

シスコ コラボレーション セキュリティ システムは、エンドポイント、ネットワーク、ポリシーを含むネットワーク全体にセキュリティが適用されるシステムです。たとえば、NetFlow コレクタは DDoS 攻撃の迅速な識別を支援し、発信元ベースの Remotely Triggered Black Hole（RTBH）フィルタリングによって、攻撃ポイントすべてで必要なあらゆるリアルタイムの防御を形成します。複数のサービスとデバイスが相互に連携して積極的な管理で攻撃を阻止します。

シスコ適応型防御システムは、複数のレイヤで動的に脅威に対応し、ネットワーク トラフィック、エンドポイント、ユーザ、アプリケーションのより厳密な制御を可能にすることで、セキュリティのリスクを最小化します。また、サービスをより少ない数のデバイス上に統合することで運用コストを抑えながら、アーキテクチャ設計を簡素化することもできます。これは、セキュアなマルチレイヤ インテリジェンス、アプリケーション保護、ネットワーク全体の制御、そして脅威の封じ込めを高性能のソリューションに組み合わせた革新的なアプローチです。

Cisco Network Foundation Protection（NFP）は、特にネットワーク レベルでネットワーク インフラストラクチャを攻撃と脆弱性から保護する Cisco SDN の大きな一部を成すコンポーネントです。これには、ハードウェアベースの CoPP、および高速化された NBAR、RTBH フィルタリング、そして Unicast Reverse Path Forwarding（URPF）などがあります。

Cisco ASR 1000 シリーズ ルータのセキュリティの機能と利点

Cisco ASR 1000 シリーズ ルータでは、ネットワーク セキュリティ機能を有効にする次の Cisco IOS ソフトウェア フィーチャ セットが用意されています。

- Advanced IP Services
- Advanced Enterprise Services

最適なフィーチャ セットの選択に関する詳細情報は、Cisco IOS XE フィーチャ セット搭載 Cisco ASR 1000 ルータ に関する製品速報 を参照してください。

Cisco ASR 1000 シリーズ ルータで多くのセキュリティ機能を使用するには、機能ライセンスが必要です。表 1 に機能とそれぞれを有効にする対応機能ライセンスを示します。

表 1　Cisco ASR 1000 シリーズ ルータ向けセキュリティ機能ライセンス

機能	必要な機能ライセンス
IPsec、Easy VPN、DMVPN、Voice and Video Enabled VPN（V3PN）、Virtual Tunnel Interface（VTI; 仮想トンネル インターフェイス）、セキュア プロビジョニングおよびデジタル証明書、IPsec ハイ アベイラビリティ、Cisco IOS ソフトウェア証明書サーバ	FLASR1-IPSEC-RTU
Cisco IOS ファイアウォールおよびファイアウォール ハイ アベイラビリティ	FLASR1-FW-RTU
NBAR および FPM	FLASR1-FPI-RTU

表 2 に Cisco ASR 1000 シリーズ ルータの統合型セキュリティの機能と利点を示します。リストにある機能のほとんどについては、この文書内で追加情報にリンクされています。

All contents are Copyright © 1992–2011 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

表 2　Cisco ASR 1000 シリーズ ルータの主な統合型セキュリティの機能と利点

機能	説明と利点
セキュアな接続	
IPsec	サポートされている IPsec 規格は、暗号化向けの Digital Encryption Standard（DES）、Triple DES（3DES）、Advanced Encryption Standard（AES; 128、192、256）、認証向けの Rivest、Shamir、Aldeman（RSA）アルゴリズム シグネチャおよび Diffie-Hellman、データ整合性向けの Secure Hash Algorithm 1（SHA-1）、または Message Digest Algorithm 5（MD5）ハッシング アルゴリズムなどです。ESP 内蔵の暗号化エンジンで、Cisco ASR 1000 シリーズ ルータは最大 7 Gbps IPsec スループットを実現します。
ハードウェア QoS	QuantumFlow Processor 内の専用 QoS チップが、数千の VPN スポークのトラフィック シェーピングおよびポリシング機能を促進し、また暗号化前後の Low Latency Queuing（LLQ; 低遅延キューイング）も含め、すべてが音声とリアルタイム データの品質維持を目的としています。
ハードウェア IP マルチキャスト処理	拡張 2 Gb バッファを装備した強力なマルチコア暗号化エンジンと、暗号化エンジンと処理エンジン間のフルサークル バックプレッシャー メカニズムが、大規模 IP マルチキャストでこれまで課題となっていたバーストの問題を解決します。
Cisco Easy VPN および Enhanced Easy VPN	IPsec 規格に高度な付加価値を提供するこれらの機能は、新しいセキュリティ ポリシーを中央ヘッドエンドのルータからリモート サイトへ能動的にプッシュすることで、ポイントツーポイント VPN の管理と維持を容易にします。Enhanced Easy VPN 機能はダイナミック VTI と統合し、最大限の使いやすさと高度なユーザ単位およびトンネル固有の機能を実現します。
Dynamic multipoint VPN（DMVPN; ダイナミック マルチポイント VPN）	複数の場所の間で仮想フルメッシュ IPsec 接続を確立するスケーラブルで柔軟な方法を提供する、サイトツーサイト VPN における革新技術です。DMVPN は高度なスポークツースポーク機能を備え、遅延の影響を受けやすい音声アプリケーションのパフォーマンスを向上します。従来のハブアンドスポークのモデルでは、DMVPN によって展開の複雑さが大幅に緩和されます。
Group Encrypted Transport VPN	Group Encrypted Transport VPN により、プライベート WAN 環境において、ネットワーク インテリジェンスとデータ プライバシーのバランスに関して妥協する必要がなくなります。VPN のプロビジョニングと管理が簡略化されるため、サービス プロバイダーはプロビジョニングと管理に煩わされることなく、管理された暗号化を提供することができるようになります。Group Encrypted Transport VPN は、VPN にトンネルを使用しない新たなカテゴリとなります。
Virtual Tunnel Interface（VTI; 仮想トンネル インターフェイス）	直接 IPsec で設定することができます。VTI は、Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）内でのカプセル化などの代替手段に比べ、VPN の構成と設計を大幅に簡素化します。ユーザ単位の属性およびトンネル固有の機能が可能になるため、管理者は細かい要求に柔軟に対応することができます。スタティックとダイナミックの両方の VTI がサポートされています。
セキュア プロビジョニングおよびデジタル証明書	この強力なメカニズムは、新しいリモート ノードを厳しいセキュリティでネットワーク インフラストラクチャに登録します。
ハイ アベイラビリティ	Cisco ASR 1000 シリーズ ルータ では、シャーシ内 ESP ツー ESP の IPsec ステートフル フェールオーバーを含む、いくつかの VPN 冗長性オプションをサポートします。
統合型脅威防御	
Cisco IOS ゾーンベース ファイアウォール	Cisco IOS ファイアウォールは、ネットワークへの WAN エントリ ポイントの保護に最適な単一デバイス セキュリティおよびルーティング ソリューションです。ゾーンベースのファイアウォールは、物理インターフェイスと仮想インターフェイスをゾーンにグループ化し、論理ネットワーク トポロジを簡素化します。これらゾーンの形成により、各インターフェイスで個別にポリシーを設定する代わりに、ファイアウォール ポリシーをゾーンごとに適用することができます。強力な QuantumFlow Processor を搭載した Cisco ASR 1000 シリーズ ルータの Cisco IOS ファイアウォールは、最大 20 Gbps のスループットを実現します。
NetFlow	NetFlow は、異常に基づいた DDoS 攻撃の検出と、攻撃元の追跡および攻撃への反応に役立つデータをリアルタイムで提供します。
NBAR	ディープ インスペクション メカニズムの NBAR は、幅広いアプリケーションを認識して分類することで、それらをコントロールします。アプリケーションを分類すると、ネットワークはそのアプリケーションに対して特定のサービスを提供することができます。
FPM	FPM はパケットのヘッダーまたはペイロード内での柔軟で詳細なレイヤ 2 ～ 7 のパターンマッチを使用して、ネットワークの脅威および主要なワームやウイルスに対する迅速な第一線の防御を提供します。
ハイ アベイラビリティ	ファイアウォール ステートフル フェールオーバーは、アクティブなセッションを中断することなく、シャーシ間の RP ツー RP のフェールオーバーと ESP ツー ESP のフェールオーバーをサポートします。
信頼性と識別	
認証、認可、アカウンティング（AAA）	AAA を使用すると、管理者は回線（ユーザ）単位またはサービス単位（たとえば IP、Internetwork Packet Exchange [IPX]、または Virtual Private Dialup Network [VPDN]）で、必要な認証および許可の種類を動的に設定できます。

All contents are Copyright © 1992–2011 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Cisco Network Foundation Protection	
ACL	ACL は、エッジ ルータの宛先アドレスに送信できる正規のトラフィックを明示的に許可することで、エッジ ルータを悪意のあるトラフィックから保護します。
CoPP	CoPP は、コントロール プレーン プロセッサ宛のトラフィックのレートを制限することで DDoS 攻撃の成功を阻止し、攻撃を受けていてもネットワークのアベイラビリティを維持します。CoPP はハードウェアの QuantumFlow Processor で実行されます。
Cisco IOS ソフトウェアのモジュール性およびカーネル保護	Cisco IOS ソフトウェアはそれ自体のメモリ領域内に保持されます。ネットワークがたとえば DDoS 攻撃などによる重度の負荷を受けていても、システムは運用可能で管理に応答できます。
QoS ツール	QoS は、帯域幅を制限するか、攻撃的なトラフィックをドロップするように QoS ポリシーを定義することで、DDoS 攻撃から保護します（識別、分類、帯域制限）。
受信 ACL	受信 ACL は、明示的にトラフィックを許可または拒否することによって、ルート プロセッサに転送されるトラフィックのタイプを制御します。
ロールベースの CLI アクセス	この機能はコマンドライン インターフェイス（CLI）コマンドにビューベースのアクセスを提供し、ルータでネットワーク操作、セキュリティ操作、エンド ユーザを高度にセキュアに論理分離します。
ルーティング保護	この機能は MD5 ピア認証と再分配保護を使用して、ルーティング ピアを検証し、ルーティングの安定性を向上すると共に、過負荷から保護します。
Secure Shell（SSH）プロトコル バージョン 2	SSHv2 は認証および暗号化などで、デバイスへのセキュアなオペレータ アクセスを提供します。
Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）バージョン 3	SNMPv3 を使用すると、カスタマー アプリケーションのデバイスをセキュアに、かつ標準に準拠した形で管理および制御できます。
送信元アドレスに基づく RTBH フィルタリング	この機能は IP ルーティング機能の組み合わせを使用して、DDoS 攻撃に対し回線速度でリアルタイム防御を提供します。
URPF	URPF は確認できる IP 送信元アドレスを持たない IP パケットを廃棄することで、不正な形式やなりすましの IP 送信元アドレスのネットワーク侵入によって起こる問題を軽減します。

セキュアな接続

一般的な IP ネットワークでは、正規および不正なアプリケーションの両方を含む、数えきれないほどのアプリケーションが実行されており、パフォーマンスの影響を受けやすい音声やビデオ、リアルタイム データ アプリケーションと競合しています。たとえば、音声トラフィックは遅延の影響を受けやすく、通常サイズが小さい音声パケットは、より大きな重要度の低いデータ パケットの後ろにキューされてしまうと、ユーザはすぐに雑音として品質の低下を感じます。ビデオ トラフィックは高帯域幅を消費し、ジッタの影響を受けやすい特徴があります。遅延中にビデオ データをバッファすることは非効率なため、迅速に安定したストリームに戻すために通常、パケットは廃棄されます。このパケット損失が頻繁に起こると、ストリームが途切れ途切れになり、ユーザは不快に感じます。

企業向け音声およびビデオ アプリケーションには、音声とビデオの品質を維持する最先端の QoS と IP マルチキャスト メカニズムが必要です。サイトツーサイトおよびリモート アクセス VPN の目的は、この混合トラフィックを暗号化されたユビキタスで、安価な公衆インターネット アクセスによってプライマリ接続およびバックアップ接続の両方向けに送信することです。音声およびビデオ アプリケーションの品質を VPN に拡張するには、IPsec と QoS または IP マルチキャストの組み合わせが必要となります。これまでは、このような課題によって拡張性が制限され、あるいはネットワーク設計が複雑化してきました。しかし VPN の採用が拡大し、リアルタイム アプリケーションが急増するにつれ、Voice over IP（VoIP）および IPTV が主流となっていくと同時に Cisco TelePresence™ の人気が高まり、ビデオ テレフォニーの拡大が予測されます。このような状況により、集約サイトにおけるパフォーマンス、規模、機能統合に対する要件も高まっています。

Cisco ASR 1000 シリーズ ルータは、スケーラビリティに優れたマルチギガビット VPN を音声、ビデオ、そしてリアルタイム データ統合と共に提供します。

- IPsec AES、DES、3DES 暗号化がプラットフォームに組み込まれ、サービス ブレードは必要ありません。

All contents are Copyright © 1992–2011 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

- 20 Gbps ESP（ESP20）が最大 4000 のトンネルと 7 Gbps IPsec パフォーマンスをサポートします。
- 将来のバージョンと互換性のあるアーキテクチャで、シャーシなどのコンポーネントを置き換えることなく ESP をアップグレードすることで暗号化を強化できます。
- サイトツーサイトおよびリモート アクセス VPN は、IPsec、Group Encrypted Transport VPN、DMVPN、Easy VPN、VTI（スタティックおよびダイナミック）などがサポートされます。
- サービス ブレード不要のハードウェア QoS、および最先端の暗号化 IP マルチキャスト処理で、音声とビデオを IPsec と統合するスケーラビリティに優れた設計を実現します。
- PKI 機能により、サイトツーサイトおよびリモート アクセスの両方において、事前共有セキュリティ キーと証明書に対応します。Cisco IOS ソフトウェア証明書サーバがセキュアなネットワークのプロビジョニングを容易にします。

ハードウェア QoS

Cisco ASR 1000 シリーズ ルータでは、QuantumFlow Processor に QoS 処理が組み込まれています。

- トラフィック プロセッサ：QuantumFlow Processor には QoS 専用のチップ 1 基が搭載されており、ルート プロセッサそのものにほぼ影響することなく、数千のスポークに対するトラフィックシェーピングおよびポリシング機能を促進します。従来の単一 CPU のミッドレンジ ルータでは、上述のような条件ではルート プロセッサに負荷がかかり、ネットワークのアベイラビリティに大きく影響する可能性があります。
- VPN 上での音声品質を確約するためには暗号化前の LLQ が非常に重要です。QuantumFlow Processor はハードウェア LLQ と、この規模のプラットフォームにおける業界最先端の機能である暗号化後のインターフェイスレベル QoS を提供します。

ハードウェア IP マルチキャスト処理

これまで、暗号化 IP マルチキャスト パケット（たとえば、IPTV やビデオ会議ストリーム）は、規模に制限がある状態でのみ可能でした。たとえば、企業のイベントは通常特定の時刻に開始されますが、同じ時刻に多くのユーザがオンラインでイベントに参加しようとすると、トラフィックの急増が起こります。大量の数のパケットが複製され、暗号化のためにキューされることで、暗号化プロセッサのキュー バッファがいっぱいになり、入力インターフェイスで好ましくないパケット廃棄が生じます。この問題を解決するための従来のアプローチは、暗号化 IP マルチキャスト トラフィックを分離するために複数のピアとトンネルを使用した複雑な設計が必要でした。

Cisco ASR 1000 シリーズ ルータでは、暗号化 IP マルチキャスト トラフィックが合理的に処理されます。3 つの主要なプロビジョンでパケット ドロップを最小限に抑え、IP マルチキャスト トラフィックの暗号化を実行しながらネットワーク設計を簡素化します。

- マルチコア暗号化エンジン：ESP 内の暗号化プロセッサにはマルチコア チップが搭載されています（10 Gbps ESP は 8 コア チップ搭載）。パケットは暗号化のため複数のコアに並行して送られ、実質的により強力なパフォーマンスが得られ、暗号化エンジンが一定の時間内により多くのパケットを処理できるようになります。
- 暗号化エンジンと QuantumFlow Processor 処理エンジン間のフルサークル バックプレッシャーメカニズム：従来では、ほぼ瞬時に起こる IP マルチキャスト バースト トラフィックの結果、フォワーディング プロセッサとパケット プロセッサで処理不能なパケット バーストを相互に送信し合い、バッファにより負担がかかっていました。Cisco ASR 1000 シリーズ ルータでは、複数のメカニズムで暗号化エンジンと処理エンジン（QuantumFlow Processor 内のパケット処理エンジン）の両方が相互にバックプレッシャーを適用し合い、パケットを保留することでバックプレッシャーに対応しています。これにより、バーストを円滑化し、パケット ドロップを最小限に抑えることができ

All contents are Copyright © 1992–2011 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

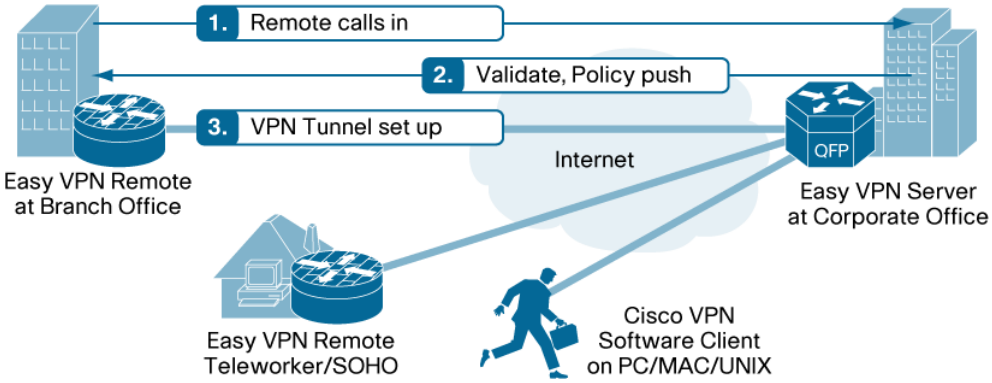
ます。このプロセスで重要なのは、QuantumFlow Processor が処理エンジンに加えて、Buffering, Queuing, and Scheduling（BQS; バッファリング、キューイング、スケジューリング）システムを装備した専用のトラフィック プロセッサを搭載していることにあります。暗号化のためにシステムに進入するパケットは BQS に送られ、ここで暗号化エンジンの暗号化の準備が整うまで待機します。つまり、暗号化エンジンが処理エンジンにバック プレッシャーを適用することができます。暗号化エンジンの準備が整い、パケットを暗号化すると、暗号化エンジンはパケットをフローに再挿入します。これを受けて今度は処理エンジンがバック プレッシャーを適用し、これらパケットを受信する余裕がないことを示して暗号化エンジンに速度を落とさせることができます。実質的にこのプロセスは、暗号化エンジンと QuantumFlow Processor の間でバックプレッシャー メカニズムのフルサークルを形成します。

- 大容量暗号化エンジン バッファ：暗号化エンジンは 2 MB のバッファを内蔵しています。

Easy VPN および Enhanced Easy VPN

シンプル、高い拡張性、リモートアクセス、という要件に対応するため、シスコは豊富な機能とポリシー制御を維持しながら、「ポリシープッシュ」テクノロジーを使って構成を簡素化した、Easy VPN ソリューションを提供します。本社で定義される Easy VPN サーバによってリモート VPN デバイスにセキュリティ ポリシーがプッシュされ、接続が確立される前に、これらの接続に最新のポリシーが適用されていることを確約します（図 4）。

図 4　Easy VPN トンネルのセットアップ



Easy VPN には次のような利点があります。

- Easy VPN は同一のセントラルサイト ルータを使用して、ハードウェア（アクセス ルータ）CPE とソフトウェア リモート アクセス クライアントの両方をサポートします。Cisco VPN クライアント ソフトウェアを Windows、Mac、および UNIX システムにインストールすることで、コストをかけずに、ルータベースの VPN にリモート アクセス接続機能を拡張できます。ハードウェア CPE とソフトウェア クライアントの両方に対して単一のテクノロジー（Easy VPN）を使用することで、プロビジョニング、モニタリング、AAA サービスが簡素化かつ一元化されるため、総所有コスト（TCO）が削減されます。
- Easy VPN は、CPE ルータと個々のユーザに対して、ローカル（ルータベース）または中央集中型の RADIUS および AAA 認証を可能にします。
- Easy VPN はデジタル証明書をサポートするため、事前共有キーを介してセキュリティを強化できます。
- 複数のセントラルサイト Easy VPN コンセントレータを対象とした負荷分散を可能にします。バックアップ コンセントレータ情報を CPE にポリシーでプッシュするため、CPE を設定し直すことなく、ソリューションを拡張できます。

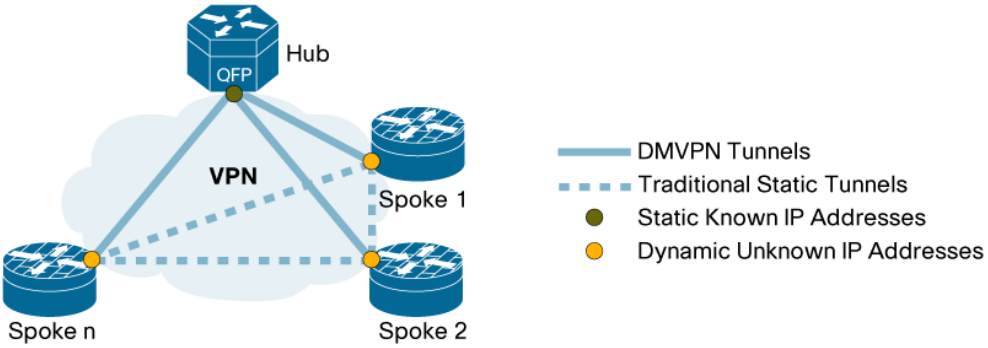
All contents are Copyright © 1992–2011 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

- Easy VPN サーバを仮想化することで、サービス プロバイダーは単一のプラットフォームで複数の顧客に対して VPN サービスを提供できます。
- Easy VPN は、動的な QoS ポリシー割り当て、ファイアウォールと IPS、スプリット トンネリング、パフォーマンス モニタリングのための Cisco IP SLA および NetFlow などすべての機能が統合されます。
- Easy VPN は、Cisco IOS ソフトウェア、Cisco ASA アプライアンスなど、すべてのシスコ VPN 製品ラインでサポートされています。
- Enhanced Easy VPN 機能を VTI と統合すると、仮想インターフェイスを直接 Easy VPN で構成できるため展開が容易になり、高度なネットワーク統合が可能になります。VTI を使って(または AAA サーバからダウンロードして)IP サービスを設定でき、接続時にはこれらのテンプレートから VTI インスタンスが動的にクローンされるため、ヘッドエンドとリモート ブランチ オフィスの設定要件を大幅に簡略化できるというメリットがあります。各リモート サイト向けに無数の似たようなコマンドを手動で作成する必要はありません。
- QoS などユーザ単位の属性:VTI はユーザ単位のポリシー設定を簡素化します。管理者は要求されるアプリケーション パフォーマンスを予防的に提供し、ユーザの生産性と動機付けを維持することができます。
- トンネル固有の機能:VTI は、各ブランチオフィス VPN トンネルの設定をそれぞれの一連のパラメータで行うことを可能にし、サイト固有のニーズに基づいて設定とセキュリティをカスタマイズする柔軟性を提供します。

Dynamic Multipoint VPN(DMVPN)

シスコのルータには DMVPN 機能が搭載されています。シスコの DMVPN は、オンデマンドのスケーラブルなフルメッシュ VPN を構築できるため、遅延時間の短縮、帯域幅の節約、VPN 展開の簡略化が可能です(図 5)。DMVPN 機能は、シスコの IPSec とルーティングにおける専門知識に基づいて構築されており、この機能を使用すれば、GRE トンネル、IPSec 暗号化、Next Hop Resolution Protocol(NHRP)、OSPF、Enhanced Interior Gateway Routing Protocol(EIGRP)を動的に設定できるようになります。

図 5 DMVPN



DMVPN の能力は企業の本社で真に発揮されます。VPN トンネルの動的構成を QoS や IP マルチキャストなどのテクノロジーと組み合わせ、管理上の負担を軽減しながら、遅延の影響を受けやすいアプリケーションを最適化できます。たとえば、WAN リンクでの IP 転送ネットワークの音声およびビデオ アプリケーションと同様のパフォーマンスを、DMVPN を使ってセキュアかつ効率的に得ることができます。

DMVPN は、企業のブランチ オフィス、在宅勤務者、エクストラネット接続の組み合わせに幅広く利用されており、主に次のような利点があります。

All contents are Copyright © 1992–2011 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

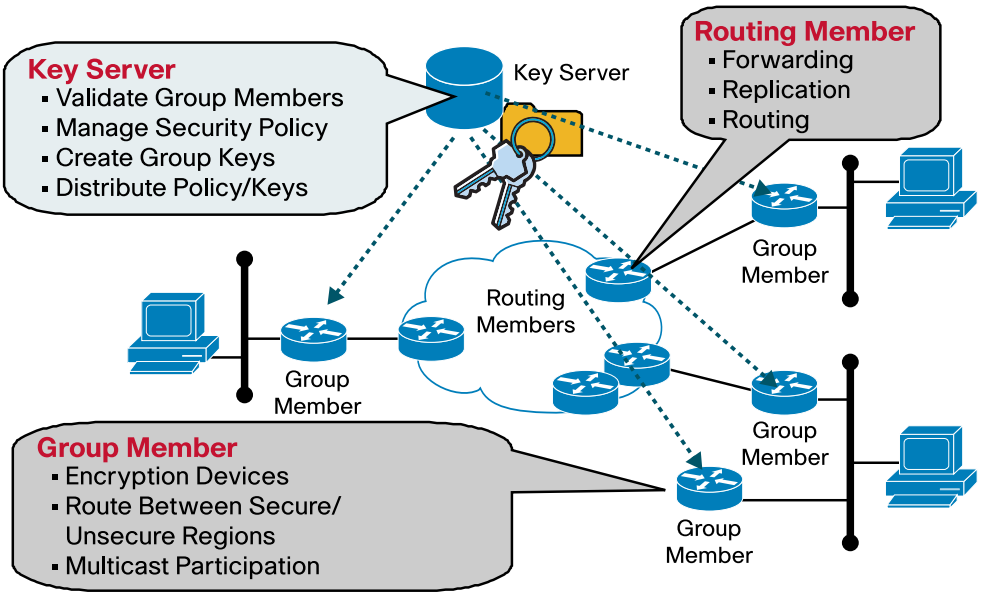
- ハブとスポークのシンプルな構成でフルメッシュの接続を提供
- IPsec トンネルの構築に IPsec 自動トリガリングを搭載
- 新しいスポーク追加をゼロタッチ設定でサポート
- 動的アドレスのスポークをサポート

Group Encrypted Transport VPN

トンネルの必要性をなくす革新的でスケーラブルな VPN を実現する Group Encrypted Transport VPN は、VPN に新たなカテゴリを確立します。暗号化された IP ユニキャストと IP マルチキャスト パケットを、ルーティング プロトコルの決定に基づいて直接リモート サイトにルーティングしたり、障害のあるパスを避けて再ルーティングしたりすることができ、アベイラビリティが向上します。組織は既存のレイヤ 3 ルーティング情報を利用できるため、非効率的なマルチキャスト レプリケーションを解消して、ネットワーク パフォーマンスを向上させることができます。分散型ブランチ ネットワークでは、QoS、ルーティング、マルチキャストなど、音声とビデオの品質に不可欠なネットワーク インテリジェンス機能を維持したまま、規模を拡張できます。

Group Encrypted Transport VPN は、「信頼できる」グループ メンバーというコンセプトに基づく、標準に準拠した新しい IPsec セキュリティ モデルを提供します。信頼できるメンバー ルータは、あらゆるポイントツーポイント IPSec トンネル関係から独立した、共通のセキュリティ方式を使用します。キー サーバは、登録および認証されたすべてのメンバー ルータにキーとポリシーを配布します（図 6）。

図 6　グループ セキュリティ機能



Group Encrypted Transport VPN はさまざまな用途にメリットがあります。

- データ セキュリティとトランスポート認証を提供し、すべての WAN トラフィックを暗号化することで、セキュリティ準拠や内部規制の要件を満たすことができます。
- グループ暗号キーを使用することで、大規模ネットワーク メッシュを可能にし、ピアツーピアの複雑なキー管理を排除できます。
- Multiprotocol Label Switching（MPLS）ネットワークでは、フルメッシュ接続、ナチュラル ルーティング パス、QoS などのネットワーク インテリジェンスを維持できます。
- 中央集中型のキー サーバでメンバシップを簡単に制御できます。

All contents are Copyright © 1992–2011 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

- 中央のハブを経由する必要がないダイレクトで常時アクティブな通信をサイト間で実現することにより、遅延とジッタを低減できます。
- マルチキャスト トラフィックの複製にコア ネットワークを使用し、個々のピア サイトでパケット複製が行われないようにすることで、顧客宅内機器（CPE）およびプロバイダーエッジ暗号化デバイスのトラフィック負荷を軽減できます。

仮想トンネル インターフェイス（VTI）

VPN はセキュアな WAN 接続のための主流のソリューションとして認識されつつあります。VPN は専用回線、フレーム リレー、ATM を使用する既存のプライベート ネットワークを代替または補強して、リモート オフィスおよびブランチ オフィス、中央サイトにより高い費用対効果と柔軟性で接続します。この新しい環境では、VPN デバイスに高いパフォーマンス、LAN および WAN インターフェイスに対するサポート、そして高いネットワーク アベイラビリティが求められます。

新しい Cisco IPsec VTI ツールを使用すると、サイトツーサイト デバイス間に IPsec ベースの VPN を構成することができます。IPsec トンネルの終端にルーティング可能なインターフェイスを提供することで、構成を簡略化します。Cisco IPsec VTI トンネルは、共有 WAN 全体に専用の経路を提供し、新しいパケット ヘッダーでトラフィックをカプセル化して、指定された宛先にトラフィックを確実に送信します。トラフィックはエンドポイントでのみ進入できるため、このネットワークはプライベートです。また、IPsec は（暗号化と同様に）真の機密性を提供し、暗号化されたトラフィックを搬送できます。

Cisco IPsec VTI で、企業は費用対効果の高い VPN をフルに活用し、品質と信頼性に関して妥協することなく、音声およびビデオをデータ ネットワークに追加し続けることができます。このテクノロジーはサイトツーサイト VPN に非常にセキュアな接続を提供し、統合された音声、ビデオ、データを IP ネットワーク経由で伝送できます。

本社向けのハイ アベイラビリティおよび負荷分散

Cisco ASR 1000 シリーズ ルータは IPsec VPN 向けにいくつかの冗長機能をサポートしています。

- シャーシ内 IPsec ステートフル フェールオーバー：計画された、または予期しない障害が発生しても IPsec パケットの処理と転送を継続するために、バックアップ IPsec 処理に切り替えることができます。この機能は 6RU Cisco ASR 1006 ルータに搭載されています。IPsec ステートフル フェールオーバーは同一シャーシ内の 2 つの ESP 間で行われます。一方の ESP がアクティブの間、他方はホット スタンバイの状態にあり、バックアップの ESP に切り替わっても IPsec セッション情報が保存されます。原因にかかわらず、アクティブなルータの接続が切断されてもピアとのセキュアな接続は維持されます。このプロセスはエンド ユーザに対して透過的であり、リモート ピアの調整や再構成は不要です。IPsec ステートフル フェールオーバーは Cisco ASR 1000 シリーズ ルータで、2 つの ESP 間のステートフル スイッチオーバー（SSO）と合わせて動作するように設計されています。IPsec、GRE カプセル化 IPsec、Cisco IOS ソフトウェア Easy VPN トラフィックを保護します。

All contents are Copyright © 1992–2011 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

統合型脅威防御

QuantumFlow Processor アーキテクチャは、ミッドレンジ ルータ セキュリティにおいて大きな変化をもたらします。これによって Cisco ASR 1000 シリーズ ルータは、アドオン サービス ブレードを追加せずに、ハードウェアを高速化するマルチギガビットの統合型脅威防御サービスを、世界水準の IP ルーティングおよびセキュアな接続と組み合わせることができます。

ファイアウォール、NBAR、NetFlow、送信元に基づく RTBH などの統合型脅威防御サービスが標準搭載されており、いずれもネットワーク エッジでのリスク軽減の方法として、ネットワークおよびセキュリティの専門家に使用されているという実績があります。

これらの機能はすべて QuantumFlow Processor そのもので実行されます。つまり、セッション パケット（レイヤ 4、ディープ パケット インスペクション、NBAR、FPM）はすべて QuantumFlow Processor で実行されます。最初のファイアウォール セッション セットアップ パケットでさえもハードウェアで処理されるため（一般に「高速パス」と呼ばれる）、ファイアウォールは「低速パス」での処理にはなりません。また、QuantumFlow Processor は直接、フォワーディング プレーン上で高速ファイアウォールおよび NAT の syslog を実行し、ルート プロセッサのパフォーマンス低下や負荷を最小限にします。

Cisco IOS ゾーンベースのファイアウォール

Cisco ASR 1000 シリーズ ルータに搭載された Cisco IOS ゾーンベースのファイアウォールは、マルチギガビット ステートフル ファイアウォール インスペクションを実行し、1 台 でセキュリティとルーティング ソリューションを提供して、ネットワークへの WAN エントリ ポイントを保護します。

ファイアウォール サービスは Cisco ASR 1000 シリーズ ルータ内の Cisco QuantumFlow Processor に組み込まれており、追加のファイアウォール ブレードやモジュールは必要ありません。同時に、システムは QoS、IPv4、IPv6、NetFlow などの機能もマルチギガビットの速度で実行します。

Cisco IOS ファイアウォールの主な機能は次をサポートします。

- ゾーンベースのポリシー：ゾーンベースのポリシーにより、Cisco ASR 1000 シリーズ ルータは同一ゾーンのメンバーではない任意のインターフェイス間の境界として動作します。各ゾーン ペアの間で明示的なゾーン ペア ポリシーが各方向に指定されていない限り、パケットは転送されません。このポリシーは Cisco Policy Language（Modular QoS CLI [MQC]）で記述されており、各ゾーン ペアリングに適用されるステートフル インスペクションのタイプとセッション パラメータを確立します。たとえば、インターネットと DMZ の境界では、HTTP およびドメイン ネーム システム（DNS）が通過できるようにする明示的なポリシーが必要です。
- マルチギガビット パフォーマンス：このアーキテクチャは、ルーティング、QoS、およびその他一般的な Cisco IOS ソフトウェア機能を有効にして、ESP5 で最大 5 Gbps、ESP10 で最大 10 Gbps、そして ESP20 で最大 20 Gbps のファイアウォールと NAT パフォーマンスを実現します。
- シャーシ内のハイ アベイラビリティ：Cisco ASR 1006 は、冗長ルート プロセッサおよび ESP をシャーシ内でサポートすることで、ハードウェアの冗長性をサポートします。アクティブなルート プロセッサまたは ESP で障害が発生すると、ホット スタンバイ コンポーネントがパケットをほぼ損失することなく処理を引き継ぎます。このプロセス中、ファイアウォールおよび NAT セッションはすべて維持されます。Cisco ASR 1002 および ASR 1004 は、2 つの Cisco IOS ソフトウェア イメージを実行することでソフトウェアの冗長機能を提供し、単一のルート プロセッサで一方をアクティブ、他方をスタンバイとして実行します。アクティブなイメージで障害が発生すると、ホット スタンバイのイメージが処理を引き継ぎ、ファイアウォールおよび NAT セッションはすべて確立したまま維持されます。

All contents are Copyright © 1992–2011 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

- 音声、ビデオ、およびその他データ アプリケーションに対する高度なプロトコル インスペクション
- ユーザ単位、インターフェイス単位、またはサブインターフェイス単位のセキュリティ ポリシー
- 加入者単位のファイアウォール：このソリューションは Cisco ASR 1000 シリーズで L2TP Network Server（LNS）として導入されます。Cisco IOS ゾーンベースのポリシー ファイアウォールを Cisco ASR 1000 シリーズの多様なブロードバンド機能セットと組み合わせ、インターネット サービス プロバイダーはブロードバンド加入者に対してファイアウォール サービスを提供できます。
- アイデンティティ識別サービスを緊密に統合して、ユーザ単位で認証と許可を提供
- ロールベースの CLI アクセス：ネットワーク管理者はルータにアクセスする必要のあるユーザのロールに基づいて異なるビューを定義できます。各ビューは、ネットワーク オペレータやセキュリティ オペレータなど、特定のロールのユーザがアクセス可能なあらゆる Cisco IOS ソフトウェア CLI コマンドのサブセットを含みます。

NetFlow イベント ロギング

Cisco ASR 1000 シリーズ ルータはマルチギガビット ファイアウォールおよび NAT syslog を生成します。ESP の QuantumFlow Processor アーキテクチャにより、ルートプロセッサのパフォーマンスを低下させることなく、NetFlow v9 バイナリ ロギング テンプレートを使って直接、フォワーディング プレーン上で数万のファイアウォールおよび NAT イベントをエクスポートすることができます。ESP は毎秒最大 40,000 イベントをエクスポートできます。

NetFlow

NetFlow はネットワークの異常を検出する業界第一のテクノロジーです。たとえば通信データの、ユーザ、使用しているプロトコルおよびポート、経過時間、速度など、IP トラフィックを分析するためのテレメトリ データを提供します。

DDoS 攻撃によってネットワークのスパイクは突然発生します。これらのスパイクは、以前に収集されたプロファイルおよびベースラインから取得した標準トラフィック パターンと比較され、すぐに異常なネットワーク「イベント」として識別されます。NetFlow フロー データを詳細に分析することで、攻撃（攻撃の送信元とターゲット）、攻撃期間、攻撃で使用されたパケットの容量を分類することもできます。

Cisco ASR 1000 シリーズ ルータの Cisco QuantumFlow Processor は、大量のフロー キャッシュ データをプロセッサ上で直接エクスポートできるため（ESP10 は 100 万フロー レコード カード）、ルーティング プラットフォーム内の制御プロセッサによる CPU の使用がさらに減少します。サンプル NetFlow でこのキャッシュの使用が最適化されます。

Network Based Application Recognition（NBAR）

NBAR は、ディープ パケット インスペクションおよびステートフル パケット インスペクションを使用して、Web ベースなどの分類が困難な動的 TCP/User Datagram Protocol（UDP）ポート割り当てを使用するプロトコルを含む幅広いアプリケーションを認識する、Cisco IOS ソフトウェア内の分類エンジンです。セキュリティを目的として使用すると、NBAR はペイロード シグニチャに基づいてワームを検出できます。NBAR がアプリケーションを認識し、分類すると、ネットワークはそのアプリケーションに対してサービスを呼び出すことができます。また、QoS 機能と協調して帯域幅の保証、帯域幅制限、トラフィック シェーピング、パケット カラーリングを提供し、ネットワーク帯域幅の効率的な使用を確約します。

Cisco ASR 1000 シリーズ ルータは QuantumFlow Processor 上で直接 NBAR を高速化し、業界をリードするマルチギガビットのパフォーマンスを実現します。

All contents are Copyright © 1992–2011 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Flexible Packet Matching（FPM）

FPM は攻撃の特性についてパケットを検査し、適切なアクション（ロギング、ドロップ、または ICMP [インターネット制御メッセージ プロトコル] 到達不能）を実行します。FPM はレイヤ 2 ～ 7 に柔軟なステートレス分類メカニズムを提供します。ユーザは、任意のプロトコルおよびトラフィックのプロトコル スタックのフィールドに基づいて、分類基準を指定できます。分類結果に基づいて、分類されたトラフィックに対してドロップまたはロギングなどのアクションを実行できます。

信頼性と識別

認証、認可、アカウンティング（AAA）

Cisco IOS ソフトウェア AAA ネットワーク セキュリティ サービスは、ルータまたはアクセス サーバにアクセス制御をセットアップするためのフレームワークを構築します。AAA により、特定のサービスまたはインターフェイスに適用される方式リストを使用して、回線（ユーザ）単位またはサービス単位（たとえば IP、IPX、または VPDN）で、管理者が必要な認証および許可の種類を動的に設定することが可能になります。

Network Foundation Protection

ネットワーク インフラストラクチャ デバイスの継続的なアベイラビリティは、企業の本社で特に重要になります。ネットワーク ルータまたはスイッチで障害が発生すると、悪意のある人物にネットワーク全体の完全なアクセスを許してしまいます。攻撃に対してはさまざまな防御機能が存在していますが、どの防御を使用するかに関わらず、未知の攻撃に対して保護を行うことは欠かせません。

次のテクノロジーは、DDoS 攻撃が発生した場合の Cisco IOS ソフトウェア デバイスの自己防衛、管理および制御インターフェイスに対するなりすまし攻撃の可能性を最小限に抑えるセキュアな管理アクセスを含め、堅牢な Network Foundation Protection の重要性を強調しています。

Control-Plane Protection

最も堅牢なソフトウェアの実装とハードウェア アーキテクチャでさえも DDoS 攻撃に対しては脆弱です。DDoS 攻撃は、コントロール プレーン プロセッサ宛の特定のタイプのコントロール パケットになりすました無意味なトラフィックでネットワーク インフラストラクチャをフラッディングすることにより、ネットワーク インフラストラクチャを麻痺状態にする悪意のある行為です。

Cisco ASR 1000 シリーズ ルータでは、コントロールとデータ フォワーディング機能を別々のプロセッサに分離し、ルート プロセッサと ESP それぞれに専用の CPU を割り当てることで、防御の第一線を提供しています。ESP がデータ フローを処理し、ルート プロセッサは DDoS 攻撃から隔離されます。

DDoS およびネットワークの心臓部に向けられた類似の脅威をブロックするための第二の防御として、Cisco IOS ソフトウェアには、コントロール プレーンに向けられるトラフィックの速度を制限する、または「取り締まる」、ルータ上のプログラマブルなポリシング機能が提供されています。この Control-Plane Protection（CoPP）と呼ばれる機能は、特定のトラフィック タイプを識別し、すべてまたは特定のしきい値レベルを超過すると制限するよう設定することが可能です（図 7）。

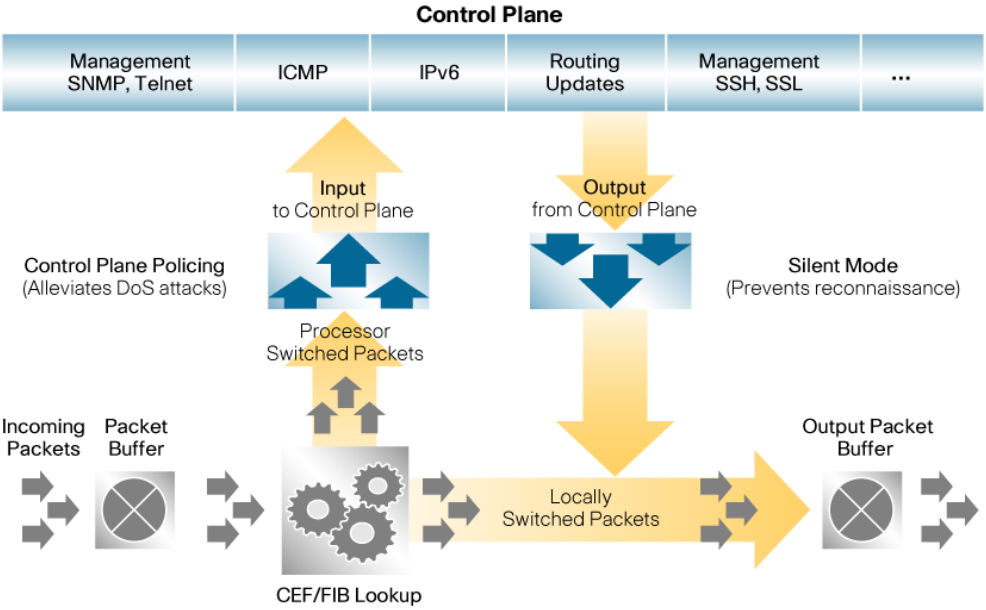
Cisco ASR 1000 シリーズ ルータの CoPP はハードウェア上の QuantumFlow Processor で実行され、CoPP および速度制限機能の実行で追加ペナルティやシステム性能の低下が発生するのをほぼ排除することができます。また、プラットフォームのパント トラフィックは最初に ESP を通過するため、悪意のあるデータがルート プロセッサに進入する機会をさらに低減します。

さらに、Cisco IOS ソフトウェアをユーザ プロセスとして Linux カーネル上で実行することで、システムを保護するレイヤが 1 つ追加されます。このカーネル保護により、DoS 攻撃などでルーティン

All contents are Copyright © 1992–2011 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

グ プロセスに負荷がかかっている場合でも、システムの稼動および管理を継続することができます。

図 7 Control-Plane Protection：パケット バッファ、受信パケット、Cisco Express Forwarding および Forwarding Information Base（FIB; 転送情報ベース）ルックアップ、出力パケット バッファ、サイレント モード



ロールベースの CLI アクセス

ロールベースの CLI アクセスでは、Cisco IOS ソフトウェアへのアクセスを選択的あるいは部分的に提供する一連の操作コマンドおよび設定である「ビュー」を、ネットワーク管理者が定義できます。ビューは Cisco IOS ソフトウェア CLI および設定情報へのユーザ アクセスを制限し、受け入れるコマンドと表示する設定情報を定義することができます。ロールベースの CLI アクセスのアプリケーションには、ネットワーク管理者が特定の機能に対するセキュリティ担当者のアクセスを許可するアプリケーションも含まれます。また、サービス プロバイダーはこの機能を使って制限つきのアクセスをエンド ユーザに付与し、ネットワークのトラブルシューティングを補助することができます。

SSHv2

SSHv2 は強力で新しい認証と暗号化機能を提供します。暗号化された接続を介するトラフィックのトンネルのタイプに、ファイルコピーおよび E メール プロトコルを含む、より多くのオプションが利用できるようになります。デジタル証明書やより多くの 2 ファクタ（T-FA）認証オプションを含む幅広い認証機能によって、ネットワーク セキュリティが強化されます。

SNMPv3

SNMPv3 は、ネットワーク上のパケットの認証と暗号化によってデバイスへのセキュアなアクセスを提供する、ネットワーク管理用の相互運用可能かつ標準規格に基づいたプロトコルです。SNMPv3 では次のようなセキュリティ機能が提供されています。

- メッセージの整合性：伝送中にパケットが改ざんされていないことを確約します
- 認証：メッセージが有効な送信元からであることを確認します
- 暗号化：パケットの内容をスクランブルして、不正な発信元から見えないようにします

SNMPv3 はセキュリティ モデルとセキュリティ レベルの両方を提供します。セキュリティ モデルは、ユーザおよびそのユーザが属するグループに対して設定される認証戦略です。セキュリティ レ

All contents are Copyright © 1992–2011 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

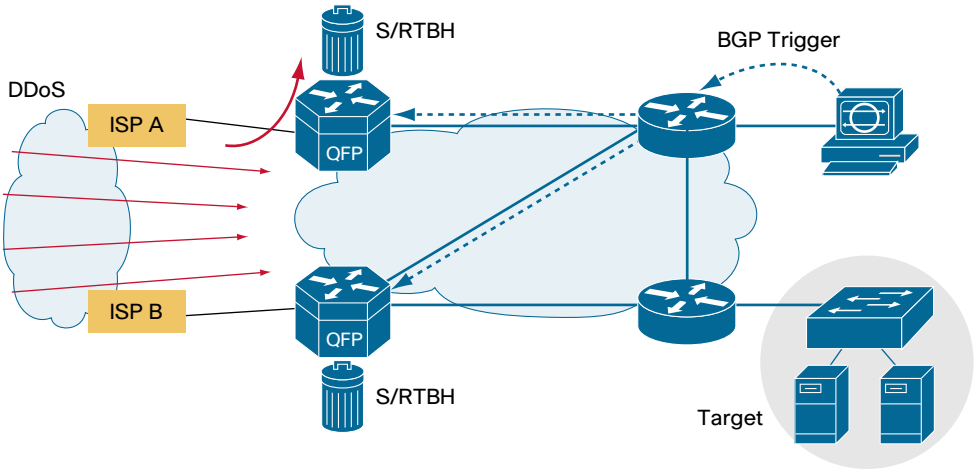
ベルは、セキュリティ モデル内で許可されるセキュリティのレベルです。セキュリティ モデルとセキュリティ レベルを組み合わせることで、SNMP パケットの処理に使用されるセキュリティ メカニズムが決定されます。SNMPv1、SNMPv2c、SNMPv3 の 3 つのセキュリティ モデルがあります。

送信元に基づく Remote-Triggered Black Hole（RTBH）フィルタリング

NetFlow データの分析などで攻撃の発信元が判明している場合、ACL などの隔離メカニズムを適用することができます。攻撃トラフィックが検出および分類されると、適切な ACL を作成して必要なルータに展開することができます。この手動プロセスには時間がかかり複雑なため、多くの組織が Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）を使い、ドロップ情報をすべてのルータに迅速かつ効率的に伝達しています。この RTBH と呼ばれる手法は、攻撃対象の IP アドレスの次のホップを null インターフェイスに設定します。攻撃対象に宛てられたトラフィックはネットワークへの進入時にドロップされます。

もう 1 つのオプションは、特定の送信元からのトラフィックのドロップです。この方法は前述のドロップ方法に似ていますが、送信元が無効のパケット（無効とは null0 へのルートを含む）をドロップする uRPF の事前展開に依存します。宛先に基づいたドロップの同じメカニズムを使って BGP 更新が送信され、送信元の次のホップを null0 に設定します。これで uRPF が有効にされたインターフェイスに進入するすべてのトラフィックで、その送信元からのトラフィックがドロップされます。拡張性はありますが、BGP でトリガされるドロップは、攻撃に対処するときに利用可能な精度のレベルが制限されます。前述したように、ブラックホール化された宛先へのトラフィック、または送信元はすべてドロップされてしまいます。通常、この対処法は大規模な攻撃に対して有効であり、確実に被害が緩和されます（図 8 参照）。

図 8　送信元に基づく RTBH フィルタリングによる DDoS 攻撃に対するリアルタイム ワイヤレート防御



Unicast Reverse Path Forwarding（uRPF）

uRPF は企業ネットワークの悪意のあるトラフィックを制限します。これは、ルータが転送されるパケット中の送信元アドレスの到達可能性を確認できるようにすることで行われます。この機能はネットワーク上のなりすましアドレスの出現を制限することができます。送信元 IP アドレスが有効でないと、パケットは廃棄されます。Cisco ASR 1000 シリーズ ルータは、ストリクト モードとルーズ モードをサポートしています。

管理者が uRPF をストリクト モードで使用する場合、パケットはルータがリターン パケットを転送するために使用するインターフェイスで受信される必要があります。ストリクト モードで設定された uRPF は、ルータがリターン トラフィックの送信に選択しなかったインターフェイスで受信された正規トラフィックをドロップすることがあります。ネットワークに非対称のルーティング パスが存在すると、この正規トラフィックがドロップされる場合があります。

All contents are Copyright © 1992–2011 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

管理者が uRPF をルーズ モードで使用する場合、送信元アドレスがルーティング テーブルにある必要があります。管理者は、送信元確認プロセスでデフォルトのルートの使用を許可するデフォルト許可のオプションで、この挙動を変更することができます。また、リターン ルートが null0 インターフェイスに向けられた送信元アドレスを含むパケットはドロップされます。uRPF ルーズ モードでは、特定の送信元アドレスを許可または拒否するアクセス リストを指定することもできます。

発注情報

シスコ製品の購入方法の詳細は、「購入案内」を参照してください。Cisco ASR 1000 シリーズ セキュリティ バンドルの総合リストは、http://www.cisco.com/go/securitybundles/ [英語] をご覧ください。

エンタープライズ WAN エッジ向けのシスコのサービス

シスコおよびシスコの認定パートナーは、実証済みの方法論に基づく広範なサービス ポートフォリオによって、お客様のエンタープライズ WAN エッジ展開の成功を支援します。ビジネス目標に整合した安全かつ復元力のある WAN アーキテクチャを構築し、Cisco® Unified Communications、Cisco TelePresence™、セキュリティ、およびモビリティ テクノロジーを、ビデオ、コラボレーション、ブランチ ソリューション、および拡張をサポートする帯域幅で適切に統合するために、シスコのサービスを是非お役立てください。計画および設計サービスでは、テクノロジーとビジネス目標との整合性を図り、展開の正確性、速度、および効率性を向上することができます。テクニカル サービスは、動作状態（ヘルス）を維持し、ソフトウェア アプリケーションの機能を強化し、パフォーマンスの問題を解決して、コストを削減します。また最適化サービスは、継続的にパフォーマンスを向上し、新しいテクノロジーを活用してお客様を成功に導きます。詳細については http://www.cisco.com/jp/go/services/ をご覧ください。

関連情報

Cisco ASR 1000 シリーズ ルータのネットワーク セキュリティ、および補完的な Cisco 800、1800、2800、3800 シリーズ ブランチオフィス ルータ ソリューションの詳細については、http://www.cisco.com/web/JP/product/hs/security/irs/index.html または最寄りのシスコ代理店にお問い合わせください。

All contents are Copyright © 1992–2011 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

©2011 Cisco Systems, Inc. All rights reserved.
Cisco、Cisco Systems、およびCisco Systemsロゴは、Cisco Systems, Inc.またはその関連会社の米国およびその他の一定の国における登録商標または商標です。
本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。
「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(0809R)
この資料に記載された仕様は予告なく変更する場合があります。

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先:シスコ コンタクトセンター
0120-092-255(フリーコール、携帯・PHS含む)
電話受付時間:平日10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

お問い合わせ先

11.10