



Check Point®

SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.



White Paper

安全なVoice over IP インフラストラクチャの構築

Check Point VPN-1 Proによる安全なVoIP通信の実現



Intelligent Security

チェック・ポイントは、境界、内部、WEBなど、ネットワークのあらゆる局面に対するセキュリティ・ソリューションを提供します。これにより、企業はネットワークや、ネットワーク・リソース等を安全に保護しながら、高い接続性を実現するリモート・アクセスを提供し、簡単に管理することができます。

Contents

本書の内容

| | |
|---------------------------|----|
| 概要 | 3 |
| 複雑で多様なVoIPプロトコルへの対応 | 4 |
| 集約されたネットワークの保護 | 5 |
| 高品質な音声の配信 | 9 |
| NATに関する問題の解決 | 10 |
| まとめ | 11 |

概要

電話専用のネットワークから、音声、映像、およびデータが混在する集中型ネットワークに企業が音声トラフィックを移行するのに伴い、Voice over IP (VoIP) の採用が急速に増加しています。Deloitte & Toucheが発表した『Getting Off the Ground: Why the Move to VoIP Is a Decision for All CxOs (2004)』は、2006年にはGlobal 2000企業の66パーセントで社員のデスクにVoIPが導入されるようになるとレポートしています。この理由として、VoIPの技術により、出張中の社員に電子メールで音声メールを配信するサービスなど、音声サービスが向上する点、および長距離通話などの電話サービスと比較して運用コストが低い点が挙げられています。

しかし、こうしたメリットにはセキュリティ上のリスクが伴います。音声トラフィックをデータ・ネットワークに移行すると、ワームやバッファ・オーバーフローなど、既存のネットワーク・インフラストラクチャに接続する場合と同じ攻撃にさらされることになります。また、VoIPのプロトコルが複雑で多様であるため、従来のセキュリティ・ソリューションでは、データ・ネットワーク上の音声を処理することは不可能に近いといえます。したがって、単にVoIPに対応するだけでなく、攻撃からVoIPネットワークを保護するために、インテリジェントにセキュリティ上の決定を下すことのできる境界ソリューションが必要となるのです。

Check Point VPN-1 Pro® は、セキュリティを維持しながらVoIPを展開するのに必要な先進の技術を備えています。VPN-1 Proでは、ステートフル・インスペクションとApplication Intelligence™ をベースにしたインテリジェントなセキュリティにより、VoIPを境界セキュリティ戦略に統合するのに伴う、以下の主要な4つの問題を解決できます。

1. 複雑で多様なVoIPプロトコルへの対応：企業のニーズに応じて、さまざまなVoIPプロトコルの中からプロトコルを選択できます。これらのVoIPプロトコルは、全く別々に機能し、従来のファイアウォールでは処理できない方法でセキュリティを維持します。VPN-1 Proは、境界セキュリティ・ソリューションで利用できる広範なVoice over IPプロトコルに対し、最もインテリジェントなセキュリティを提供します。VPN-1のインテリジェントなセキュリティには、他の境界ソリューションにはない2つのメリットがあります。第1のメリットとして、ネットワーク・レイヤとVoIPデータが含まれるペイロードとの双方を徹底的に検査できます。第2のメリットとして、VoIPセッションの動作が正常かどうかを判別できるように設計されているため、管理者が介入することなく、悪意のあるVoIPアクティビティを検知および停止できます。

2. 集中型ネットワークの保護：音声トラフィックをデータ・ネットワークに移行すると、従来型のデータ攻撃にさらされることになります。VPN-1 Proは、単純なVoIPプロトコルのサポートにとどまらず、VoIPの動作や振る舞いを認識できるため、VoIPネットワークとその基盤となるインフラストラクチャの双方に先制的な保護を提供します。

3. 高品質な音声の配信：VoIPを展開するにあたり、従来の電話サービスと同じ高いレベルの音声品質を維持できるかどうか重要な懸念事項となります。VPN-1 Proでは、サービス品質 (QoS) のメカニズムを統合することにより、高レベルのセキュリティを維持しながら、音声トラフィックの品質維持も実現します。

4. NATに関する問題の解決：ネットワーク・アドレス変換 (NAT) は、一般的なセキュリティ機能ですが、VoIPと互換性がないことも少なくありません。VPN-1 Proには、サードパーティの製品を使用しなくても、NAT環境にVoIPを展開できる幅広い展開オプションが用意されています。

本書では、VoIPの導入、展開を検討している企業を対象に、なぜ従来のセキュリティ手法では上記4つの問題を解決できないのか、およびインテリジェントで柔軟性の高いセキュリティを備えたCheck Point VPN-1 Proによってこれらの問題がどう解決されるのかについて説明します。

複雑で多様なVoIPプロトコルへの対応

Voice over IPは、ある決まったいくつかの標準からなる完全に統一された技術ではありません。実際には、インターネット上に音声を送るプロトコルはいくつも存在しています。現在、最も一般的に採用されているVoIPプロトコルはH.323とSIPです。MGCPは、大規模ネットワークで多く採用されており、異なるVoIP導入環境間で調整を図るサービス・プロバイダのネットワークなどで利用されています。SCCP (Skinny) はCiscoが独自に開発したプロトコルで、旧式のVoIPの展開で多く採用されています。

| | |
|--------------|--|
| シグナリング・プロトコル | H.323 セッション開始プロトコル (SIP) SCCP メディア・ゲートウェイ制御プロトコル (MGCP) |
| メディア・プロトコル | リアルタイム転送プロトコル (RTP) リアルタイム制御プロトコル |

一般的に導入されているVoIPプロトコル

特定のプロトコルまたは標準においても、ファイアウォールでは1回のVoIP通話について複数のプロトコルを処理する必要があります。シグナリング・プロトコルは、通話の発信側と着信側の特定、および通話の確立に使用されます。実際の会話は、メディア・プロトコルのRTPおよびRTCPによって伝送されます。H.323の場合、通話の確立には、H.225やH.245などの標準が使用されます。

問題をさらに複雑にしているのが、各プロトコルに多数のバリエーションがあることです。例えば、H.323のバージョン2、3、および4は、VoIPの展開で一般的に利用されています。同様に、SIPには、SIP over UDPやSIP over TCPなど多数の形態があります。ファイアウォールでは、これらのプロトコルを認識したうえでセキュリティを確保しなければなりません。多くの企業がさまざまなバリエーションのVoIPを併用するに至った背景には、買収や合併、ITに関連する意思決定権を地区や各事業所に付与するというポリシー、あるいは単純に時間の経過と共に複数のアプリケーションが導入されたことなどが挙げられます。

VoIPの複雑さは、プロトコルの多様性とどまらず、プロトコルとセキュリティとの関係にまで及びます。H.323は、VoIPのセキュリティ確保が困難であることを示す典型例です。従来のファイアウォールでは、トラフィックの入り口となる特定のポートを定義することで境界のセキュリティを確保します。例えば、Webトラフィックの場合はポート80を通過することになっているため、ファイアウォールではトラフィックがポート80に入るのを許可します。しかし、H.323では、静的ポート（通話の確立用のポート1720など）とランダムな動的ポートの両方が使用されます。従来の境界ファイアウォールがH.323のファイアウォールの通過を許可する場合、音声トラフィック用に何千もの動的ポートと静的ポートを開いたままの状態にしなければなりません。このため、攻撃者が悪用する大きなセキュリティ・ホールが生じてしまいます。

H.323トラフィックはASN.1に基づいてバイナリ形式で符号化されるため、先進のファイアウォールでも、ネットワークに入るVoIPトラフィックを解析して適切なセキュリティを決定するのに相当の時間がかかります。パケット内に存在する（配信アドレスのデータなどの）重要な情報は、VoIPアプリケーションの種類によって配置位置が微妙に異なります。このため、十分なインテリジェンスを備えていない従来のファイアウォールでは、セキュリティの決定に必要なメッセージおよび情報を解析することができません。VoIPのセキュリティの複雑さを解決するには、従来のファイアウォールではなく、VoIPのプロトコルと機能に高度に対応するセキュリティ・ソリューションが必要となります。

チェック・ポイントの解決策

Check Point VPN-1 Proは、Application Intelligence技術と特許取得済みのステートフル・インスペクション技術により、単純なプロトコルのサポートにとどまらず、VoIPの動作や振る舞いをより深いレベルで認識できます。現在使用されている最も一般的なプロトコルおよびバリエーションを認識できるため、境界ファイアウォールで使用可能なVoIPを幅広くサポートします。1つのVoIPプロトコルしかサポートせず、非標準のセキュリティ機能を搭載したVoIP専用ゲートウェイと異なり、VPN-1 Proは、現在企業で必要とされる信頼性の高いセキュリティと広範なプロトコルのサポートを両立して実現します。

SIP、H.323、MGCP、およびSCCP (Skinny) の場合、VPN-1 Proでは、会話の状態とコンテキスト(前後関係)に基づいてポートを動的に開くことができます。この機能は、ほとんどのファイアウォールで行われている一般的なステートフル・パケット・インスペクションの機能にとどまらず、実際のVoIPでの会話も認識できます。例えば、H.323の場合、セッションの進行と共に情報とポート番号が動的に変化し、新しいポートの情報が会話の前の部分に配置されます。VPN-1 Proでは、H.323で使用されるASN.1形式を逆アセンブルして、利用可能なセキュリティを検査し、コンテキストに基づいてセキュリティを決定します。また、トラフィックのコンテキストを認識および適用して、自動転送や保留などのVoIPの機能をサポートします。

| | |
|-------|--|
| SIP | RFC 3261 - 最新のSIP RFC、RFC 3372 - SIP-T、RFC 3311 - UPDATEメッセージ、RFC 2976 - INFOメッセージ、RFC 3515 - REFERメッセージ、RFC 3265 - SIPイベント、RFC 3266 - SDPにおけるIPv6対応、RFC 3262 - プロビジョナル応答の信頼性、RFC 3428 - MESSAGEメッセージ、MSN messenger over SIP、SIP over TCP、SIP over UDP、SIP Early Media |
| H.323 | H.323 V.2、V.3、V.4、H.225 V.2、V.3、V.4、H.245 V.3、V.5、V.7 |
| SCCP | |
| MGCP | RFC 3435 - MGCP v1、J.171 - TGCP |

サポートされているVoIPプロトコル

集約されたネットワークの保護

Distributed Networking Associatesの『The 2004 VoIP State of the Market Report』によると、音声通信をデータ・ネットワーク上で行うことに関して、回答者の25パーセントが音声通信のセキュリティが「著しく低下する」と感じています。セキュリティが「低下する」と感じるという回答を合わせると、VoIPネットワークはセキュリティ・レベルが低いと感じる回答者の割合は60パーセントにも上ります。

2002年末のSlammerワームは、音声とデータ・ネットワークを集中化する場合のセキュリティ上のリスクを如実に示しています。Gartner Groupのレポート『VoIP Security Behind the Firewall (2003)』では、Slammerなどのワームにより、集中型ネットワークにどのような損害が発生するかについて述べられています。Gartnerのあるクライアントは、顧客電話窓口のアプリケーションにVoIPを導入して成果を収めていました。しかし、VoIP電話ネットワークと従来型の外部の電話システムを接続するIP-PBXがワームの攻撃を受け、顧客電話窓口の通信機能が全損し、データが消失してしまいました。このVoIPシステムが攻撃に対して脆弱だったのは、ネットワーク経由で攻撃を受ける可能性の高いオペレーティング・システムがその基盤となっていたためです。

音声トラフィックとデータ・ネットワークとの統合を成功裏に実現するには、何よりもまずネットワークに強固なセキュリティ基盤を確立する必要があります。これを実行できない場合は、以下に示すリスクが生じることになります。

VoIPの構成要素に対する攻撃：Gartnerのクライアントの事例が示すように、IP PBXやIP電話機などのVoIPの構成要素は、パケット・ベースの攻撃にさらされる可能性があります。このような電話機やシグナル・ルーティング・デバイスには、2つの潜在的な脆弱性があります。第1に、悪用の標的となる脆弱性を含む可能性のあるオペレーティング・システムに、すべての構成要素が依存している点です。

第2に、構成要素自体に悪用の標的となる脆弱性があるかもしれないという点です。VoIPトラフィックで使用されるプロトコルは、比較的新しく常に変化を遂げているため、攻撃者によるシステムへのアクセス、デバイスのクラッシュ、または電話の不正利用を可能にしてしまうような未知の脆弱性を含んでいる可能性が大いにあります。例えば、Voice over IPによる通話は、通話制御チャンネルと実際のメディアまたはデータ・チャンネルの2つの通信チャンネルで構成されており、これらのチャンネルは同時に開いています。VoIPシステムの悪用の一例は、このメディア・チャンネルを開いたまま、通信制御チャンネルを終了し、通話が終了したことを示す信号を信号ルーティング・デバイスに送出するというものです。これは、実際より安い料金で電話サービスを不正使用することを可能にしまいます。

音声サービス妨害：正当なWebページ要求によってもWebサーバのサービスを妨害できるのと同様に、攻撃者は、適切な形式の通話要求を大量に送信することで、VoIPシステムを使用不能の状態にすることができます。このような単純な攻撃でも正当な通話要求が確立できなくなってしまいます。

ソフト・フォンの危険性：VoIPによるソフト・フォンを利用すると、料金が割高な携帯電話や長距離電話を使用せずに、遠隔地にいる社員と無料で通話できます。ソフト・フォンとは、ラップトップ・コンピュータに導入可能な、電話機器を必要としない仮想VoIP電話アプリケーションのことです。ソフト・フォンを使用すると、外出中であっても、ネットワーク内にいるのと同じように電話をかけることができます。しかし、リモート・コンピュータのセキュリティが確保されていない場合、リモート・コンピュータが攻撃者のアクセス・ポイントとなる可能性があります。セキュリティが確保されていないコンピュータは、攻撃の標的になりやすく、データの収集や企業ネットワークへのアクセスに悪用される可能性があります。また、VoIPトラフィックは、インターネット上で伝送される際、デフォルトで暗号化されることはほとんどありません。リモート・ユーザにVoIPを展開する場合は、会話の機密性を保護するために、暗号化技術を追加で導入する必要があります。

チェック・ポイントの解決策

Check Point VPN-1 Proは、Application Intelligence技術を備えており、アプリケーション・レイヤの脅威を正確に認識でき、VoIP展開に対する完全な侵入防止を実現します。Application Intelligence技術は、H.323やSIPなどのVoIPプロトコルではどのような動作が想定されているのかを深いレベルで理解することを可能にします。攻撃者が脆弱性を悪用しようとしているなどでトラフィックに異常がある場合は、VPN-1 Proがそれを検知し、攻撃の発生自体を未然に防ぎます。

Application Intelligence技術は、Voice over IPのトラフィックに関して、サポート対象のプロトコルと標準への準拠、およびそれらにおいて想定されている使用方法への準拠を厳格に実施します。例えば、展開環境においてSIP over UDPが使用されている場合、VPN-1 Proは、トラフィックが確実にRFC 3261に準拠するようにします。これを実現するために、Application Intelligence技術では、次の点をチェックします。

- ・ 不正なバイナリまたはパケット内の不正な文字
- ・ ヘッダ文字に関するRFC標準への厳格な準拠
- ・ ヘッダ・フィールド長の制限
- ・ 未知のメディア・タイプの除去
- ・ アドレス内での使用が禁止されている文字の除去

VPN-1 Proでは、VoIPセッションが、想定される動作や振る舞いのパターンに準拠しているかどうかを検証できます。これを実現するための重要な方法となるのが通話制御とメディア・トラフィックの実施です。通話の終了時には、終了信号がVoIPの信号ルーティング・デバイスに送信され、これに伴い監査と課金が停止されます。しかし、通話の終了が通知された後でも、やり方によっては、正規の課金チェックと監査の目をかいくぐり、通話を継続することができてしまいます。VPN-1 Proでは、信号の送出手と通話情報の双方が存在するかどうかをチェックし、必要に応じて通話を終了させることが可能です。

サービス妨害攻撃を防止するために、VPN-1 Proでは、通話の確立時と終了時の動作が想定されたものであるかどうかをチェックします。発信者が通話セッションを確立してすぐに終了した場合、これはサービス妨害攻撃と一致する動作であるため、それ以降、通話の確立要求は拒否されます。また、管理者は、個別のIPアドレスを基に一定の期間内における通話の試行回数を設定できます。

VPN-1 Proでは、VoIPハンドオーバー・ドメインを使用することにより、外部の第三者がVoIPの会話にアクセスして、サービスを不正使用したり通話をハイジャックしたりするのを抑制します。管理者は、特定の信号ルーティング・デバイスで管理するエンド・ポイントのIPアドレスを定義できます。信号ルーティング・デバイスにより2つのIP電話間で通話が確立されると、VoIPドメインと照合してIPアドレスがチェックされ、ドメイン内の通話の当事者のみが通話を許可されます。スパムがその標的をインスタント・メッセージングや電子メールからVoIPに切り替えたときのことを考慮すると、ハンドオーバー・ドメインを厳格に実施することがVoIP展開の価値を維持するうえで非常に重要になります。

チェック・ポイントのVoIPセキュリティの守備範囲は境界だけにとどまりません。先に述べたように、VoIPは、モバイル・ラップトップ・コンピュータに導入されるソフト・フォンにも組み込まれます。Integrity SecureClient™を導入すると、悪意のあるコードからリモートPCを保護すると共に、会話を暗号化することが可能になります。Integrity SecureClientは、一元管理されたパーソナル・ファイアウォールであると同時に、ネットワークのセキュリティを損なわずに管理者がVoIPサービスをリモート・ユーザに提供できる、統合されたVPNクライアントです。コンピュータからインターネットへのアクセスを許可または禁止するアプリケーションを管理者が定義できるため、スパイウェアやワームなど、悪意のあるコードがリモート・コンピュータを利用してネットワークに感染を拡げるのを防止できます。また、管理者は、アプリケーションのアクセス制御機能を使用して、ソフト・フォンにアクセスできるユーザを完全に制限できます。

Integrity SecureClientのOffice Modeでリモート・コンピュータの仮想IPアドレスを取得することで、管理者はリモート・ソフト・フォンを企業ネットワークにあるのと同じように管理できます。リモート・コンピュータには、無線ホットスポットやホテルのブロードバンド・サービスからランダムに割り当てられるIPアドレスではなく、VoIPドメインの一部として定義できる予測可能なIPアドレスが割り当てられます。

VoIPサービスの監査とログ

厳格な監査機能とログ機能を備えていないセキュリティは無意味です。これは、VoIPセキュリティにも当てはまります。VoIPのセキュリティ・ポリシーが適切に機能するようにするために、VPN-1 Proでは、発信元のIPと送信先のIP (SIPの場合は、発信元のURLと送信先のURL、および電話番号) など、通話に関する詳細なログが作成されます。

| SIPセキュリティ | H.323の高度なセキュリティ |
|--|--|
| <p>SIPメッセージのステートフル・インスペクション</p> <ul style="list-style-type: none"> ・ RTP/RTCP接続を動的に開く ・ 信号を送出する接続がない場合はRTP/RTCP接続を閉じる ・ 制御データの関係を継続的に適用 <p>SIP over TCPでのストリーミング・メカニズムの使用</p> <ul style="list-style-type: none"> ・ 複数のパケットに分割された場合でも、全メッセージを完全に検査 <p>次のフィールドの制限</p> <ul style="list-style-type: none"> ・ RFCの適用 ・ プロトコル状態マシン ・ ユーザ名 ・ Call-ID ・ SDPヘッダ <p>次のSIPメッセージの特別な構文の制御</p> <ul style="list-style-type: none"> ・ 登録 (REGISTER、ACK) ・ 接続許可制御 (INVITE) ・ 機能の交換 (SDP、OPTION) <p>ハンドオーバー・ドメイン</p> <ul style="list-style-type: none"> ・ VoIPのリダイレクトとハンドオーバーにセキュリティを適用 | <p>H.323メッセージのステートフル・インスペクション</p> <ul style="list-style-type: none"> ・ RTP/RTCP接続を動的に開く ・ 信号を送出する接続がない場合はRTP/RTCP接続を閉じる ・ T.120接続を動的に開く ・ 信号を送出する接続がない場合はT.120接続を閉じる ・ 制御データの関係を継続的に適用 <p>H.225およびH.245でのストリーミング・メカニズムの使用</p> <ul style="list-style-type: none"> ・ 複数のパケットに分割された場合でも、全メッセージを完全に検査 <p>次のH.323メッセージの特別な対応</p> <ul style="list-style-type: none"> ・ H.225 RASメッセージ ・ Q.931メッセージ ・ H.245 ・ Fast Start機能のサポート — H.225メッセージへのH.245のカプセル化 ・ H.245トンネリング機能のサポート — H.225メッセージへのH.245のカプセル化 <p>次のフィールドの制限</p> <ul style="list-style-type: none"> ・ RFCの適用 ・ 電話番号 ・ 特定のメッセージ内に存在するIPアドレス ・ 特定のメッセージ内に存在する電話番号 ・ プロトコル・フローのロジック <p>ハンドオーバー・ドメイン</p> <ul style="list-style-type: none"> ・ VoIPのリダイレクトとハンドオーバーにセキュリティを適用 |

SIPとH.323のセキュリティ・メソッド

高品質な音声の配信

AT&TとEconomist Business Unitが共同で行った調査（『Voice over IP Comes of Age (2004)』）では、回答者の64パーセントがVoIPの最も重要な懸案事項としてサービス品質（QoS）を挙げています。一般の人々は、非常に高いサービス・レベルの電話通信に慣れています。VoIPにいくら多くのメリットがあっても、従来の電話サービスと同じレベルの利便性と音声品質を提供できなければ、顧客には受け入れられないのです。

VoIPサービスの品質が低下する主な要因として2つの点が挙げられます。第1の要因は遅延、つまり、電話機間でVoIPパケットの伝送に要する時間についての問題です。National Institute of Science and Technologyの『Security Considerations for Voice over IP Systems (2005)』では、音声通信の最大遅延は片道150ミリ秒未満に抑えることが推奨されています。遅延に影響を及ぼす要因は、ルータのパケット処理能力など数多くあります。セキュリティの観点では、セキュリティ・ゲートウェイでのVoIPトラフィックの検査と暗号化に要する時間が最も大きな要因として挙げられます。

第2の要因はジッタです。ジッタは、VoIPパケットを受信する際の遅延が不規則な場合に発生し、パケットの到着順序が入れ替わったり、パケットが到着しなかったりする原因となります。到着時における音声トラフィックの調整は、プロセッサに非常に大きな負荷がかかります。このため、会話の音声が遅れて聞こえてきたり、音声の一部が途切れたりする現象が生じます。通常、このようなギャップは非常に小さいのですが、VoIPによる通話は大変聞き取りづらいという印象を与えてしまいます。エンドポイントまたはセキュリティ・ゲートウェイで処理される暗号化もジッタの主な要因です。

チェック・ポイントの解決策

Check Point VPN-1 Proは、必要なセキュリティを適用することで生じるジッタと遅延を最小限に抑える、統合されたサービス品質を実現します。VPN-1 Proには、高品質の音声通信を確保するためのさまざまな方法が用意されています。これらの方法を組み合わせて利用することにより、ローカル・ネットワークでも公衆ネットワークでもVoIPトラフィックの優先順位を高めることができます。例えば、管理者は、低遅延キューイング（LLQ）を使用して、セキュリティ検査による遅延を低減できます。LLQでは、VoIPなどの遅延の影響を受けやすいアプリケーションに、遅延の影響をあまり受けないアプリケーションよりも高い優先順位を付与します。同様に、重み付け優先度を使用すると、他のトラフィックよりも大きな帯域幅をVoIPトラフィックに割り当てることが可能になります。

QoSの制御に加え、セキュリティ・プラットフォームについても考慮が必要です。暗号化とトラフィックの検査の処理速度は、プラットフォームのパフォーマンスに左右され、ジッタ、遅延、およびVoIP利用の有効性に直接影響します。オープン・サーバとチェック・ポイントによってセキュリティが確保された機器を組み合わせることにより、最も厳しいパフォーマンス要件を満たすセキュリティ環境を設計できます。また、ハードウェア・アクセラレーションを使用して暗号化のパフォーマンスを強化することで、暗号化処理で生じるジッタを低減できます。

| ローカル・アクセス・リンクの制御 | |
|--------------------|--|
| 低遅延キューイング (LLQ) | LLQでは、VoIPといった遅延の影響を受けやすいトラフィックに、最大遅延の設定も含め、セキュリティ処理を考慮した最高レベルの優先順位を設定できます。 |
| 帯域幅保証 | VoIP転送専用で帯域幅の一部を確保することにより、他の重要度の低いトラフィックが原因で通話の音声途切れるのを防止できます。 |
| 重み付け優先度 | ビジネスの目的に応じて、トラフィックのタイプごとに異なる優先度を割り当てることができます。例えば、VoIPトラフィックには50の重要度の比重を指定し、ファイル共有には5の比重を指定するといったことができます。この場合、ネットワークが過密状態になると、VoIPとファイル共有のネットワーク占有比率は10対1になります。 |
| エンドツーエンドの制御 | |
| 差別化サービス (DiffServ) | DiffServのサポートが統合されているので、サービス・プロバイダは、企業のワイド・エリア・ネットワーク (WAN) 上でVoIPトラフィックを識別し、それらを優先的に処理することができます。 |

チェック・ポイントのQoSのメソッド

NATに関する問題の解決

ネットワーク・アドレス変換 (NAT) は、現在最も普及しているセキュリティ手段ですが、VoIP環境で使用する場合にはそれ特有の問題を解決する必要があります。NATは、境界ファイアウォールで一般的に使用され、IPアドレスを節約したり、ネットワーク内部の構造を隠蔽したりします。NATでは、インターネット上でルーティング不可能な内部IPアドレスを、インターネット上のリソースに使用されている外部IPアドレスにマップします。この過程でNAT対応のファイアウォールは、パケットのアドレスをネットワーク・レイヤ (レイヤ3) で変更して、マッピングを行います。ほとんどアプリケーションでは、これで問題が発生することはありません。

しかし、VoIPプロトコルの場合、IPアドレスはネットワーク・レベルだけでなくアプリケーション・レベルでも組み込まれます。VoIPのエンドポイントまたはデバイスが、NATゲートウェイの背後にあるエンドポイントから送られた信号送出トラフィックまたはメディア・トラフィックを受け取った場合、そのエンドポイントまたはデバイスは、ルーティング不可能な内部IPアドレスを正しいIPアドレスとして認識し、そのIPアドレスにトラフィックを返そうとしますが、当然のことながらこれは失敗します。着信通話の場合、外部にルーティング可能なIPアドレスが何百、何千というエンドポイントで共有されている可能性があるため、問題はさらに深刻になります。

チェック・ポイントの解決策

Check Point VPN-1 Proは、ネットワーク・アドレス変換やプライベートでルーティング可能なIPアドレスの使用を停止することなく、既存のネットワーク・アーキテクチャとVoIPの共存を実現するソリューションを提供します。VPN-1 Proは、信号ルーティング・デバイス上の情報と同期されたVoIPユーザのデータベースを保持しています。IP電話は、通話を行う前に自分自身を信号送出デバイスに登録する必要があります。この際に、VPN-1 Proがその登録要求を認識し、必要な情報を自身の内部データベースに登録します。これによって、VPN-1 Proで保護されたネットワークの外部から、Hide NAT (多対1のNAT)を使用して変換されたアドレスを持つ機器に電話をかけることが可能になります。Check Point VPN-1 Proは、この機能をH.323プロトコルとSIPプロトコルの両方で実現する唯一の境界セキュリティ・ソリューションです。

| SIPネットワークでのNATのサポート |
|---|
| <ul style="list-style-type: none"> Static NATまたはHide NATを使用して、内部ネットワーク、外部ネットワーク、またはDMZにエンドポイントを導入することが可能 Hide NATによりゲートウェイの背後に隠されているエンドポイントに対する着信通話をサポート Hide NATを使用して、内部ネットワーク、外部ネットワーク、またはDMZにSIP-PSTNゲートウェイを導入することが可能 Static NATを使用して、内部ネットワーク、外部ネットワーク、またはDMZにSIP-PSTNゲートウェイを導入することが可能 |
| H.323ネットワークでのNATのサポート |
| <ul style="list-style-type: none"> Static NATを使用して、外部ネットワーク、内部ネットワーク、DMZにゲートキーパを導入することが可能 Static NATを使用して、外部ネットワーク、内部ネットワーク、DMZにゲートウェイ/PBXを導入することが可能 Static NATを使用して、任意の場所にエンドポイントを導入することが可能 Hide NATを使用して、任意の場所にエンドポイントを導入することが可能 Hide NATを使用したエンドポイントへの着信通話をサポート Static NATを使用して、任意の場所にH.323-PSTNゲートウェイを導入することが可能 Hide NATを使用して、任意の場所にH.323-PSTNゲートウェイを導入することが可能 |

VPN-1 ProにおけるNATのサポート

まとめ

VoIPをネットワークに導入する場合、展開の範囲を定義したり、音声とデータの集中型ネットワークのメリットを実現したりするうえで、境界セキュリティ・ソリューションが非常に重要な役割を果たします。VPN-1 Proは、導入の目的を犠牲にすることなく、VoIPを包括的なセキュリティ・ポリシーに統合するためのプラットフォームを提供します。ステートフル・インスペクションとApplication Intelligenceを備えたVPN-1 Proは、VoIPのための最もインテリジェントな境界セキュリティ・ソリューションを実現します。

Check Point Software Technologiesについて

チェック・ポイント・ソフトウェア・テクノロジーズ (www.checkpoint.com) はインターネット・セキュリティにおける世界トップ企業として、特に企業向けファイアウォール、パーソナル・ファイアウォール、およびVPNの市場においてマーケット・リーダーとして広く認められています。

チェック・ポイントはNext Generation製品ラインナップを通じ、インテリジェント性を兼ね備えた境界、内部、およびWeb環境に対するセキュリティ・ソリューションを提供し、エンタープライズ・ネットワークをはじめ、アプリケーション、エンドポイント、支店・支社環境、更にはパートナー各社のエクストラネットなどに対する包括的なセキュリティ保護を実現します。

チェック・ポイントの一部門である Zone Labs (www.zonelabs.com) は、インターネット・セキュリティの分野で高い信頼性を誇るブランドとして数々の賞に輝くエンドポイント・セキュリティ・ソリューションを提供し、世界中で何百万台ものコンピュータをハッカーやスパイウェア、データの盗難などから守っています。

またチェック・ポイントは、350社を超える各分野のトップベンダーが提供する最高のソリューションとの統合および相互運用性を実現するフレームワークであるOPSEC (Open Platform for Security) により、自社ソリューションの能力をさらに拡大します。現在チェック・ポイントは世界88ヶ国、2200社を超えるパートナー・ネットワークを通じてソリューションの販売、導入、サービス提供を行っています。

©2005 Check Point Software Technologies Ltd. All rights reserved.

Check Point, Application Intelligence, Check Point Express, Check Pointのロゴ、AlertAdvisor, ClusterXL, Cooperative Enforcement, ConnectControl, Connectra, CoSa, Cooperative Security Alliance, Eventia, Eventia Analyzer, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Hacker ID, IMsecure, INSPECT, INSPECT XL, Integrity, InterSpec, IQ Engine, Open Security Extension, OPSEC, Policy Lifecycle Management, Provider-1, Safe@Home, Safe@Office, SecureClient, SecureKnowledge, SecurePlatform, SecuRemote, SecureServer, SecureUpdate, SecureXL, SiteManager-1, SmartCenter, SmartCenter Pro, Smarter Security, SmartDashboard, SmartDefense, SmartLSM, SmartMap, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartViewTracker, SofaWare, SSL Network Extender, TrueVector, UAM, User-to-Address Mapping, UserAuthority, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 VSX, Web Intelligence, ZoneAlarm, ZoneAlarm Pro, Zone Labs, Zone Labsのロゴは、Check Point Software Technologies Ltd.およびその関連会社の商標、サービス・マーク又は登録商標です。その他の企業、製品名は各企業が所有する商標または登録商標です。本書に記載された製品は米国の特許 No.5,606,668、5,835,726および6,496,935により保護されています。その他の 米国における特許や他の国における特許で保護されているか、出願中の可能性があります。

Creating a secure Voice over IP infrastructure

P/N:501865-J 2005.10

※記載された製品仕様は予告無く変更される場合があります。



Check Point
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.

チェック・ポイント・ソフトウェア・テクノロジーズ株式会社
〒160-0022 東京都新宿区新宿5-5-3 建成新宿ビル6F
http://www.checkpoint.co.jp/ E-mail: info_jp@checkpoint.com Tel: 03(5367)2500