Cisco SAFE
エンタープライズネットワークのための セキュリティブループリント

著者について

Sean Convery（CCIE #4232）とBernie Trudel（CCIE #1884）がこのホワイトペーパーの著者です。Seanは、米国カリフォルニア州のサンノゼにあるシスコ本社においてこのアーキテクチャの参照実装を考案した指導者です。SeanとBernieは共にシスコのEnterprise Line of BusinessにおけるVPNおよびセキュリティアーキテクチャ・テクニカルマーケティングチームのメンバーです。

概要

シスコのエンタープライズネットワーク向けセキュリティブループリントCisco SAFEの一番の目的は、安全なネットワークの設計と実装における最善の情報を当事者に提供することです。SAFEは、ネットワークのセキュリティ要件を検討するネットワーク設計者に対する指針としての役割を持ちます。SAFEは、ネットワークセキュリティ設計に対して徹底した防御アプローチをとります。この種の設計は、「ファイアウォールをここに置き、侵入検知システムをそこに置く」のではなく、予測される脅威と、その脅威を軽減する方法に照準を定めています。この戦略によってセキュリティに対して段階的なアプローチがとられるため、セキュリティシステムの１つに障害が発生してもネットワークリソースが被害を受ける可能性が低くなります。SAFEは、シスコ製品およびパートナーの製品に基づいています。

この文書では、まずアーキテクチャの概要について説明してから、実際のネットワーク設計を構成する特定のモジュールについて詳しく説明します。各モジュールの最初の３つのセクションでは、トラフィックフロー、主要デバイス、および予測される脅威について説明し、基本的な軽減を図示します。続いて、技術面から設計を詳細に分析し、脅威軽減の手段および移行戦略についてより詳細に説明します。付録Aでは、SAFEの検証実験について詳しく説明し、構成のスナップショットを示します。付録Bは、ネットワークセキュリティの手引きです。ネットワークセキュリティの基本概念をよく理解していない場合は、最初にこのセクションを読んでからほかのセクションを読むことをお勧めします。付録Cには、この文書で使用される技術用語の解説と、図の凡例を掲載します。

この文書は、主に企業環境で見られる脅威に焦点を当てています。こうした脅威を理解しているネットワーク設計者は、軽減手段としてのテクノロジーを配置する場所とその方法について、適切な判断を下すことができます。ネットワークセキュリティに伴う脅威を十分に理解していないと、配置が間違って構成されたり、セキュリティデバイスに重点を置きすぎていたり、脅威対応オプションが不足したりします。この文書は、脅威軽減アプローチをとることで、ネットワークセキュリティに関する適切な選択を行うための情報をネットワーク設計者に提供します。

本ドキュメントの対象

この文書は技術的な観点から書かれていますが、目的に応じて自由に読むことができます。たとえば、ネットワーク管理者は、各分野の冒頭のセクションを読んで、ネットワークセキュリティ設計における戦略と考慮事項の概要を理解することができます。ネットワークエンジニアまたは設計者は、この文書全体を通して読んで、必要なデバイスの構成スナップショットも含め、設計情報や脅威分析の詳細を知ることができます。

注意事項

この文書は、すでにセキュリティポリシーが実施されていることを前提としています。シスコシステムズでは、関連するポリシーを実装せずにセキュリティテクノロジーを配置することを推奨していません。この文書は、大企業カスタマのニーズに直接応えるものです。ここで述べる原則の大部分は、程度の差こそありますが、

中小企業や在宅オフィスにもそのまま適用されます。この文書では、こうした企業の分類についての詳細は省きますが、より小規模なネットワークの問題に少しでも対処するため、「代替案」と「エンタープライズオプション」のセクションで、アーキテクチャのコストを削減したい場合に排除できるデバイスについて概説しています。

この文書のガイドラインに従うことで、すべての侵入を防止する安全な環境が保証されるわけではありません。本当に完全なセキュリティを実現するには、システムをネットワークから切り離し、そのシステムをコンクリートで固め、Fort Knoxの地下室に置くことですが、これでは確かにデータは安全でも、アクセスすることができません。しかし、適切なセキュリティポリシーを設定し、この文書のガイドラインに従い、ハッカーおよびセキュリティ業界における開発の最新情報を常に把握し、すべてのシステムを適切なシステム管理の慣行によって維持および監視すれば、適度なセキュリティを実現することができます。そのほか、この文書では包括的に扱っていませんが、アプリケーションセキュリティの問題に対する認識も必要です。

VPN（仮想プライベートネットワーク）がこのアーキテクチャに含まれますが、これについては詳しく説明しません。拡張に関する詳細、回復力戦略などの情報や、VPN関連のその他のトピックについては扱っていません。VPNと同様に、ID（本人証明）戦略（認証局 [CA] を含む）についてもこの文書では詳しく説明しません。CAについても詳しい説明が必要ですが、この文書ではこれに対応せず、ネットワークセキュリティのほかのすべての関連する分野を十分に取り扱います。また、大部分のエンタープライズネットワークではまだ完全に機能的なCA環境が展開されていないため、こうした状況でどのように安全にネットワークを配置するかを検討することが重要です。最後に、特定の高度なネットワーク用アプリケーションおよびテクノロジ（コンテンツネットワーキング、キャッシング、サーバ負荷分散など）についてもこの文書では説明しません。これらはSAFEで使用される見通しですが、この文書では特定のセキュリティニーズまで扱っていません。

SAFEでは、シスコシステムズとそのパートナーの製品が使用されています。この文書では特に製品名を挙げて説明していませんが、機能上の目的から、モデルの番号や名前ではなくコンポーネントについて言及しています。SAFEが検証された間、実際の製品は、この文書で説明されているとおりのネットワーク実装で構成されました。研究所からの特定の構成スナップショットは、付録A「設定例」に含まれています。

この文書全体を通して、「ハッカー」は、故意にネットワークリソースへの不正なアクセスを試みる人物を指しています。この種の人物を表すには「クラッカー」の方がより正確な用語として一般にみなされていますが、ここでは、読みやすいようにハッカーを使用しています。

アーキテクチャの概要

設計の基本

SAFEは、できるだけ忠実に、今日のエンタープライズネットワークにおける機能上の要件にならっています。要求されるネットワーク機能によって実装の決定は異なりますが、優先順に挙げた次の設計目標に従って、意思決定プロセスが行われました。

- シーに基づいたセキュリティおよび攻撃の軽減
- （専用のセキュリティデバイスだけでなく）インフラストラクチャ全体におけるセキュリティの実装
- 安全な管理とレポート
- クリティカルなネットワークリソースに対し、ユーザーと管理者の認証および権限付与
- クリティカルなリソースおよびサブネットのための侵入検知
- 新しいネットワーク用アプリケーションのサポート

SAFEは、何よりもまずセキュリティアーキテクチャであるため、大部分の攻撃によって貴重なネットワークリソースに影響が及ぶことを防ぐ必要があります。最初の防御線を突破することに成功した攻撃やネットワーク内部で発生した攻撃は、正確に検知して素早くくい止めることにより、ネットワークの残りの部分への影響を最小限に抑える必要があります。その一方で、セキュアなネットワークによって、ユーザーが期待するクリティカルなサービスを提供し続ける必要があります。こうした適切なネットワークセキュリティと優れたネットワーク機能は、同時に提供することができます。SAFEアーキテクチャは、革新的なネットワーク設計法ではなく、ネットワークをセキュアにするためのブループリントであるに過ぎません。

SAFEは、回復力と拡張性にも優れています。ネットワークにおける回復力には、構成の誤り、物理的障害、ネットワーク攻撃のいずれかによるデバイス障害を防ぐための物理的な冗長性が含まれます。ネットワークパフォーマンスに対するニーズが高くない場合は特に単純な設計も可能ですが、単純な環境より複雑な環境におけるセキュリティ設計の方が多いため、この文書では複雑な設計を例に挙げています。複雑な設計を単純にするオプションについては、この文書全体を通して説明します。

ネットワーク設計プロセスにおける多くのポイントで、ネットワークデバイスの統合された機能性を使用するか、または機能的な専用機器を使用する必要があります。多くの場合、統合された機能性の方が優れています。これは、既存の機器に実装できるため、または機能がデバイスのほかの機能と相互に作用して、より優れた機能的ソリューションを提供することができるためです。これに対し、専用機器がよく使用されるのは、要求される機能性のレベルが非常に高度である場合や、パフォーマンスのニーズによって専用のハードウェアを使用する必要がある場合です。この判断は、機器のキャパシティと機能性をとるか、デバイスの統合におけるメリットをとるかを考慮したうえで行ってください。たとえば、小型のIOSルータに個別のファイアウォー

ルを実装するのではなく、高い処理能力の統合されたCisco IOSルータにIOSファイアウォールソフトウェアを実装することを選択できるときがあります。このアーキテクチャ全体において両方の種類のシステムが使用されていますが、クリティカルなセキュリティ機能の大部分は、大規模なエンタープライズネットワークのパフォーマンス要件に従って専用機器へと移行しています。

モジュールの設計概念

エンタープライズネットワークの大部分は、企業のIT要件の拡大に伴って進化していますが、SAFE アーキテクチャでは、グリーンフィールドモジュラ型アプローチを採用しています。モジュラ型のアプローチには主に２つの利点があります。１つ目は、アーキテクチャがネットワークのさまざまな機能ブロック間におけるセキュリティの関連性に対応できる点です。２つ目は、設計者が、各段階で完全なアーキテクチャを設計しようとしなくても、モジュールのセキュリティをモジュール単位で評価および実装できる点です。

図1に、SAFEのモジュール全体における最初の階層を示します。各ブロックは機能的領域を表しています。インターネットサービスプロバイダ(ISP)モジュールは企業では実装されませんが、特定の攻撃を軽減するためにISPの特定のセキュリティ機能が必要とされる範囲で含まれます。

図1:エンタープライズコンポジットモジュール

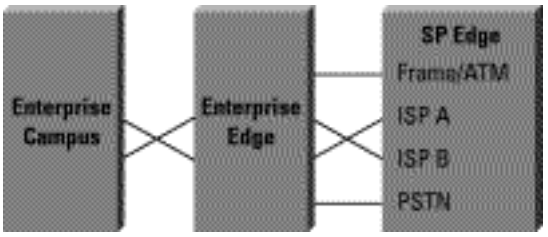
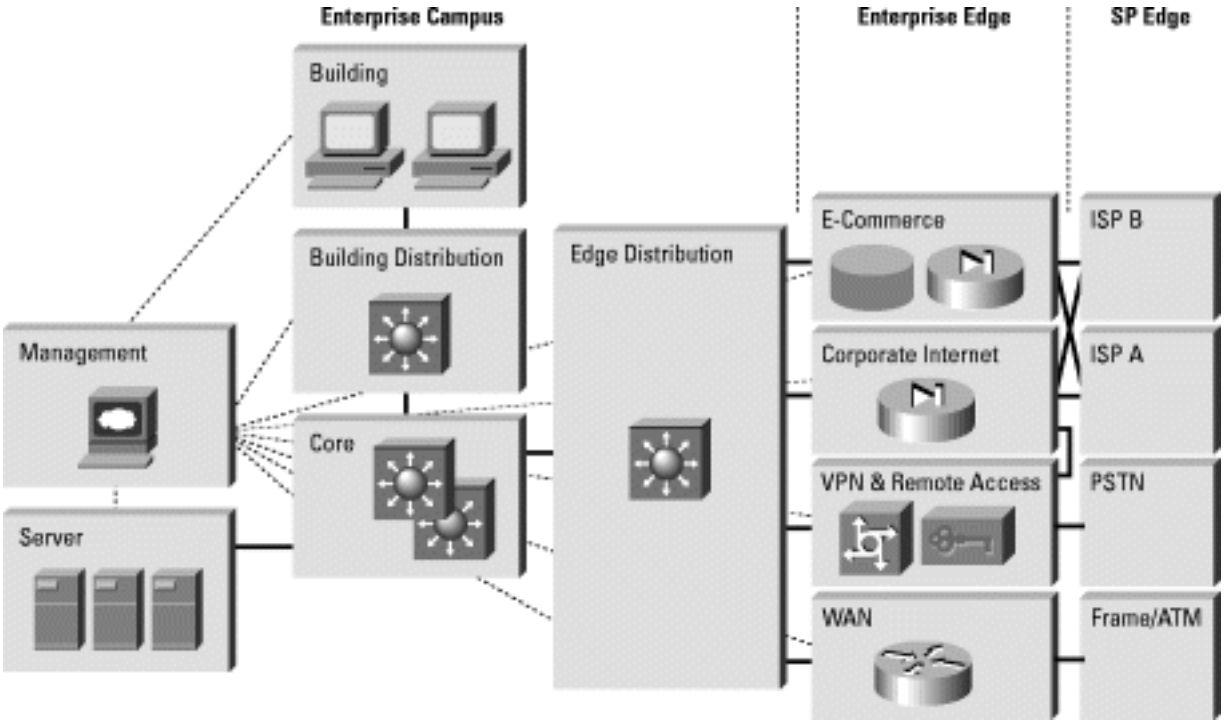


図2に示すモジュール方式の２つ目の階層は、それぞれの機能的領域におけるモジュールの全体像を表します。これらのモジュールはネットワークにおいて特定の役割を果たし、特定のセキュリティ要件を持ちますが、それぞれの大きさは特に実際のネットワークにおける規模を反映していません。たとえば、エンドユーザー向けデバイスを表すビルディングモジュールには、ネットワークデバイスの80パーセントが含まれることがあります。各モジュールのセキュリティ設計については個別に説明しますが、それぞれ完全なエンタープライズ設計の一部分として検証済みです。

図2: エンタープライズSAFEブロック図



既存のエンタープライズネットワークの大部分が、明確なモジュール単位に細かく切り分けることが容易でないことは事実ですが、このアプローチによって、異なるセキュリティ機能をネットワークの至るところに実装することが可能になります。この文書は、ネットワークエンジニアがSAFE実装と同じネットワークを設計するのではなく、以下に述べるモジュールを組み合わせて既存のネットワークに組み込むことを目的としています。

SAFE の原理

ルータがターゲットとなる場合

ルータは、すべてのネットワークからすべてのネットワークへのアクセスを制御します。ネットワークを公示し、使用できるユーザーをフィルタリングするルータは、ハッカーにとって最大の味方となる可能性を秘めています。ルータセキュリティは、すべてのセキュリティの実装においてクリティカルな要素です。ルータは、本来アクセスを提供するものであるため、その安全を確保することによって直接被害を受ける可能性を減らすことが必要です。ルータセキュリティに関するほかの文書を参照してください。次のテーマに関する詳細が記述されています。

- ルータへのtelnetアクセスのロックダウン
- ルータへのSNMP（Simple Network Management Protocol）アクセスのロックダウン
- TACACS+（Terminal Access Controller Access Control System Plus）を使用した、ルータへのアクセスの制御
- 不要なサービスの停止
- 適切なレベルでのロギング
- ルーティングアップデートの認証

ルータセキュリティに関する最新の文書は、次のURLで参照できます。

http://www.cisco.com/warp/public/707/21.html

スイッチがターゲットとなる場合

ルータと同様に、スイッチ（レイヤ2およびレイヤ3の両方）は、独自のセキュリティセットを考慮します。ルータと異なり、スイッチにおけるセキュリティのリスクや、リスクを軽減するために何ができるかについての情報は、それほど多く公開されていません。「ルータがターゲットとなる場合」のセクションで詳しく説明したセキュリティ技術のほとんどがスイッチにも適用されますが、さらに、あらかじめ次の対策を講じる必要があります。

- トランキングの不要なポートは、すべてのトランク設定をautoではなくoffに設定する必要があります。これにより、ホストがトランクポートとなって、通常はトランクポート上にあるすべてのトラフィックを受信することを防止します。
- トランクポートで使用される VLAN（仮想 LAN）番号が、スイッチのほかの場所で使用されていないことを確認してください。これにより、トランクポートと同じVLANのタグが付いたパケットが、レイヤ3デバイスを通過しないで別のVLANに到達することを防止します。詳細については、次のURLを参照してください。

  http://www.sans.org/newlook/resources/IDFAQ/vlan.htm

- スイッチの未使用ポートをすべて、レイヤ 3 接続のないVLANに設定してください。さらに、不要なポートをすべてディセーブルにしてください。これにより、ハッカーが未使用のポートにプラグインしてネットワークのその他の部分と通信することを防止します。
- 2 つのサブネット間におけるアクセスの安全を確保するための方法として、VLANを多用しないようにしてください。人為的ミスの可能性が生じるうえ、VLANおよびVLANタギングプロトコルがセキュリティの備わった設計になっていないことも考え合わせれば、機密を扱った環境でVLANを使用することはお勧めできません。VLANがセキュリティの実装において必要な場合は、必ず、前述の構成とガイドラインによく注意してください。

既存のVLANでは、プライベートVLANによって一部の追加セキュリティが特定のネットワークアプリケーションに提供されます。プライベートVLANは、同じVLAN内のほかのポートと通信可能なポートを制限することによって機能します。VLAN内で切り離されたポートは、無差別ポートとだけ通信できます。コミュニティポートは同じコミュニティポートおよび無差別ポートのほかのメンバーとだけ通信することができ、無差別ポートはすべてのポートと通信することができます。これは、被害を受けた単一ホストの影響を軽減するための効果的な方法です。Web サーバ、FTP サーバ、および DNS（Domain Name System）サーバが実装された標準のパブリックサービスセグメントを考えてみてください。DNSサーバが被害を受けると、ハッカーはファイアウォールを突破しなくてもほかの2つのホストを追跡することができます。しかし、プライベートVLANが配置されていれば、いったん被害を受けたシステムはほかのシステムと通信不可能になり、ハッカーが追跡できるターゲットは、ファイアウォールの反対側にあるホストだけになります。

ホストがターゲットとなる場合

ホストは、攻撃の際に最もターゲットになりやすく、セキュリティ面で最も困難な問題がいくつか生じます。ハードウェアプラットフォーム、オペレーティングシステム、およびアプリケーションの数は非常に多く、さらに、そのすべては、それぞれ別々にアップデート版、パッチ、および修正版が使用される必要があります。ホストは、要求するほかのホストに対してアプリケーションサービスを提供するため、ネットワーク内においてかなり目立つ存在となっています。たとえば、ホストのhttp://www.whitehouse.gov/にアクセスしたことのある人は大勢いても、ルータの s2-0.whitehouseisp.net にアクセスしようとする人はほとんどいません。こうしたアクセ

スのしやすさによって、ホストは、ネットワークに侵入しようとして攻撃される頻度が最も高いデバイスとなっています。

上述のセキュリティ問題もあって、ホストは被害を与えることに最も成功するデバイスでもあります。たとえば、インターネット上のある特定のWebサーバは、あるベンダ製のハードウェアプラットフォーム、別のベンダ製のネットワークカード、別のベンダ製のオペレーティングシステム、およびオープンソースまたは別のベンダ製のWebサーバを実行することがあります。さらに、同じWebサーバが、インターネットを介して自由に配布されるアプリケーションを実行し、その種類を繰り返し起動するデータベースサーバと通信することもあります。こうしたすべてにおけるマルチソースな性質が特にセキュリティの脆弱性の原因となっているとは言わないまでも、システムの複雑さが増すにつれ、障害が発生する可能性も高くなります。

ホストの安全を確保するには、システムにおけるそれぞれのコンポーネントによく注意を払ってください。どのシステムも、常に最新のパッチ、修正版などによって最新の状態になるようにしてください。特に、これらのパッチがほかのシステムコンポーネントの運用にどのような影響を及ぼすかに注意してください。すべてのアップデートは、テスト用のシステムで評価してから実稼動環境に実装してください。これを怠ると、パッチ自体がサービス拒否(DoS)を引き起こす原因となることがあります。

ネットワークがターゲットとなる場合

最悪の攻撃は、阻止することの不可能な攻撃です。正常に実行される場合、分散型サービス拒否 ((DDoS) がこうした攻撃となります。付録B「ネットワークセキュリティ入門」で概説しているとおり、DDoSは、何十台または何百台ものマシンから疑似データをIPアドレスに同時に送信するように仕向けることによって機能します。こうした攻撃の目的は、一般に特定のホストをシャットダウンすることではなく、ネットワーク全体を応答不可能にすることです。たとえば、E-コマースサービスをWebサイトユーザーに提供するインターネットにDS3 (45 Mbps) 接続した組織を考えてみてください。このようなサイトは、セキュリティに対する意識が非常に高く、侵入検知、ファイアウォール、ロギング、およびアクティブモニタリングを実装しています。しかし、残念なことに、ハッカーがDDoS攻撃を成功させた場合、こうしたセキュリティデバイスはどれも役に立ちません。

それぞれがインターネットにDS1(1.5 Mbps)接続している、世界中の100のデバイスを考えてみてください。これらのシステムは、E-コマース組織のインターネットルータのシリアルインターフェイスをフラッディングするようにリモートで指示されると、誤ったデータで容易にDS3をフラッディングすることができます。各ホストで1 Mbpsのトラフィックしか生成されない場合でも(研究所のテストによると、ストックのUnix ワークステーションは一般的なDDoSツールで50 Mbpsを容易に生成可能)、その量は依然としてE-コマースサイトが処理できるトラフィック量の2倍以上にもなります。この結果、公正なWeb要求が失われ、ほとんどのユーザーにはサイトがダウンしているように見えます。ローカルファイアウォールによって誤ったデータがすべてドロップされたときには、トラフィックはすでにWAN接続を介してリンクをいっぱいにしているため、被害が及んだ後となります。

ISPとの協力によってのみ、この架空のE-コマース会社がこうした攻撃を妨げることを期待できます。ISPは、企業サイトへの送信インターフェイス上にレート制限を設定することができます。このレート制限により、事前に指定された使用可能な帯域幅の容量を超えた最も不要なトラフィックをドロップすることができます。この場合、トラフィックを不要であるとして正しくフラグを立てることが鍵となります。

DDoS 攻撃の一般的な形態は、ICMP フラッド、TCP SYNフラッド、またはUDPフラッドです。E-コマース環境においては、この種のトラフィックはかなり分類しやすいものとなっています。ポート80(http)におけるTCP SYN攻撃を制限するときだけ管理者は、攻撃される間、公正なユーザーをロックアウトする(締め出す)という危険を冒します。このような場合でも、ルータをあふれさせてすべての接続を失うことに比べれば、一時的に新しい公正なユーザーをロックアウトしてルーティングと管理接続を保持する方がましです。

より高度な攻撃になると、ACKビットを設定したポート80トラフィックが使用されるため、トラフィックは公正なWebトランザクションであるかのように見えます。確認応答されたTCP通信はネットワークに許可したい種類のものであるため、管理者がこうした攻撃を正しく類別できる見込みはありません。

この種の攻撃を制限するアプローチの1つとして、RFC 1918およびRFC 2827に記述されるガイドラインに従う方法があります。RFC 1918では、プライベート使用のために予約済みで、パブリックインターネットを越えてはいけないネットワークについて規定しています。RFC 2827のフィルタリングについては、付録B「ネットワークセキュリティ入門」のセクション「IPスプーフィング」で説明しています。インターネットに接続したルータにおける受信トラフィックに対しては、RFC 1918および2827フィルタリングを使用すれば、不正なトラフィックが企業ネットワークに到達することを防止することができます。このフィルタリングをISPが実装した場合、これらのアドレスを送信元とするDDoS攻撃パケットがWANリンクを通ることを防止するため、攻撃されている間、潜在的に帯域幅を節約することができます。集束的に世界中のISPがRFC 2827のガイドラインを実装したとすると、送信元アドレスのスプーフィングは大幅に減少するでしょう。この戦略は、DDoS攻撃を直接防御するわけではありませんが、こうした攻撃の発生元が隠ぺいされることを防止するため、ネットワーク攻撃の追跡がかなり容易になります。

アプリケーションがターゲットとなる場合

アプリケーションのコーディングは（ほとんど）人間によるものであるため、たくさんのエラーが発生することがあります。こうしたエラーには、文書を不正確に印刷するエラーなどの害のないものもあれば、データベースサーバ上にあるクレジットカードの番号を、匿名FTPを介して使用可能にするエラーなどの極めて有害なものもあります。侵入検知システム（IDS）が検知のターゲットとするのは、極めて有害な問題と、より一般的なほかのセキュリティの脆弱性です。侵入検知は、物理的にはアラームシステムと同様に機能します。IDSが攻撃とみなすものを検知した場合、IDSが自ら適切に対処するか、管理者が管理システムに通知して対処してもらうことができます。一部のシステムは、多かれ少なかれこうした攻撃に対応して防御するために装備されています。ホストベースの侵入検知は、個々のホストでOSおよびアプリケーションコールを代行受信することによって機能できるほか、ローカルログファイルを事後分析することによって機能することもできます。初めのアプローチの方が攻撃に対する防御に優れているのに対し、後のアプローチの方はより受け身で攻撃に対応する役割が要求されます。こうした特異な役割を持つため、大抵は攻撃を発見すると警報を発するだけのネットワークIDS（NIDS）より、ホストベースIDS（HIDS）システムの方が、多くの場合、特定の攻撃を防御するのに優れています。しかし、この特異性によってネットワーク全体の見通しが失われることになり、この点ではNIDSの方が優れています。シスコでは、完全な侵入検知システムを実現するために、クリティカルホスト上のHIDSと、ネットワーク全体を見渡すNIDSの2つのシステムを組み合わせることをお勧めします。

いったん配置されたIDS実装は、調整によってその効果を高め、「偽陽性」(Fault Positive)を排除する必要があります。偽陽性は、公正なトラフィックまたはアクティビティが原因のアラームとして定義されています。偽陰性は、IDSシステムによって見落とされた攻撃です。調整されたIDSは、脅威を軽減する役割に応じてより明確に構成することができます。HIDSは、特定のアクティビティが実は脅威であると判断するためのものであるため、前述のとおり、最も有効な脅威をホストレベルで阻止するようにHIDSを構成する必要があります。

NIDSにおける軽減の役割を決定する場合、2つの主なオプションがあります。

1つ目のオプションで、正しく配置されないと潜在的に最も被害を与えるのは、ルータにアクセスコントロールフィルタを追加することによってトラフィックを「排除（シャニング）」することです。NIDSは、特定のプロトコルで特定のホストからの攻撃を検出すると、そのホストがネットワーク内に入り込むことを、事前に決められた時間だけブロックすることができます。この方法は、表面上はセキュリティ管理者にとって心強い味方のように見えるかもしれませんが、実際は、実装するにはかなりの注意を払う必要があります。まず、スプーフィングされたアドレスという問題があります。攻撃に匹敵するトラフィックがNIDSによって検知され、その特定のアラームによって排除応答が発生すると、NIDSはアクセスリストをデバイスに配置します。ただし、アラームの原因となった攻撃にスプーフィングされたアドレスが使用されていた場合、NIDSは、攻撃を開始していないアドレスをロックアウトしてしまいます。ハッカーが使用したIPアドレスがたまたま主要なISPの送信HTTPプロキシサーバのIPアドレスである場合、膨大な数のユーザーがロックアウトされる可能性があります。ただし、これ自体は創造力のあるハッカーの手による興味深いDoSの脅威であると言えます。

排除のリスクを軽減するには、一般に、スプーフィングの成功がUDPよりずっと困難なTCPトラフィック上だけで使用する必要があります。脅威が現実のものとなり、攻撃が偽陽性である見込みが極めて低い場合にだけ使用してください。ただし、ネットワークの内部には、より多くのオプションがあります。効果的に配置されたRFC 2827フィルタリングにより、スプーフィングされたトラフィックをかなり制限する必要があります。また、通常、カスタマは内部ネットワーク上にいないため、内部で発生する攻撃に対してより規制したスタンスをとることができます。これは、多くの場合、エッジ接続に実装されるステートフルフィルタリングの同じレベルが内部ネットワークに実装されているためでもあります。このため、外部環境よりもIDSにより重点を置くことが必要です。

NIDSの脅威の軽減における2つ目のオプションは、TCPリセットの使用です。名前のとおり、TCPリセットはTCPトラフィックでのみ動作し、攻撃する、または攻撃されるホストにTCPリセットメッセージを送信することによって、アクティブな攻撃を終わらせます。TCPトラフィックではスプーフィングがより困難になるため、排除よりTCPリセットを多用することを検討する必要があります。

パフォーマンスの面から、NIDSはワイヤ上でパケットを監視します。NIDSの処理能力より速くパケットが送信されてきた場合、NIDSは直接データの流れの中にあるわけではないため、ネットワークには影響がありません。ただし、NIDSは効果を失い、パケットは見落とされている可能性があり、偽陰性や偽陽性の原因となります。利点を活かすことができるように、できるだけ、IDSの処理能力を超えないようにしてください。ルーティングの面から、IDSは、多くの状態認識エンジンと同様に非対称ルーティング環境では正しく動作しません。あるルータとスイッチの組み合わせから送出されて別の組み合わせから戻されるパケットは、IDSシステムがトラフィックの半分しか監視できない原因となるため、偽陽性および偽陰性が発生することになります。

安全な管理とレポート

「ログをとるなら、読みなさい。」とても単純な命題であるため、ネットワークセキュリティに精通した人なら、少なくとも一度はこう言ったことがあるでしょう。しかし、100を超えるデバイスから情報をロギングおよび読み取ることは、骨の折れる仕事であることがわかっています。どのログが最も重要なのか。重要なメッセージとただの通知はどうやって区別するのか。送信中にログが改ざんされな

いようにするにはどうするのか。複数のデバイスが同じアラームを報告する場合にタイムスタンプが互いに一致するようにするにはどうするのか。ログデータが犯罪調査に要求される場合、どの情報が必要なのか。大規模なネットワークで生成される大量のメッセージをどのように処理するのか。ログファイルの効果的な管理を検討する際は、こうした問いのすべてに取り組む必要があります。管理の面からは、次の一連の問いに答える必要があります。どうやってデバイスを安全に管理するのか。コンテンツをパブリックサーバに送信し、送信中に改ざんされないようにするにはどうするのか。攻撃またはネットワーク障害が発生した場合、どうやってデバイス上の変更を突き止められるのか。

アーキテクチャの面からは、ネットワークシステムをアウトバンドで管理することが、管理およびレポート戦略における第一歩として最も適しています。アウトバンド（OOB）とは、名前が示すとおり、実稼動トラフィックのないネットワークを指します。デバイスは、可能な限り、こうしたネットワークに直接ローカルで接続し、不可能な場合（地理的またはシステム関連の問題のため）は、実稼動ネットワーク上の暗号化されたプライベートトンネルを通って接続する必要があります。このようなトンネルは、管理およびレポートに必要な特定のポート間だけで通信するように事前に構成し、さらに、適切なホストだけがトンネルを開始および終端できるようにロックダウンする必要もあります。必ず、アウトバンドネットワーク自身によってセキュリティ問題が生じることのないようにしてください。詳細については、この文書の「管理モジュール」のセクションを参照してください。

OOB管理ネットワークを実装すると、ロギングおよびレポート処理はより確実になります。ネットワーキングデバイスの大部分がsyslogデータを送信することができるため、ネットワークの問題やセキュリティの脅威をトラブルシュートする場合に計り知れないほど貴重なものとなります。このデータを管理ネットワーク上の1つまたは複数のsyslog分析ホストに送信してください。デバイスによってさまざまなロギングレベルから選択でき、正しい量のデータをロギングデバイスに送信することができます。また、細かい表示やレポートを可能にするには、解析ソフトウェアのデバイスログデータにフラグを立てる必要もあります。たとえば、攻撃の間、レイヤ2スイッチによって提供されるログデータは、侵入検知システムによって提供されるデータに比べて関心を引かないことがあります。IDSなどの専用のアプリケーションでは、ほとんどの場合、独自のロギングプロトコルを使用してアラーム情報を送信しています。通常、このデータをロギングして、攻撃アラームを処理するために装備されている管理ホストを切り離す必要があります。多数の異なるソースからのアラームデータは、統合されると、ネットワーク全体の状態に関する情報を提供することができます。ログメッセージの時刻が互いに同期するように、ホストとネットワークデバイスの時計が同期している必要があります。これがサポートされるデバイスでは、ネットワークタイムプロトコル（NTP）によって、すべてのデバイスで正確な時刻に維持されることが保証されます。攻撃に対処するときは、1秒単位が問題になります。指定の攻撃が発生した順番を識別するために重要となるためです。

この文書は、管理者が管理目的でロギングやレポート以外にデバイス上で実行する機能について記述していますが、その管理の面から、ほかの問題および解決策があります。ロギングやレポートの場合と同様に、OOBネットワークでは、改ざんされにくい管理環境で情報をトランスポートすることができます。ただし、セキュアソケットレイヤ（SSL）またはセキュアシェル（SSH）の使用などによって安全な構成が可能な場合は、こちらを選択する必要があります。基礎となるプロトコル自身に一連のセキュリティの脆弱性があるため、SNMPは最大の注意を払って処理する必要があります。SNMPによってデバイスへ読み取り専用でアクセスすることを検討し、ルートパスワードをクリティカルなUnixホスト上で処理する場合と同様に、注意してSNMPコミュニティストリングを処理してください。

安全管理に関しては、構成変更管理という問題もあります。ネットワークが攻撃を受けた場合、クリティカルなネットワークデバイスの状態と、最後の変更がいつ行われたのかを知ることが重要です。包括的なセキュリティポリシーの一部分として、変更管理の計画を立てることが必要ですが、最低限、デバイス上の認証システムを使用して変更を記録し、FTPまたはTFTPによって構成をアーカイブしておいてください。

エンタープライズモジュール

企業は、機能上、キャンパスとエッジの2つの領域から構成されています。この2つの領域はさらに、各領域のさまざまな機能が詳細に規定されたモジュールに分けられます。この文書の「エンタープライズキャンパス」と「エンタープライズエッジ」のセクションで各モジュールについて詳しく説明した後、「エンタープライズオプション」のセクションで設計のさまざまなオプションについて説明します。

予測される脅威

エンタープライズネットワークは、脅威の面でインターネットに接続した大部分のネットワークと同様であり、外部へのアクセスが必要な内部ユーザーと、内部へのアクセスが必要な外部ユーザーがあります。一般的な脅威のなかには、最初に被害を受けた後に、二次的な悪用によってハッカーがさらにネットワークに侵入する可能性のあるものもあります。

1つ目は、内部ユーザーからの脅威です。統計によって割合が異なりますが、大多数の攻撃が内部のネットワークから発生しているということは既成の事実です。不平不満を持った従業員、企業スパイ、訪問客、不注意で無能なユーザーはすべて、こうした攻撃の原因となる可能性を秘めています。セキュリティを設計する際は、内部からの脅威の可能性を考慮することが重要です。

2つ目は、インターネットに接続した、公的にアドレス指定可能なホストに対する脅威です。こうしたシステムは、アプリケーションレイヤの脆弱性とDoS攻撃によって攻撃される可能性が高くなります。

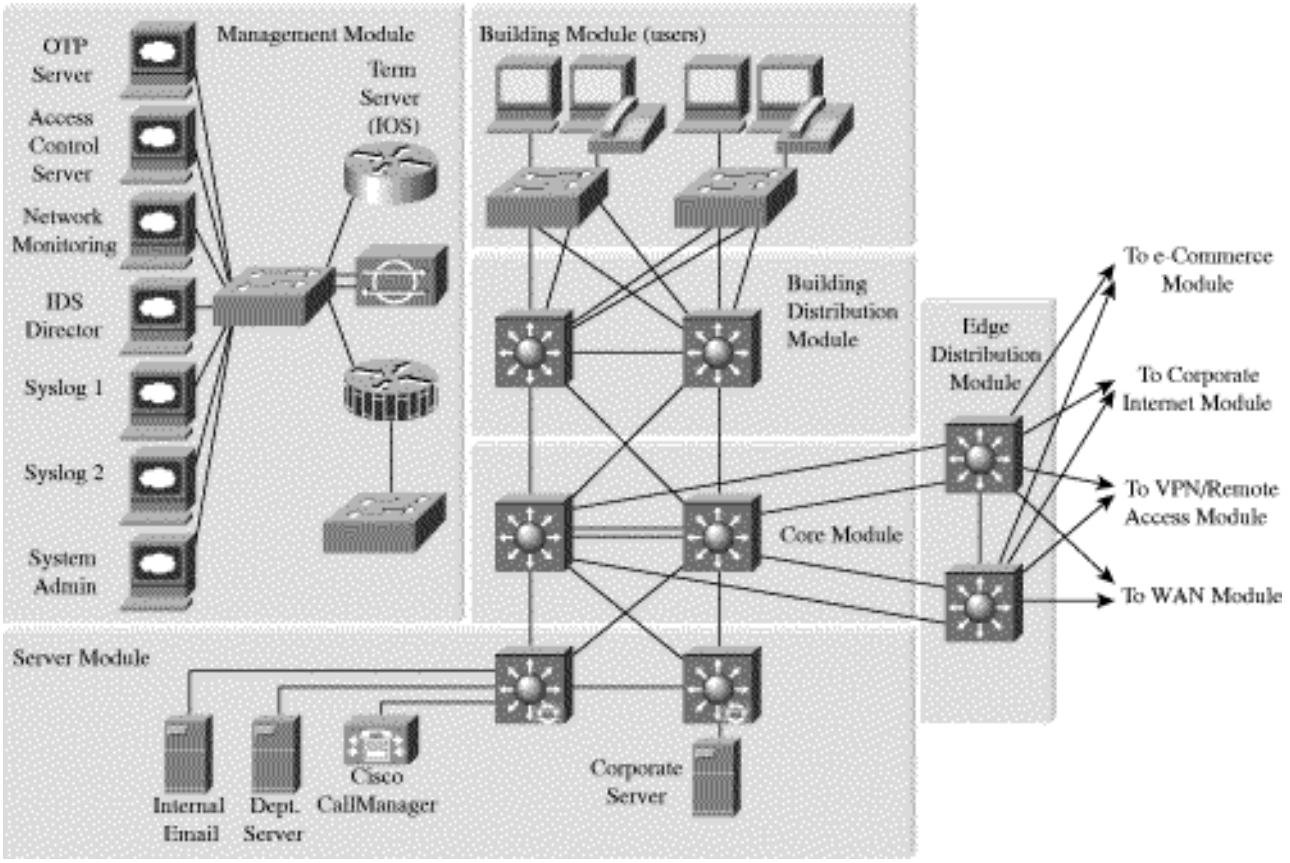
最後の脅威は、ハッカーが「war-dialer」を使用してデータの電話番号を特定し、ネットワークにアクセスしようとするものです。war-dialerは、多数の電話番号をダイヤルして接続先のシステムの種類を判別するために設計されたソフトウェアでありハードウェアでもあります。リモート制御ソフトウェアがユーザーによってインストールされているパーソナルシステムは、通常、安全性が極めて低いため、最も脆弱性が高くなります。こうしたデバイスはファイアウォールの後方にあるため、いったんダイヤルインしたホストを介してアクセス権を取得すれば、ハッカーはネットワーク上のユーザーになりすますことができるのです。

脅威に関する詳細については、付録B「ネットワークセキュリティ入門」を参照してください。

エンタープライズキャンパス

エンタープライズキャンパスに含まれるすべてのモジュールの詳細な解析図を以下に示します。

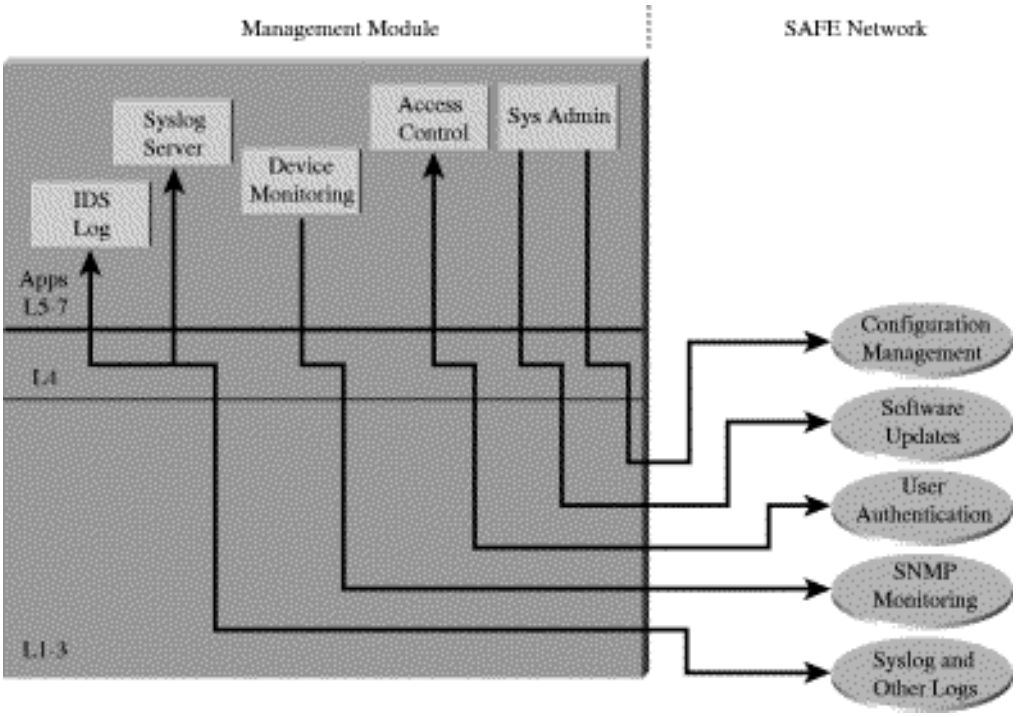
図3: エンタープライズキャンパスの詳細



管理モジュール

管理モジュールの主な目的は、企業のSAFEアーキテクチャにおけるすべてのデバイスおよびホストの安全な管理を容易にすることです。ログ情報とレポート情報がデバイスから管理ホストの方向へ送信され、コンテンツ、構成、および新しいソフトウェアが管理ホストからデバイスの方向へ送信されます。

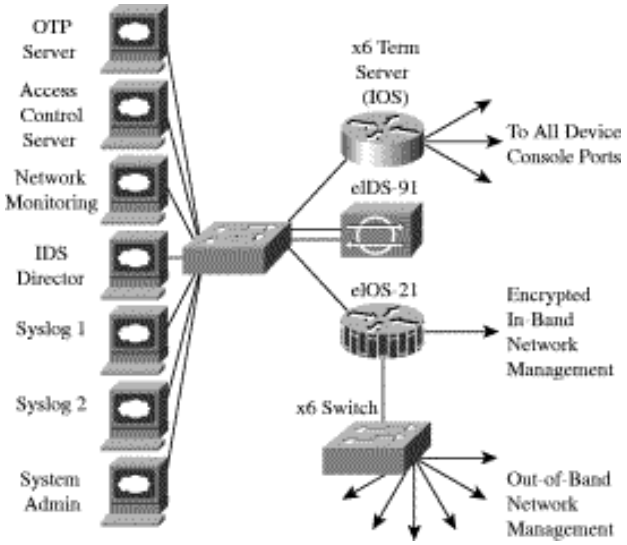
図4: 管理トラフィックフロー



主要デバイス

- **SNMP管理ホスト** --- デバイスのSNMP管理を提供
- **NIDSホスト** --- ネットワーク内のNIDSデバイスすべてのアラームを集束
- **Syslogホスト** --- ファイアウォールとNIDSホストのログ情報を集束
- **アクセスコントロールサーバ** --- ワンタイムの2ファクタ認証サービスをネットワークデバイスに提供
- **ワンタイムパスワード(OTP)サーバ** --- アクセスコントロールサーバから送信されたワンタイムパスワード情報に権限を付与
- **System Adminホスト** --- デバイスの構成、ソフトウェア、およびコンテンツを変更
- **NIDS機器** --- モジュール内における主なネットワークセグメントのレイヤ4～レイヤ7モニタリングを提供
- **Cisco IOSファイアウォール** --- 管理ホストと管理対象デバイスの間のトラフィックフローを細かく制御
- **レイヤ2スイッチ(プライベートVLANのサポート)** --- 管理対象デバイスからのデータだけに直接IOSファイアウォールを通過させる

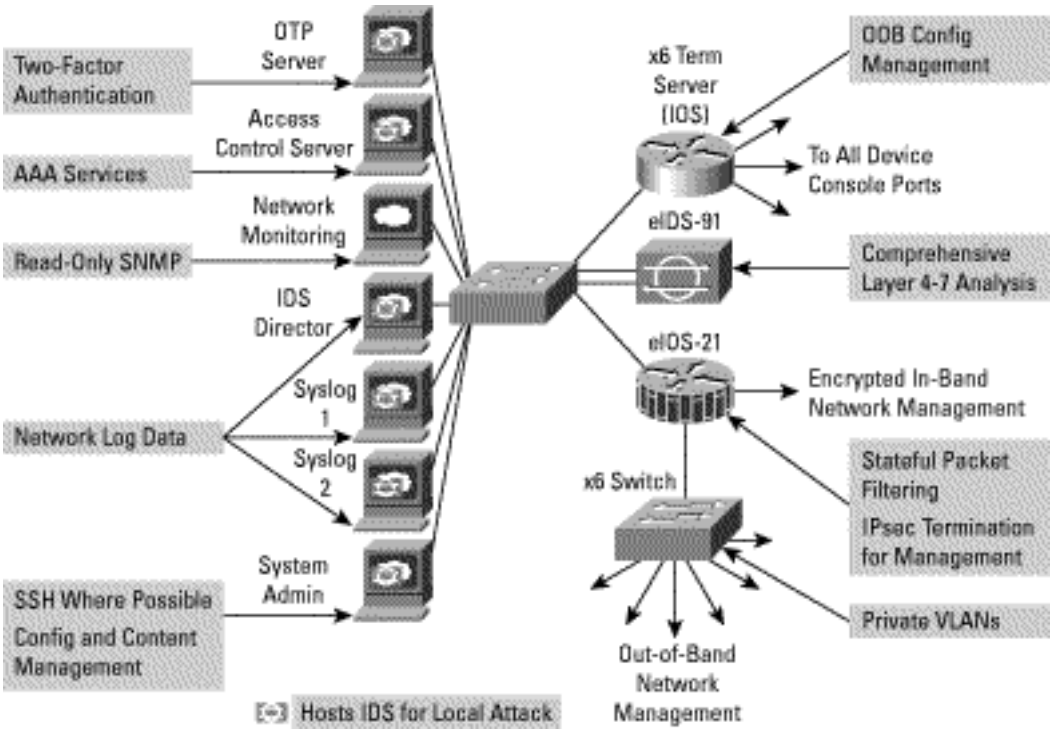
図5: 管理モジュール(詳細)



脅威の軽減

- **不正アクセス** --- IOSファイアウォールでのフィルタリングにより、両方向における不正なトラフィックの大部分を阻止
- **Man-in-the-Middle攻撃** --- 管理データが、man-in-the-middle攻撃の困難なプライベートネットワークを通過
- **ネットワーク偵察** --- すべての管理トラフィックがこのネットワークを通るため、傍受される可能性のある実稼動ネットワークを通らない
- **パスワード攻撃** --- アクセスコントロールサーバにより、デバイスごとに強固な2ファクタ認証が可能
- **IPスプーフィング** --- IOSファイアウォールで、両方向におけるスプーフィングされたトラフィックを阻止
- **パケットスニファ** --- スイッチ型インフラストラクチャにより、スニッフィングの効果を制限
- **信用詐欺** --- プライベートVLANにより、被害を受けたデバイスが管理ホストになりすますことを防止

図6: 攻撃軽減における管理モジュールの役割



設計ガイドライン

上図で示したように、SAFE企業管理ネットワークは2つのネットワークセグメントから構成されており、ファイアウォールやVPN終端デバイスとしての機能を持つIOSルータによって分けられています。ファイアウォールの外側のセグメントは、管理を必要とするすべてのデバイスに接続します。ファイアウォールの内側のセグメントには、管理ホスト自身と、ターミナルサーバとしての機能を持つIOSルータが含まれます。残りのインターフェイスは、あらかじめ決められたホストからのIPSecで保護された管理トラフィックだけを除き、実稼動ネットワークに接続します。これにより、通常の管理接続をサポートするための十分な物理的インターフェイスがなかったCiscoデバイスの管理が可能になります。最初にtelnet、SSH、およびSNMPが内部のネットワークで開始されるとsyslog情報も管理セグメントに送信されるように、IOSファイアウォールが構成されています。

いずれの管理サブネットも、実稼動ネットワークの残りの部分からは完全に切り離されたアドレス空間の下で動作します。このため、管理ネットワークがルーティングプロトコルによって公示されることはありません。さらに、実稼動ネットワークデバイスは、実稼動ネットワークリンク上に出現する管理サブネットからのトラフィックをすべてブロックすることができます。

管理モジュールでは、ターミナルサーバとして動作するCisco IOSルータ、専用の管理ネットワークセグメントの2つの主要テクノロジの使用によって、ネットワーク内のほとんどすべてのデバイス構成を管理します。ルータは、企業全体におけるCiscoデバイスのコンソールポートへの逆telnet機能を備えています。また、より広範な管理機能(ソフトウェアの変更、コンテンツのアップデート、ログおよびアラーム集束、およびSNMP管理)が、専用の管理ネットワークセグメントによって提供されます。その他少数の管理対象外のデバイスやホストは、管理ルータから発生するIPSecトンネルを介して管理されます。

管理ネットワークは、管理上、ネットワークのほとんどすべての領域にアクセスできるため、ハッカーにとって格好のターゲットとなり得ます。管理モジュールは、こうしたリスクを軽減するために設計された各種のテクノロジを使用して構築されています。最初の主な脅威は、ハッカーが管理ネットワークにアクセスしようと試みることです。この脅威を軽減するには、企業の残りのモジュールにセキュリティ機能を効果的に配置する方法しかありません。これ以外の脅威はすべて、主要な防御線を突破していると推測されます。被害を受けたデバイスの脅威を軽減するためには、ファイアウォールやほかの考えられるデバイスのすべてにおいてアクセス制御を実施することで、管理チャネルの悪用を防止します。被害を受けたデバイスは、同じサブネット上のほかのホストと通信することさえできなくなります。これは、管理セグメントスイッチにおけるプライベートVLANによって、すべてのトラフィックが管理対象のデバイスからフィルタリングが行われるIOSファイアウォールに直接送信されるためです。パスワードスニッフィングの場合、ワンタイムパスワード環境により、役に立たない情報のみを明かします。また、ホストおよびネットワークIDSも管理サブネット上に実装され、かなり規制したスタンスで構成されています。このネットワーク上のトラフィックの種類は制限される必要があるため、このセグメントでシグニチャが一致した場合は即時に対応する必要があります。

SNMP管理は、固有の一連のセキュリティを必要とします。SNMPトラフィックは、管理セグメント上に保持されるため、デバイスから管理情報を受け取るときに分離されたセグメントを通ることができます。SAFEの場合、SNMP管理では情報を変更することはできず、デバイスから情報を受け取るだけです。これを保証するため、各デバイスは「読み取り専用」ストリングだけで構成されています。

syslog情報を正しく集束して分析することは、ネットワークを正しく管理するうえで重要です。セキュリティの面から、syslogはセキュリティ違反や構成の変更に関する重要な情報を提供します。問題のデバイスによっては、複数レベルのsyslog情報が要求されることがあります。フルロギングによってすべてのメッセージが送信された場合、個別のまたはsyslog分析アルゴリズムでソートするには情報が多すぎることがあります。ロギングのためのロギングでは、セキュリティは向上しません。

SAFE検証実験では、すべての構成にスタンドアロン型の管理アプリケーションとコマンドラインインターフェイス（CLI）が使用されましたが、ポリシー管理システムを使用することも可能です。この管理モジュールを設定すれば、こうしたテクノロジの配置が完全に実行可能になります。CLIおよびスタンドアロン型の管理アプリケーションを選択したのは、現在のネットワーク展開の大多数がこの構成手段をとっているためです。

代替案

完全なアウトバンド管理が常に可能であるとは限りません。デバイスでサポートされないことや、地理的な相違によってインバンド管理が必要になることがあるためです。インバンド管理が要求される場合は、管理プロトコルのトランスポートにおける安全性の確保により重点を置く必要があります。これを可能にするため、管理情報が通過できる、IPSec、SSH、SSLなどの暗号化および認証されたトランスポートを使用します。ユーザーデータ用に使用されるデバイスの同じインターフェイスで管理が発生する場合は、パスワード、コミュニティストリング、暗号キー、および管理サービスとの通信を制御するアクセスリストに重点を置く必要があります。

近い将来のアーキテクチャの目標

レポートおよびアラーム機能の実装は、現在は複数のホストに分かれています。一部のホストはファイアウォールとIDSデータを分析するためのインテリジェンスを備えていますが、それ以外のホストはルータ分析とデータ交換により適した設計になっています。将来的には、すべてのデバイス間においてイベントの相関性ができるように、すべてのデータが同じ冗長ホスト群に集束される予定です。

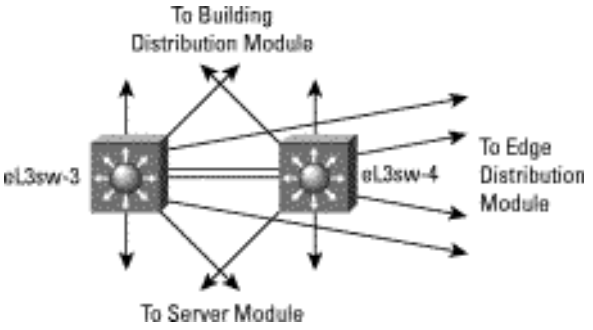
コアモジュール

SAFEアーキテクチャのコアモジュールは、ほかのすべてのネットワークアーキテクチャのコアモジュールとほぼ同じです。トラフィックをあるネットワークから別のネットワークにできるだけ速くルーティングおよび交換します。

主要デバイス

- **レイヤ3スイッチング** --- 実稼動ネットワークデータをあるモジュールから別のモジュールにルーティングおよび交換

図7:コアモジュール（詳細）



脅威の軽減

- **パケットスニファ** --- スイッチ型インフラストラクチャにより、スニッフィングの効果を制限

設計ガイドライン

優れた設計のCiscoベースネットワークに共通して見られる「コア、ディストリビューション、およびアクセスレイヤ」の配置に対応した標準実装のガイドラインに従っています。

エンタープライズネットワークのコアに固有の要件はSAFEアーキテクチャで定義されていませんが、コアスイッチは「スイッチがターゲットとなる場合」のセクションのスイッチセキュリティの原理に従い、直接の攻撃から十分に保護されることを保証しています。

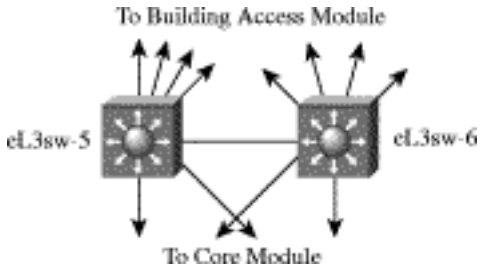
ビルディングディストリビューションモジュール

このモジュールの目的は、ルーティング、QoS（Quality of Service）、アクセス制御といったディストリビューションレイヤサービスをビルディングスイッチに提供することです。データの要求はビルディングスイッチおよびコアの方向へ送信され、応答は同じパスを反対方向に送信されます。

主要デバイス

- **レイヤ3スイッチ** --- ビルディングモジュール内のレイヤ2スイッチを集束し、高度なサービスを提供

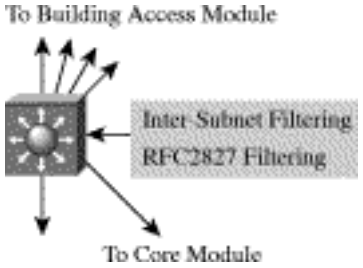
図8: ビルディングディストリビューションモジュール（詳細）



脅威の軽減

- **不正アクセス** --- サーバモジュールのリソースに対する攻撃を、特定のサブネットのレイヤ3フィルタリングによって制限
- **IPスプーフィング** --- RFC 2827フィルタリングにより、スプーフィング試行の大部分を阻止
- **パケットスニファ** --- スイッチ型インフラストラクチャにより、スニッフィングの効果を制限

図9: 攻撃の軽減におけるビルディングディストリビューションモジュールの役割



設計ガイドライン

基本的な標準ネットワーク設計のほかに、「スイッチがターゲットとなる場合」のセクションで述べた最適化を実装することで、企業ユーザーに対して追加のセキュリティを提供します。侵入検知は、攻撃される可能性が高いコンテンツのリソース（サーバ、リモートアクセス、インターネットなど）を含むモジュールに実装されるため、ビルディングディストリビューションモジュールには実装されません。ビルディングディストリビューションモジュールは、最初の防御線と、内部で発生した攻撃に対する防御を提供します。また、アクセス制御によって、ある部門が別の部門のサーバ上にある機密情報にアクセスする可能性を減らすことができます。たとえば、マーケティング、調査、および開発を行うネットワークにおいて、R&Dサーバを特定のVLANに分化し、フィルタリングによってR&Dスタッフだけがそのに VLANにアクセスできるようにする場合があります。パフォーマンスの理由から、このアクセス制御は、フィルタリングされたトラフィックをほぼワイヤレートで配送可能なハードウェアプラットフォーム上で実行することが重要です。このため、通常、より従来型の専用ルーティングデバイスと対照的なレイヤ3スイッチングの使用が必要になります。この同じアクセス制御で、RFC 2827フィルタリングを使用してローカルな送信元アドレススプーフィングを防止することもできます。最後に、サブネットの切り離しにより、VoIP（Voice over IP）トラフィックがコールマネージャおよび関連するゲートウェイのすべてにルーティングされます。これにより、ほかのすべてのデータトラフィックが通過できる同じセグメントをVoIPトラフィックが通過できないため、音声通信がスニッフィングされる可能性が減り、QoSがよりスムーズに実施されます。

代替案

ネットワークの大きさおよびパフォーマンス要件次第で、ディストリビューションレイヤをコアレイヤと一体化することにより、その環境に必要なデバイスの数を減らすことができます。

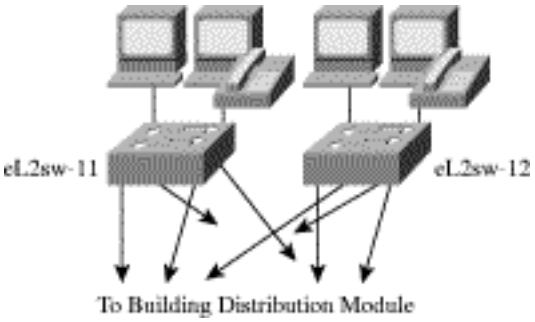
ビルディングモジュール

SAFEでは、ビルディングモジュールを、エンドユーザーワークステーション、電話、および関連するレイヤ2アクセスポイントを含む広範囲なネットワーク部分として定義しています。ビルディングモジュールの主な目的は、サービスをエンドユーザーに提供することです。

主要デバイス

- **レイヤ2スイッチ** --- レイヤ2サービスを電話とユーザーワークステーションに提供
- **ユーザーワークステーション** --- データサービスをネットワーク上の権限のあるユーザーに提供
- **IP電話** --- IPテレフォニーサービスをネットワーク上のユーザーに提供

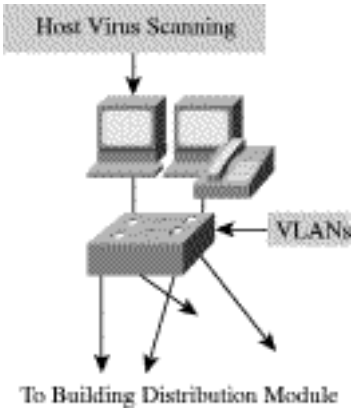
図10: ビルディングアクセスモジュール(詳細)



脅威の軽減

- **パケットスニファ** --- スイッチ型インフラストラクチャと既定のVLANサービスにより、スニッフィングの効果を制限
- **ウイルスおよびトロイの木馬アプリケーション** --- ホストベースのウイルススキャンにより、大部分のウイルスと多くのトロイの木馬を防止

図11: 攻撃の軽減におけるビルディングアクセスモジュールの役割



設計ガイドライン

ユーザーデバイスは、通常、ネットワークの最も大きい単一要素であるため、簡潔かつ効果的な方法でセキュリティを実装することは困難です。セキュリティの面から、ビルディングモジュール内のものではなく、ビルディングディストリビューションモジュールがエンドユーザーレベルで行われるアクセス制御の大部分を提供します。これは、ワークステーションや電話が接続するレイヤ2スイッチではレイヤ3のアクセスを制御できないためです。スイッチセキュリティの原理で述べたネットワークセキュリティのガイドラインのほかに、ホストベースのウイルススキャンがワークステーションレベルで実装されます。

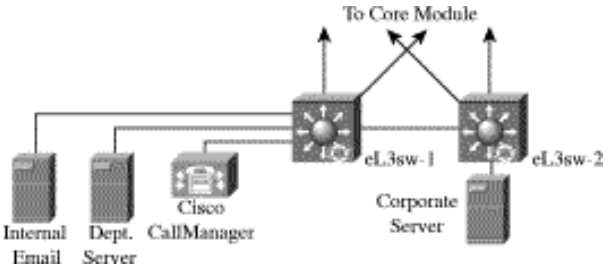
サーバモジュール

サーバモジュールの主な目的は、アプリケーションサービスをエンドユーザーとデバイスに提供することです。サーバモジュールにおけるトラフィックフローは、レイヤ3スイッチ内蔵の侵入検知によって検査されます。

主要デバイス

- **レイヤ3スイッチ** --- レイヤ3サービスをサーバに提供し、サーバモジュールを通過するデータをNIDSによって検査
- **コールマネージャ** --- 企業内のIPテレフォニーデバイスのコールルーティング機能を実行
- **企業サーバと部門サーバ** --- ファイル、印刷、DNSの各サービスをビルディングモジュール内のワークステーションに提供
- **電子メールサーバ** --- SMTPサービスとPOP3サービスを内部ユーザーに提供

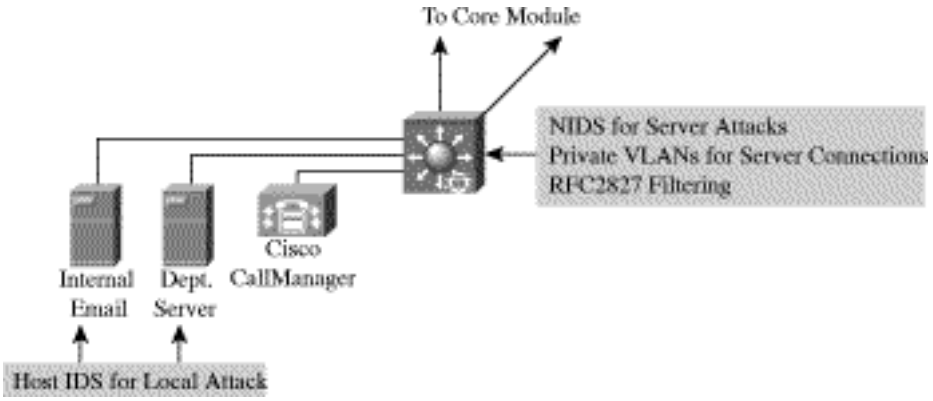
図12: サーバモジュール(詳細)



脅威の軽減

- **不正アクセス** --- ホストベースの侵入検知とアクセス制御によって軽減
- **アプリケーションレイヤ攻撃** --- オペレーティングシステム、デバイス、およびアプリケーションを常に最新のセキュリティ修正の状態にし、ホストベースのIDSによって保護
- **IPスプーフィング** --- RFC 2827フィルタリングにより、送信元アドレススプーフィングを防止
- **パケットスニファ** --- スイッチ型インフラストラクチャにより、スニッフィングの効果を制限
- **信用詐欺** --- 信頼の取り決めが明確で、必要でない限り、プライベートVLANによって同じサブネット上のホストが通信することを防止
- **ポート転送** --- ホストベースのIDSにより、ポート転送エージェントがインストールされることを防止

図13: 攻撃の軽減におけるサーバモジュールの役割



設計ガイドライン

サーバモジュールは、セキュリティの面で見落とされがちです。大部分の従業員が接続するサーバに対して持つアクセスのレベルを調査すると、多くの場合、サーバは内部で発生した攻撃の主な目標地点となる可能性があります。単に効果的なパスワードを使用するだけでは、包括的な攻撃軽減戦略に対応できません。ホストおよびネットワークベースのIDS、プライベートVLAN、アクセス制御、および十分なシステム管理の慣行（システムを常に最新のパッチ状態にするなど）によって、攻撃に対するより包括的な対応が可能になります。

NIDSシステムで分析可能なトラフィック量は制限されるため、攻撃されやすいトラフィックだけを送信することが重要です。ネットワークによって異なりますが、SMTP、Telnet、FTP、WWWなどがこれに含まれる必要があります。スイッチベースのNIDSが選択されたのは、すべてのVLANにおいて、セキュリティポリシーで規定した目的のトラフィックだけを監視できるためです。要求されるトラフィックストリームは周知のものであることが必要なため、いったん適切に調整すれば、このIDSの設定に制約を加えることができます。

代替案

ビルディングディストリビューションモジュールと同様に、パフォーマンスの必要性によって切り離す必要がない場合は、サーバモジュールをコアモジュールに一体化することができます。機密性の極めて高い高性能サーバ環境の場合は、複数のNIDSブレードをインストールし、ポリシーと一致したトラフィックを特定のブレードに送信することで、レイヤ3スイッチのNIDS機能を拡張することができます。

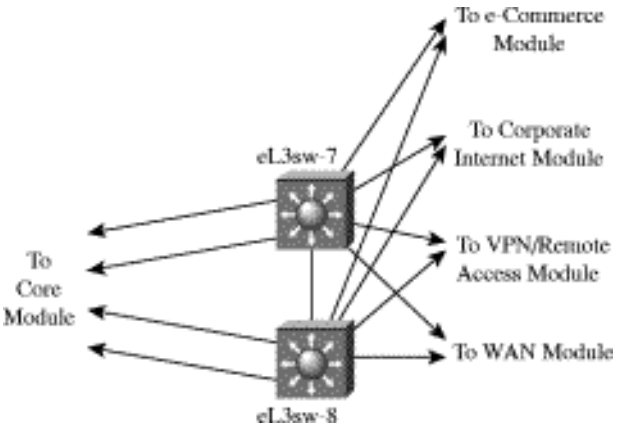
エッジディストリビューションモジュール

このモジュールの目的は、さまざまな要素からの接続をエッジで集束することです。トラフィックはフィルタリングされ、エッジモジュールからコアにルーティングされます。

主要デバイス

- **レイヤ3スイッチ** --- エッジの接続を集束し、高度なサービスを提供

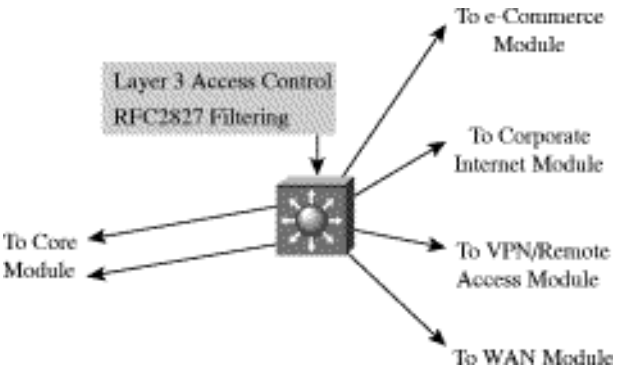
図14: エッジディストリビューションモジュール（詳細）



脅威の軽減

- **不正アクセス** --- フィルタリングにより、特定のエッジサブネット、およびサブネットが到達できるキャンパス内の領域を細かく制御
- **IPスプーフィング** --- RFC 2827フィルタリングにより、ローカルで開始されるスプーフ攻撃を制限
- **ネットワーク偵察** --- フィルタリングによって重要でないトラフィックをキャンパス内に入れないことで、ハッカーによるネットワーク偵察を制限
- **パケットスニファ** --- スイッチ型インフラストラクチャにより、スニッフィングの効果を制限

図15: 攻撃の軽減におけるエッジディストリビューションモジュールの役割



設計ガイドライン

エッジディストリビューションモジュールは、機能全体から見て、ビルディングディストリビューションモジュールといくつかの点で似ています。いずれのモジュールもトラフィックのフィルタリングにアクセス制御を使用していますが、エッジディストリビューションモジュールは、エッジの機能的領域全体にある程度依拠して追加のセキュリティ機能を実行することができます。いずれのモジュールも、レイヤ3スイッチングの使用によって高性能を実現しますが、パフォーマンス要件がそれほど高くないため、エッジディストリビューションモジュールはさらにセキュリティ機能を追加することができます。エッジディストリビューションモジュールは、エッジモジュールからキャンパスモジュールに宛てたすべてのトラフィックに対して最後の防御線を提供し、スプーフィングされたパケットや間違ったルーティング更新の軽減、およびネットワークレイヤのアクセス制御といった機能を提供します。

代替案

サーバモジュールやビルディングディストリビューションモジュールと同様に、パフォーマンス要件がSAFE参照実装ほど厳しくない場合は、エッジディストリビューションモジュールをコアモジュールに一体化することができます。NIDSはこのモジュールに置かれませんが、レイヤ3スイッチでIDSラインカードを使用すれば置くことができます。こうすることで、クリティカルなエッジモジュールからキャンパスに接続する出力点において、NIDS機器の必要性が少なくなります。ただし、パフォーマンスが原因で、SAFEの参照設計の場合のように、エッジディストリビューションモジュールと対照的なさまざまなエッジモジュールに専用の侵入検知を配置することを要求されることがあります。

エンタープライズエッジ

エンタープライズエッジに含まれるすべてのモジュールの詳細な解析図を以下に示します。

図16: エンタープライズエッジの詳細（パート1）

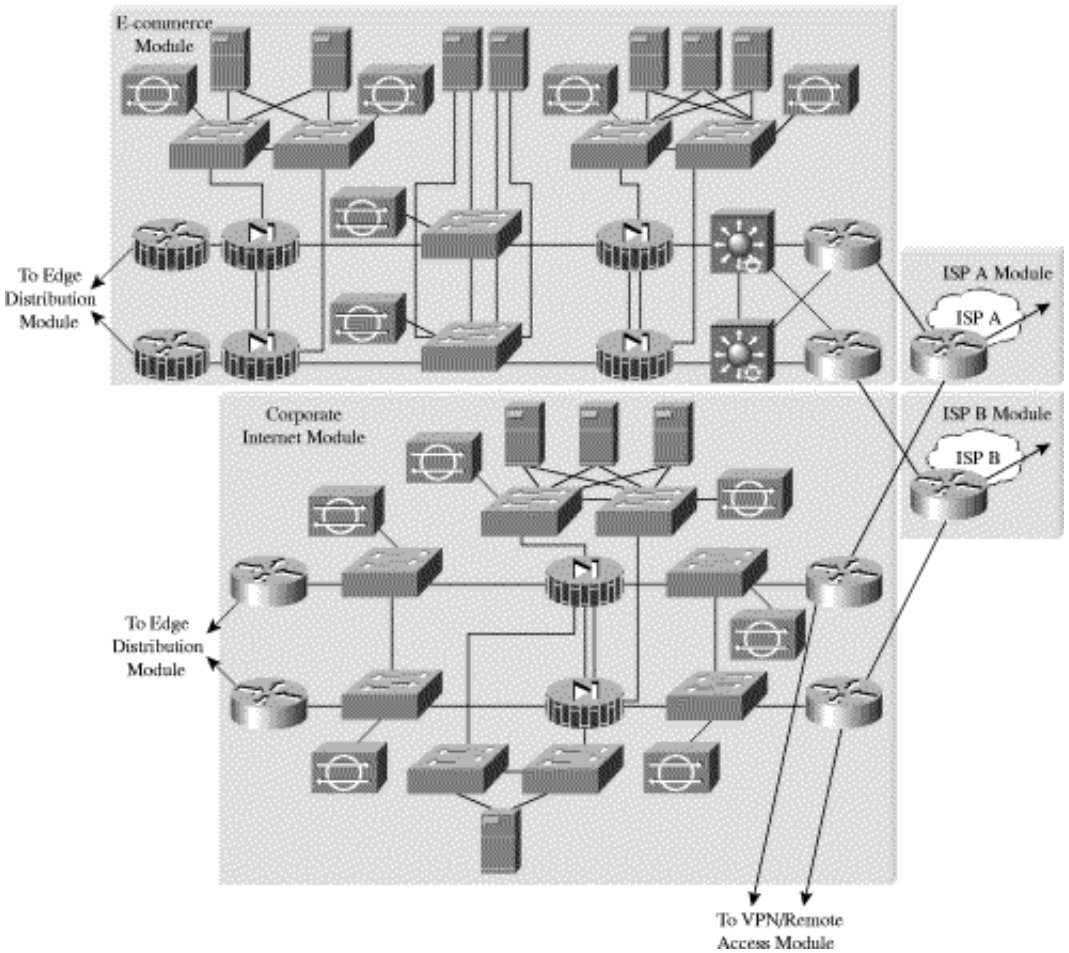
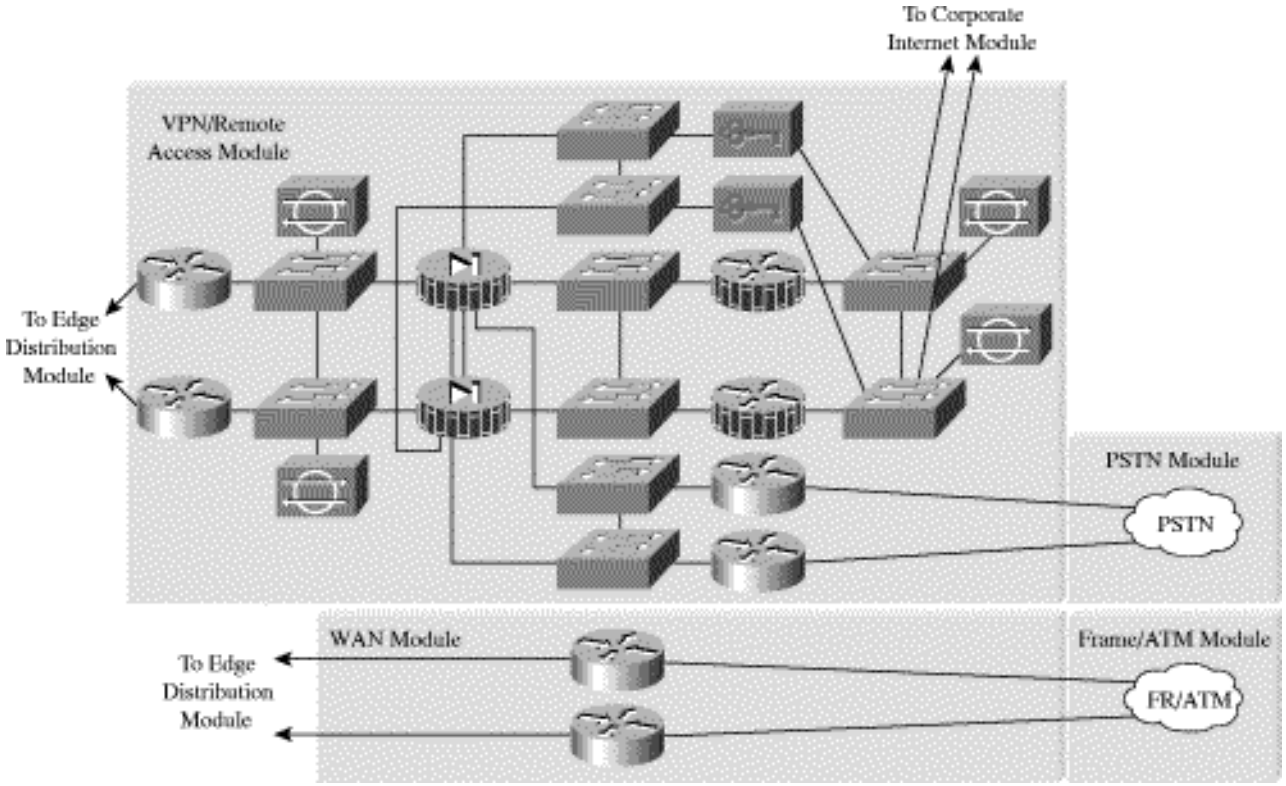


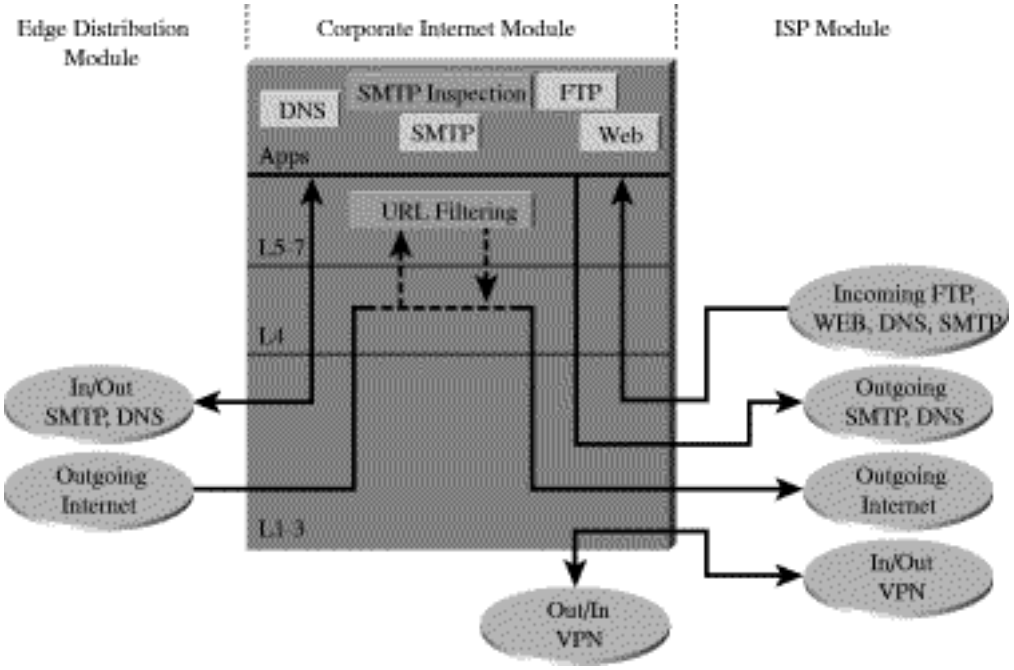
図17 :エンタープライズエッジの詳細(パート 2)



企業インターネットモジュール

企業インターネットモジュールは、インターネットサービスへの接続、およびパブリックサーバ上の情報へのインターネットユーザーアクセスを内部ユーザーに提供します。トラフィックは、このモジュールから、VPN 終端が発生するVPNおよびリモートアクセスモジュールの方向へ送信されます。このモジュールは、E-コマースタイプのアプリケーションに対応していません。インターネットコマースの提供における詳細については、この文書の「E-コマースモジュール」のセクションを参照してください。

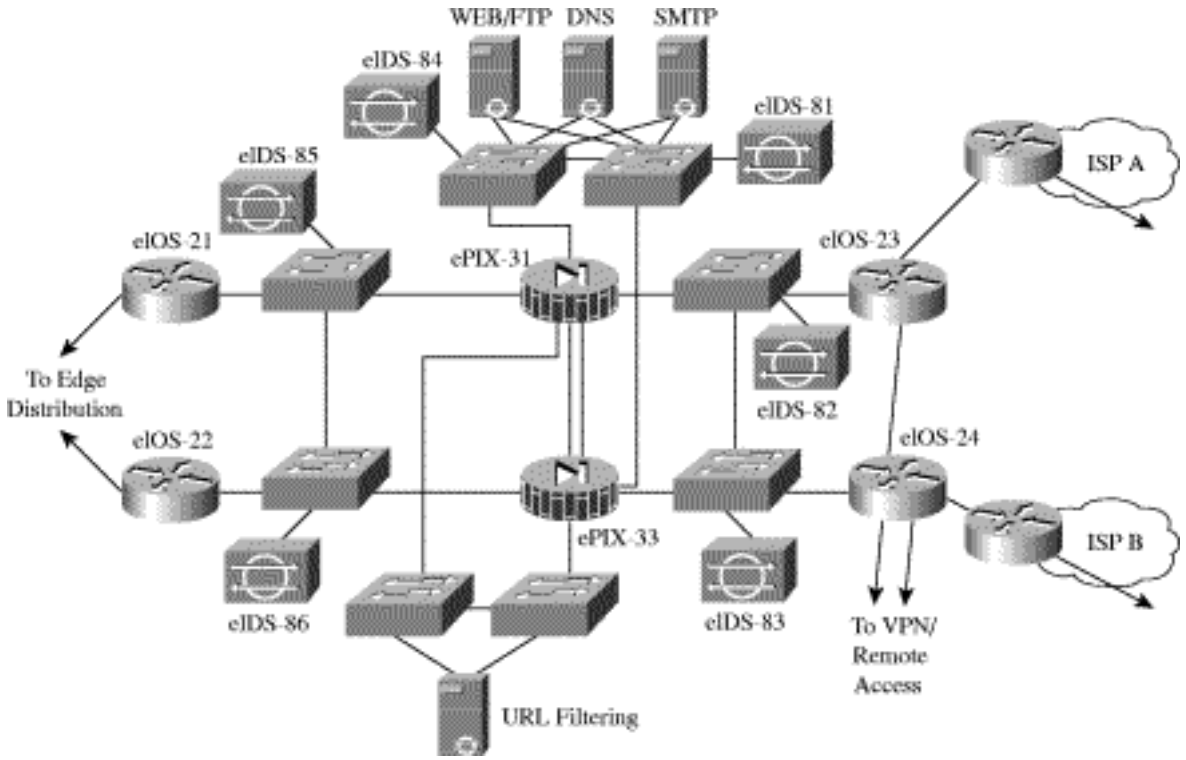
図18 :企業インターネットのトラフィックフロー



主要デバイス

- SMTP サーバ --- インターネットとインターネットメールサーバの間の中継装置として動作し、コンテンツを検査
- DNSサーバ --- 企業の権威ある外部DNSサーバとしての役割を果たし、インターネットへの内部要求を中継
- FTP/HTTPサーバ --- 組織に関する公開情報を提供
- **ファイアウォール** --- ネットワークレベルのリソース保護、およびトラフィックのステートフルフィルタリングを提供
- **NIDS機器** --- モジュール内における主なネットワークセグメントのレイヤ4～レイヤ7モニタリングを提供
- **URLフィルタリングサーバ** --- 企業からの不正なURL要求をフィルタリングする

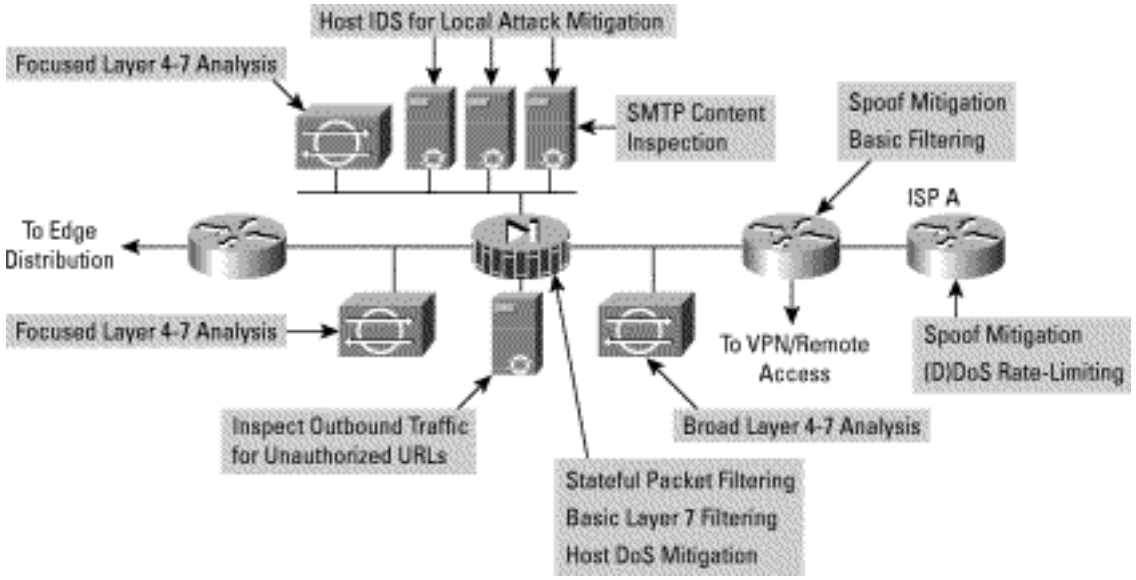
図19: 企業インターネットモジュール（詳細）



脅威の軽減

- **不正アクセス** --- ISP、エッジルータ、および企業ファイアウォールでのフィルタリングによって軽減
- **アプリケーションレイヤ攻撃** --- ホストレベルおよびネットワークレベルでのIDSによって軽減
- **ウイルスとトロイの木馬** --- 電子メールコンテンツフィルタリングとホストIDSによって軽減
- **パスワード攻撃** --- ブルートフォースに使用されるサービスの制限、OS、およびIDSによって脅威を検知
- **サービス拒否（DoS）** --- ISPエッジにおけるCAR、およびファイアウォールにおけるTCPセットアップ制御
- **IPスプーフィング** --- ISPエッジおよびエンタープライズエッジルータにおけるRFC 2827および1918フィルタリング
- **パケットスニファ** --- スイッチ型インフラストラクチャとホストIDSによって脅威を制限
- **ネットワーク偵察** --- IDSによって偵察を検知し、プロトコルフィルタリングによって効果を制限
- **信用詐欺** --- 制約のある信頼モデルとプライベートVLANにより、信頼を利用した攻撃を制限
- **ポート転送** --- 制約のあるフィルタリングとホストIDSによって攻撃を制限

図20: 攻撃の軽減における企業インターネットモジュールの役割



設計ガイドライン

このモジュールの中心は回復力のある1組のファイアウォールであり、これによってインターネットパブリックサービスと内部ユーザーが保護されます。ステートフルな検査によってすべての方向のトラフィックを調査し、公正なトラフィックだけがファイアウォールを通過できるようにします。このモジュールに組み込まれるレイヤ2とレイヤ3の回復力、およびファイアウォールのステートフルなフェールオーバ機能を除いて、すべての設計はセキュリティと攻撃の軽減を中心に考慮されています。

ISPのカスタマエッジルータで開始し、ISPからの出力点において、(D)DoS攻撃を軽減するために、あらかじめ指定したしきい値を超える重要でないトラフィックをレート制限します。また、ISPルータの出力でも、RFC 1918およびRFC 2827フィルタリングにより、ローカルネットワークやプライベートアドレスの範囲で送信元アドレススプーフィングを軽減します。

エンタープライズネットワークにおける最初のルータの入力点では、基本的なフィルタリングによって期待される(アドレスとIPサービス)トラフィックに制限するため、最も基本的な攻撃に対して大まかなフィルタリングが行われます。ここでは、ISPのフィルタリングの確認として、RFC 1918および2827フィルタリングも提供されます。さらに、攻撃によって大きなセキュリティの脅威にさらされるため、インターネット上の標準タイプのトラフィックでは通常見られない断片化されたパケットの大部分をドロップするように、ルータが構成されています。このフィルタリングによって公正なトラフィックも失われますが、こうしたトラフィックを許可するリスクに比べれば安心です。最後に、VPNおよびリモートアクセスモジュール宛てのIPSecトラフィックはすべて適切にルーティングされます。VPNモジュールに接続したインターフェイスでのフィルタリングは、IPSecトラフィックだけ、しかも権限のあるピアに送受信する場合だけ通過させるように構成されています。リモートアクセスVPNでは、入ってくるシステムのIPアドレスが通常は分からないため、リモートユーザーが通信するヘッドエンドピアだけにフィルタリングを特定することができます。

ファイアウォールのパブリック側にあるNIDS機器は、レイヤ4からレイヤ7の分析および既知のシグニチャとの比較に基づいて、攻撃がないかを監視します。ISPや企業のエッジルータは特定のアドレス範囲およびポートをフィルタリングするため、NIDS機器はより複雑な攻撃に照準を定めることができます。ただし、ここで示されるアラームは実際の違法行為ではなく試みを表すに過ぎないため、このNIDSでは、ファイアウォールの内側にある機器より低いレベルにアラームを設定する必要があります。

ファイアウォールは、ファイアウォールを介して開始されたセッションに対して、接続状況の制御と詳細なフィルタリングを行います。公的にアドレス指定可能なサーバは、ファイアウォール上で半オープン接続制限を使用すれば、TCP SYNフラッドを一部防御することができます。フィルタリングの面からは、パブリックサービスセグメント上のトラフィックを関連するアドレスおよびポートに制限するほかに、反対方向でのフィルタリングも行われます。攻撃によってパブリックサーバの1つが(ファイアウォール、ホストベースのIDS、およびネットワークベースのIDSを巧みに回避して)被害を受けた場合は、そのサーバがさらにネットワークを攻撃できないようにする必要があります。この種の攻撃を軽減するため、特定のフィルタリングによって、パブリックサーバがほかの場所に不正な要求を発せられないようにします。たとえば、Webサーバは、Webサーバ自身の要求を発することはできず、単にクライアントからの要求に応答できるようにフィルタリングされる必要があります。これにより、ハッカーが最初の攻撃の後に被害を与えた箱に追加のユーティリティをダウンロードすることや、主な攻撃の間にハッカーによって不要なセッションが発生する

ことも防止されます。Webサーバからファイアウォールを介してハッカーのマシンへxtermを生成する攻撃が、こうした攻撃の例です。さらに、プライベートVLANにより、被害を受けたパブリックサーバが同じセグメント上のほかのサーバを攻撃することも防止されます。このトラフィックはファイアウォールでさえも検知することができないため、プライベートVLANは極めて重要です。

コンテンツ検査セグメント上のトラフィックは、ファイアウォールからURLフィルタリングデバイスへのURLフィルタリング要求に制限されます。さらに、認証された要求は、データベース更新のために企業のURLフィルタリングデバイスからマスタサーバへと送信されます。URLフィルタリングデバイスは、送信トラフィックに不正なWWW要求がないかを検査し、ファイアウォールと直接通信して、ファイアウォールからURL検査エンジンに送信されたURL要求を承認または拒否します。この決定は、サードパーティのサービスによって提供されるWWWのクラス分け情報を使用して、企業が管理するポリシーに基づいて行われます。標準のアクセスフィルタリングよりURL検査を選んだのは、不正なWebサイトのIPアドレスが頻繁に変更され、こうしたフィルタが非常に大規模になる可能性があるためです。このサーバ上におけるホストベースのIDSソフトウェアは、なんとかしてファイアウォールをかいくぐろうとする考えられる攻撃から防御します。

パブリックサービスセグメントには、ファイアウォールの構成で許可されているポート上の攻撃を検知するために、NIDS機器が含まれています。こうした攻撃は、ほとんどの場合、特定のサービスに対するアプリケーションレイヤ攻撃か、保護されたサービスに対するパスワード攻撃です。ここで一致したシグニチャはファイアウォールの通過に成功しているため、このNIDSは、ファイアウォールの外側にあるNIDSより制約の多いスタンスで設定する必要があります。それぞれのサーバにはホスト侵入検知ソフトウェアが実装され、一般的なサーバアプリケーション（HTTP、FTP、SMTPなど）のアクティビティを監視するほか、異常なアクティビティがないかをOSレベルで監視します。DNSホストは、目的のコマンドだけに応答し、ハッカーのネットワーク偵察を支援することにもなりかねない不要な応答をなくすようにロックダウンする必要があります。このため、内部のDNSサーバ以外の場所からのゾーン転送を防止する必要もあります。SMTPサーバは、メール内容検査サービスによって、通常メールシステムを介して侵入する、内部のネットワークへのウイルスおよびトロイの木馬攻撃を軽減します。ファイアウォール自身は、レイヤ7でSMTPメッセージをフィルタリングして、必要なコマンドだけをメールサーバに送信します。

ファイアウォールの内側のインターフェイスにあるNIDS機器は、最終的な攻撃の分析を行います。このセグメントでは、ごくわずかな攻撃だけが検知される必要があります。開始された要求への応答、およびパブリックサービスセグメントからの選ばれた少数ポートだけが入ることができるためです。また、このセグメントでは高度な攻撃だけが検知される必要があります。高度な攻撃は、通常、パブリックサービスセグメント上のシステムが被害を受け、ハッカーがこの足場を利用して内部ネットワークを攻撃しようとしていることを意味するためです。たとえば、パブリックSMTPサーバが被害を受けた場合、ハッカーが、2つのホスト間でのメール転送を可能にするTCPポート25の内部メールサーバを攻撃しようとすることがあります。このセグメントで攻撃が見つかった場合は、すでに被害を受けている可能性があるため、ほかのセグメントで見つかった場合より厳重に攻撃に対処する必要があります。たとえば、TCPリセットを使用して前述のSMTP攻撃の裏をかくといった対処法を真剣に検討する必要があります。

代替案

このモジュールにおける代替の設計がいくつかあります。たとえば、攻撃の認識に対する姿勢によって、NIDS機器がファイアウォールの前方には必要ない場合があります。実際、アクセスルータで基本的なフィルタリングを行わない場合、この種の監視はお勧めできません。適切で基本的なフィルタがこの設計に実装されている場合は、ファイアウォールの外側にあるIDSによって重要なアラーム情報が提供されますが、そうでない場合はファイアウォールによってドロップされます。このセグメントではたくさんのアラームが生成される可能性があるため、ここで生成されるアラームは、ファイアウォールの後方で生成されるアラームより重大度が低いことが必要です。また、ほかのセグメントからの公正なアラームにきちんと注意が向けられるように、アラームをこのセグメントから個別の管理ステーションにロギングすることを検討してください。ファイアウォールの外側のNIDSによって視認性が提供される場合は、組織が受けている攻撃の種類の評価がより見やすくなります。さらに、ISPや企業のエッジフィルタの効果も評価することができます。

提案した設計以外に考えられる代替案は、ファイアウォールとエッジディストリビューションモジュールの間にあるルータを除去することです。この場合、ルータの機能はエッジディストリビューションモジュールに統合することができますが、モジュール間における機能的な切り離しは失われます。これは、エッジディストリビューションスイッチが、正しいルーティングを保証するために企業インターネットモジュールのトポロジ全体を認識することが必要になるためです。さらに、これによって、このアーキテクチャをモジュラ方式で配置できることも制限されます。たとえば、企業の現在のコアがレイヤ2である場合は、企業インターネットモジュールで提供されるルーティングが必要になります。

近い将来のアーキテクチャの目標

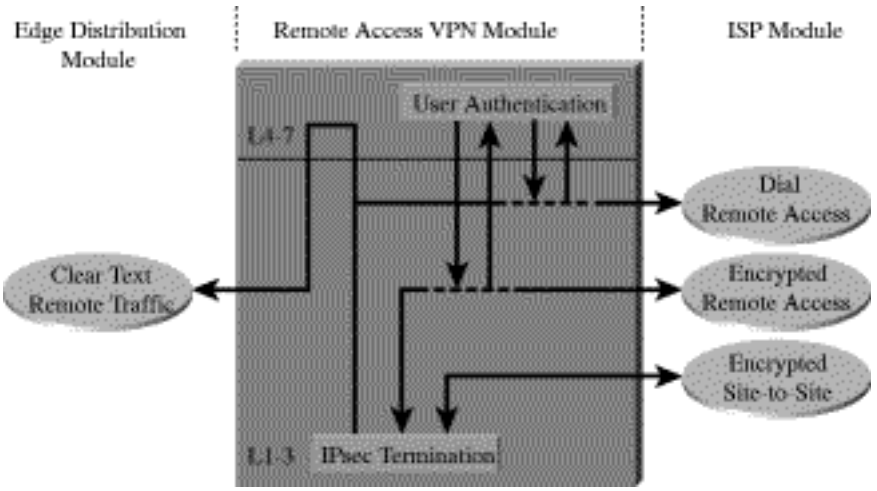
ほかのコンテンツ検査デバイスと直接通信可能なシスコのファイアウォールテクノロジ（たとえば、ネットワークベースのウイルススキャン）の開発が、必要に迫られています。現在は、URLフィルタリングだけが、シスコのファイアウォールテクノロジに直接統合されるコンテンツフィ

ルタリング機能としてサポートされています。統合されない製品は、適切に拡張されないプロキシモードで操作するユーザーが使用しています。

VPN およびリモートアクセスモジュール

このモジュールの主な目的は、名前が示すとおり、リモートユーザーからのVPNトラフィックを終端させる、リモートサイトからのVPNトラフィックを終端させるためのハブを提供する、従来のダイヤルインユーザーを終端させる、という3つに分かれています。エッジディストリビューションに転送されるトラフィックはすべて、ファイアウォールの通過を許可される前に何らかの方法で認証されたリモートの企業ユーザーからのものです。

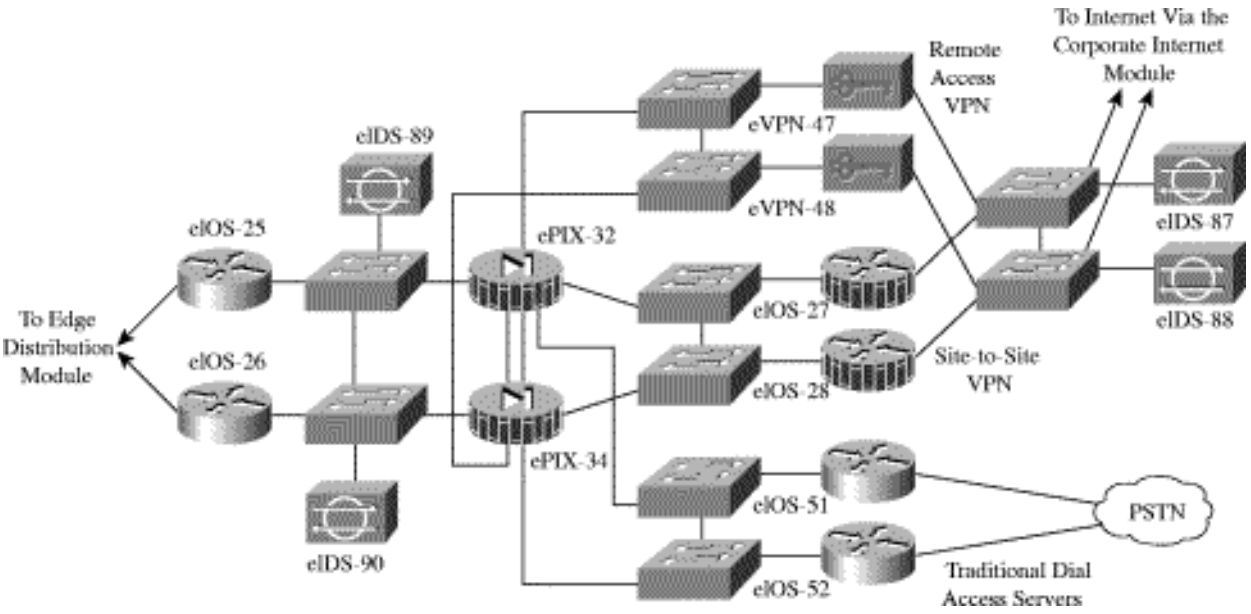
図21:リモートアクセスVPNモジュールのトラフィックフロー



主要デバイス

- **VPNコンセントレータ** --- XAUTH(Extended Authentication)を使用して個々のリモートユーザーを認証し、IPSecトンネルを終端
- **VPNルータ** --- 信頼できるリモートサイトを認証し、GRE/IPSecトンネルを使用して接続
- **ダイヤルインサーバ** --- TACACS+を使用して個々のリモートユーザーを認証し、アナログ接続を終端
- **ファイアウォール** --- 3通りのリモートアクセスに差別化したセキュリティを提供
- **NIDS機器** --- モジュール内における主なネットワークセグメントのレイヤ4～レイヤ7モニタリングを提供

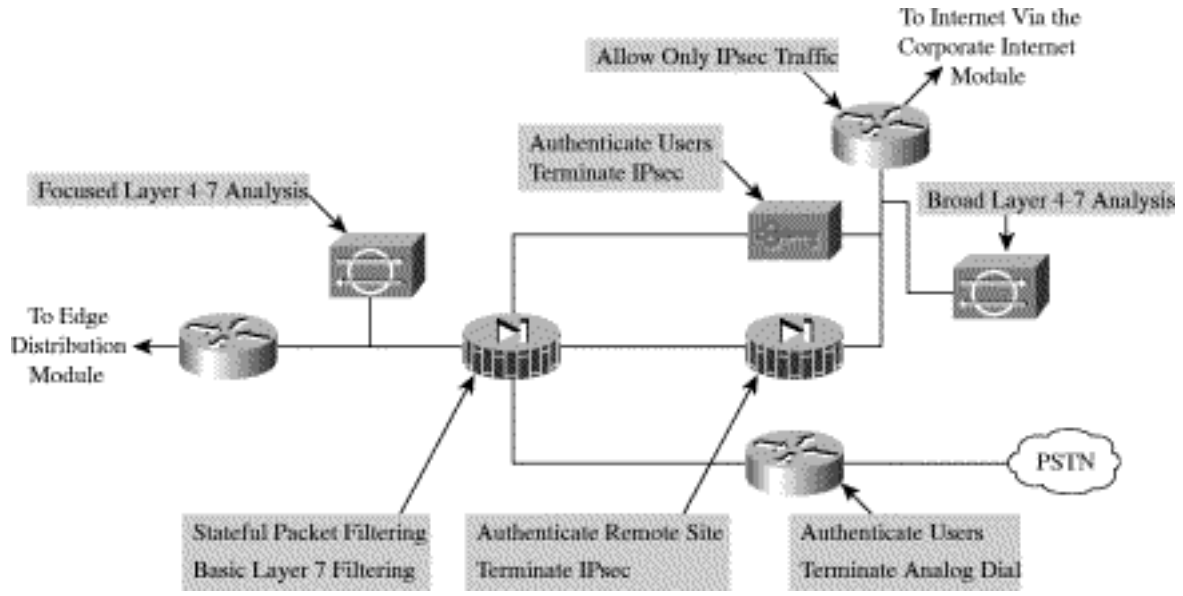
図22:リモートアクセスVPNモジュール(詳細)



脅威の軽減

- **ネットワークトポロジディスカバリ** --- インターネットからIKE(Internet Key Exchange)とESP(Encapsulating Security Payload)だけをこのセグメントに許可
- **パスワード攻撃** --- OTP認証により、パスワード攻撃が成功する可能性を低下
- **正アクセス** --- パケットの暗号解読後のファイアウォールサービスにより、不正なポート上のトラフィックを防止
- **Man-in-the-Middle** --- 暗号化されたリモートトラフィックによって軽減
- **パケットスニファ** --- スイッチ型インフラストラクチャにより、スニッフィングの効果を軽減

図23: 攻撃の軽減におけるリモートアクセスVPNモジュールの役割



設計ガイドライン

このモジュールの中心となる要件は、回復力のほかに、3つの個別の外部ユーザーサービスを認証および終端させることです。トラフィックはエンタープライズネットワークの外側にある複数の送信元から送信されてくるため、これら3つのサービスのそれぞれにファイアウォール上で個別のインターフェイスを提供するために決定されました。それぞれのサービスを設計する際の考慮事項について、次に説明します。

リモートアクセスVPN

VPNトラフィックは企業インターネットモジュールのアクセスルータから転送され、VPNサービスの一部である特定のIPアドレスおよびプロトコルへの出力点で、最初のフィルタリングが行われます。今日のリモートアクセスVPNでは、いくつかの異なるトンネリングおよびセキュリティプロトコルを使用することができます。IPSecは最も優れたトンネリングプロトコルですが、多くの組織ではPPTP（Point-to-Point Tunneling Protocol）およびL2TP（Layer 2 Tunneling Protocol）が使用されています。これらは一般大衆向けのデスクトップオペレーティングシステムで固有にサポートされているためです。クライアントが最小限の構成を要求すると同時に高いセキュリティを提供するため、SAFEではIPSecが選択されています。

リモートアクセスVPNトラフィックは、IKE(UDP 500)プロトコルを使用してある特定のパブリックアドレスにアドレス指定されます。正しい認証情報が提供されるまではIKE接続が確立されないため、これによって潜在的なハッカーを妨害することができます。IKEの拡張機能(ドラフトRFC)の一部であるXAUTHにより、リモートユーザーにIPパラメータが割り当てられる前に追加のユーザー認証メカニズムが提供されます。VPNコンセントレータは、管理インターフェイスを介して管理サブネット上のアクセス制御サーバに「接続」されています。強固なパスワードはワンタイムパスワードサーバを介して提供されます。

いったん認証されると、リモートユーザーは、IKEの別の拡張機能であるMODCFGを使用してIPパラメータを受け取ることでアクセス権が提供されます。IPアドレスやネームサーバ(DNSとWINS)の場所以外にも、MODCFGは、リモートユーザーのアクセスを制御するための認証サービスも提供します。たとえば、SAFEでは、ユーザーがスプリットトンネリングをイネーブルにすることができないため、ユーザーは企業接続を介してインターネットにアクセスせざるをえなくなります。IPSecパラメータは、暗号化に対してはトリプルDES、データの完全性に対してはSHA-HMACが使用されています。VPNコンセントレータのハードウェア暗号化モジュールにより、リモートアクセスVPNサービスは、多数のリモートユーザーに展開するための拡張性を備

えることができます。VPNトンネルが終端すると、トラフィックは、VPNユーザーが適切にフィルタリングされるようにファイアウォールを介して送信されます。

このサービスの安全な管理を実現するために、すべてのIPSecおよびセキュリティパラメータが中央サイトからリモートユーザーに送信されます。さらに、すべての管理機能への接続が専用の管理インターフェイス上で行われます。

ダイヤルインアクセスユーザー

従来のダイヤルインユーザーは、モデムが内蔵された2つのアクセスルータのうちの1つに終端します。レイヤ1接続がユーザーとサーバの間で確立されると、3方向CHAPを使用してユーザーを認証します。リモートアクセスVPNサービスと同様に、AAAおよびワンタイムパスワードサーバを使用してパスワードを認証および提供します。認証されたユーザーは、PPPによってIPプールからIPアドレスが提供されます。

サイト間 VPN

サイト間接続に関連するVPNトラフィックは、ESP（Encapsulated Security Payload）を使用してトランスポートモードのIPSecプロトコルによって保護されたGREトンネルで構成されます。リモートアクセスの場合と同様に、企業インターネットモジュールから転送されるトラフィックは、2つのVPNルータにおける特定の送信先アドレス、およびリモートサイトから期待される送信元アドレスに制限することができます。このリンク上では、ESPプロトコル（IP 50）とIKEプロトコルの2つだけが期待されます。

GREを使用して、マルチプロトコル、ルーティングプロトコル、およびマルチキャストトラフィックを搬送するフルサービスのルーテッドリンクが提供されます。ルーティングプロトコル（リモートサイト間ではEIGRP [Enhanced Interior Gateway Routing Protocol] を使用）はリンク障害を検知できるため、リモートサイトが中央のVPNルータのそれぞれに2つのGRE（汎用ルーティングカプセル化）接続を確立する場合、GREトンネルによって、そのリモートサイトに回復メカニズムが提供されます。

リモートアクセスVPNと同様に、3DESとSHA-HMACがIKEおよびIPSecパラメータに使用されることで、パフォーマンスにほとんど影響を及ぼさずに最大のセキュリティを提供します。IPSecハードウェアアクセラレータはVPNルータで使用されます。

その他のモジュール

3つのサービスからのトラフィックは、ファイアウォールによって1つのプライベートインターフェイスに集束されてから、1組のルータを介してエッジディストリビューションモジュールに送信されます。ファイアウォールは、アクセス制御に適切な制約を加えて、それぞれのサービスから適切なトラフィックだけがファイアウォールの内側のインターフェイスに到達できるように構成する必要があります。1組のNIDS機器はこのモジュールのパブリック側に置かれ、VPN終端デバイスをターゲットにしたネットワーク「偵察」アクティビティを検知します。このセグメントでは、IPSec（IKE/ESP）トラフィックだけが監視される必要があります。NIDSシステムはIPSecパケットの内側を監視できないため、このネットワーク上でアラームが発せられた場合は、周辺デバイスに障害または被害があることを示しています。このため、このアラームは高いレベルの重大度に設定される必要があります。2組目のNIDSはファイアウォールの後方に置かれ、その他のモジュールを通過することに成功した攻撃を検知します。このNIDSデバイスには、制約のあるポリシーもあります。このセグメントを通るユーザーはすべてリモートロケーションへ、またはリモートロケーションからである必要があるため、シャニングまたはTCPリセットだけがこれらのユーザーに影響を与えます。

代替案

VPNおよび認証テクノロジでは、ネットワークの要件によってたくさんの代替案があります。参考までに代替案を以下に列挙しますが、詳細についてはこの文書で扱いません。

- スマートカードおよびバイオメトリック（生物測定学を応用した）認証、またはそのいずれか
- L2TPおよびPPTPリモートアクセスVPNトンネル、またはそのいずれか
- 認証局（CA）
- IKEの継続回復力メカニズム
- マルチプロトコルラベルスイッチング（MPLS）VPN

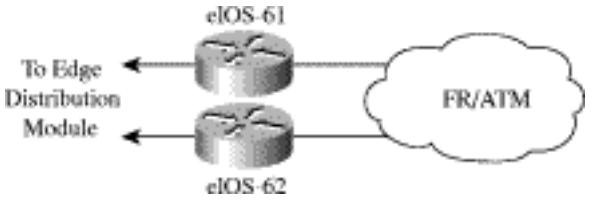
WAN モジュール

潜在的なWAN設計をすべて包括するのではなく、このモジュールは、WAN終端のための回復力とセキュリティを提供します。フレームリレーのカプセル化を使用して、トラフィックがリモートサイトと中央サイトの間でルーティングされます。

主要デバイス

- **IOSルータ** --- ルーティング、アクセス制御、QoSメカニズムを使用

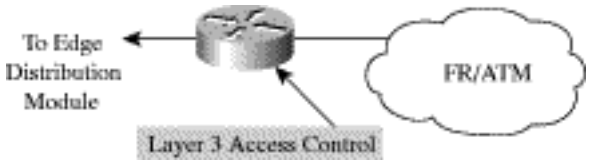
図24：WANモジュール（詳細）



脅威の軽減

- **IPスプーフィング** --- L3フィルタリングによって軽減
- **不正アクセス** --- ルータにおける簡単なアクセス制御により、ブランチからアクセス可能なプロトコルの種類を制限

図25: 攻撃の軽減におけるWANモジュールの役割



設計ガイドライン

回復力を提供するために、サービスプロバイダからルータを経たエッジディストリビューションモジュールまでデュアル接続されています。セキュリティを提供するために、IOSセキュリティ機能が使用されています。インプットアクセスリストを使用して、リモートブランチからの望ましくないトラフィックをすべてブロックします。

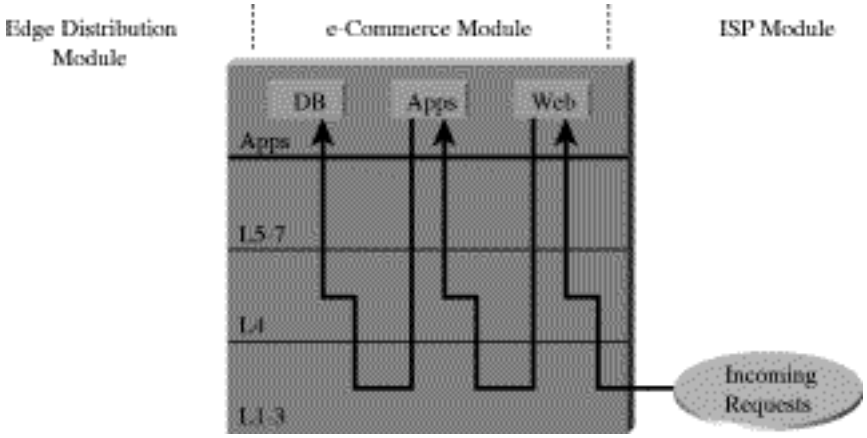
代替案

情報プライバシに対する関心の高い一部の組織では、WANリンク上で機密性の高いトラフィックを暗号化しています。サイト間のVPNと同様に、IPSecを使用すれば、この情報プライバシを実現することができます。

E- コマースモジュール

E-コマースがこのモジュールの主な目的であるため、アクセスとセキュリティとのバランスの加減によく注意する必要があります。E-コマーストランザクションを3つのコンポーネントに分割することで、このアーキテクチャがアクセスを妨げることなくさまざまなレベルのセキュリティを提供することができます。

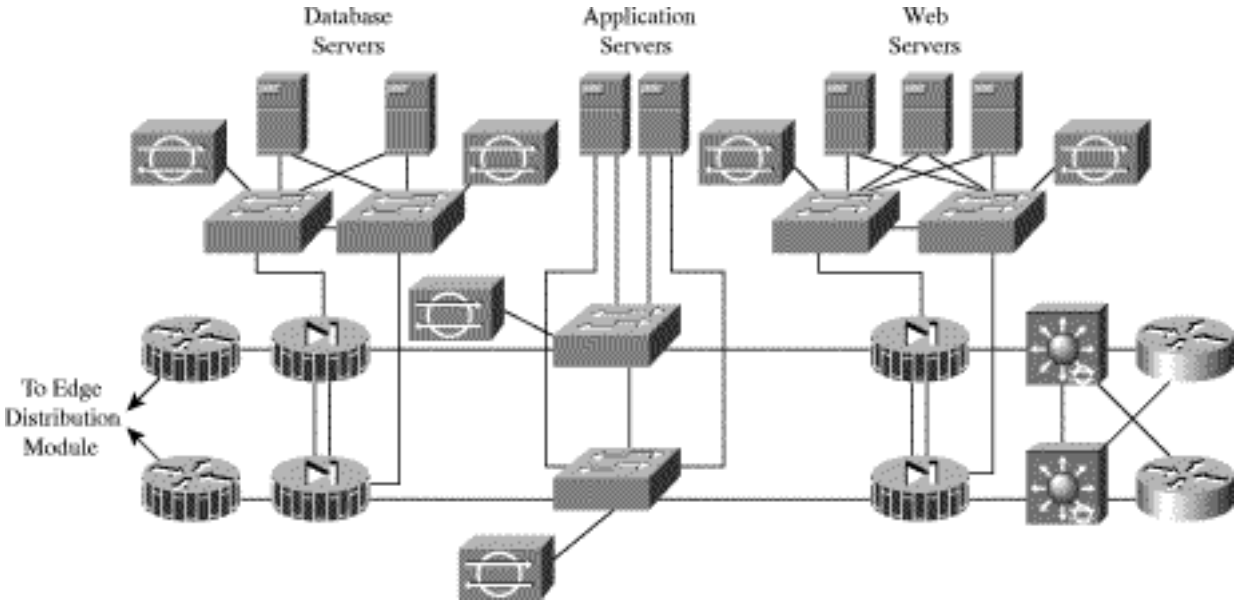
図26: E-コマースのトラフィックフロー



主要デバイス

- **Webサーバ** --- E-コマースストアを移動するためのプライマリユーザーインターフェイスとして動作
- **アプリケーションサーバ** --- Webサーバに必要なさまざまなアプリケーションのプラットフォーム
- **データベースサーバ** --- E-コマースビジネス実装の中心である重要な情報
- **ファイアウォール** --- システム内のさまざまなレベルのセキュリティと信頼との通信を管理
- **NIDS機器** --- モジュール内の主なネットワークセグメントを監視
- **IDSモジュールを装備したレイヤ3スイッチ** --- 統合セキュリティ監視機能を備えた、拡張性のあるE-コマース入力デバイス

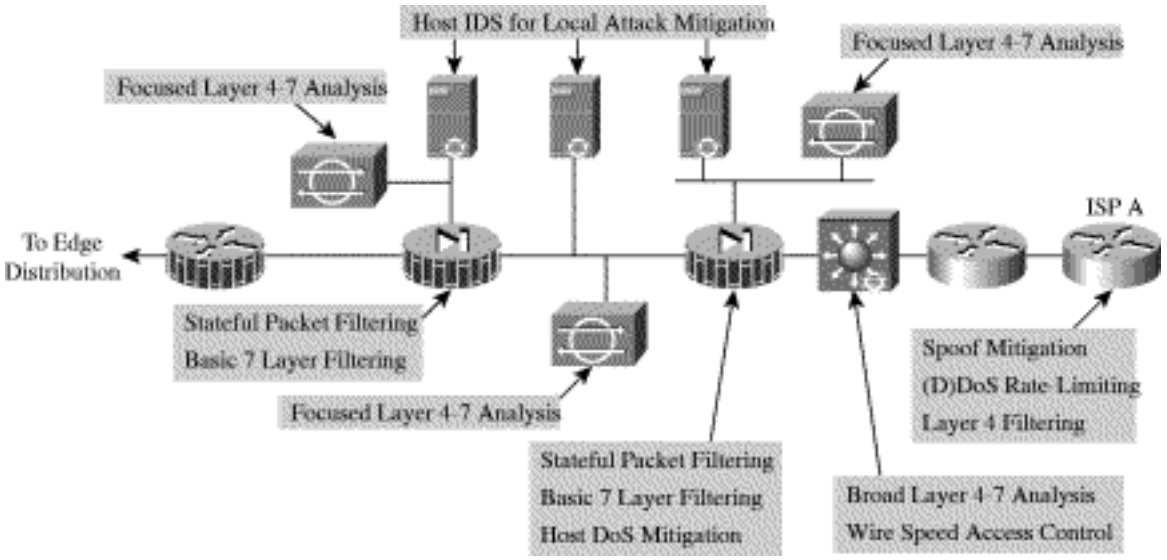
図27: E-コマースモジュール(詳細)



脅威の軽減

- **不正アクセス** --- ステートフルファイアウォールとACLにより、脅威を特定のプロトコルに制限
- **アプリケーションレイヤ攻撃** --- IDSの使用によって攻撃を軽減
- **サービス拒否(DoS)** --- ISPフィルタリングとレート制限により、潜在的な(D)DoSを減少
- **IP スプーフィング** --- RFC 2827および1918により、ローカルでのパケットのスプーフィングを防止し、リモートでのスプーフィングの試みを制限
- **パケットスニファ** --- スイッチ型インフラストラクチャとHIDSにより、スニッフィングの効果を制限
- **ネットワーク偵察** --- ポートを必要なものだけに制限し、ICMPを制限
- **信用詐欺** --- ファイアウォールにより、正しいサービスにおける正しい方向の通信フローだけを確保
- **ポート転送** --- HIDSとファイアウォールフィルタリングにより、脅威をこの攻撃に制限

図28: 攻撃の軽減におけるE-コマースモジュールの役割



設計実装の説明

このモジュールの中心は、Web、アプリケーション、データベースの3レベルの各サーバを保護する、回復力を備えた2組のファイアウォールです。ISPと企業では、追加の保護がISPエッジルータによっていくつか提供されます。通常のE-コマーストランザクションにおけるトラフィックフローシーケンスおよび方向を考えてみれば、この設計が十分に理解できます。

E-コマースカスタマは、ISPネットワークでホスティングされるDNSサーバからIPアドレスを受け取った後、WebサーバへのHTTP接続を開始します。DNSが異なるネットワークでホスティングされているため、E-コマースアプリケーションに必要なプロトコルの量が減ります。1組目のファイアウォールは、このプロトコルがその特定のアドレスに到達できるように構成する必要があります。この接続のリターントラフィックは戻ることができますが、Webサーバによって開始された通信はインターネットへ戻る必要はありません。ハッカーがWebサーバの1つを制御する際の選択肢を制限するために、ファイアウォールはこのパスをブロックする必要があります。

ユーザーがWebサイト間を移動する際に特定のリンクを選択すると、Webサーバがインターフェイスの内側にあるアプリケーションサーバに対して要求を開始します。この接続は、関連するリターントラフィックと同様に、1つ目のファイアウォールによって許可される必要があります。Webサーバの場合と同様に、アプリケーションサーバが、Webサーバやさらには外部のインターネットへの接続を開始するための理由はありません。同様に、ユーザーのセッション全体は、アプリケーションサーバまたはデータベースサーバと直接通信できないHTTPおよびSSL上で実行されます。

ある時点でユーザーが取り引きを行おうとすると、Webサーバがこの取り引きを保護しようとし、SSLプロトコルがインターネットからWebサーバに要求されます。これと同時に、アプリケーションサーバがデータベースサーバに対して照会や情報送信を行うことがあります。このSQLクエリーは、通常、アプリケーションサーバによってデータベースサーバに対して行われるもので、その逆は行われません。このクエリーは、2つ目のファイアウォールを経てデータベースサーバに対して実行されます。使用する特定のアプリケーションによっては、データベースサーバが企業のサーバモジュールに配置されているバックエンドシステムと通信することが必要になります。

要約すると、ファイアウォールは、それぞれ独自のプロトコルを持つ3つの特定の通信パスだけを許可し、この3つのパスに関連する戻りパスパケットでない限り、ほかのすべての通信をブロックする必要があります。

公的にアドレス指定可能なホストであるサーバ自身は(特にWebサーバ)、完全に保護される必要があります。オペレーティングシステムとWebサーバアプリケーションは、最新バージョンによってパッチが適用され、ホスト侵入検知ソフトウェアによって監視される必要があります。こうすることで、ポート転送やルートキットなどといったアプリケーションレイヤの1次および2次攻撃の大部分が軽減されます。1つ目のサーバまたはファイアウォールが被害を受けた場合は、ほかのサーバが同様のセキュリティを持つ必要があります。

ファイアウォールの外側

E-コマースファイアウォールは、ISPではまずカスタマエッジルータによって保護されています。ISPでは、ルータ出力点における企業へのトラフィックを、E-コマースに必要なWebサーバの送信先アドレスだけを持つ少数プロトコルに制限することができます。ルーティングプロトコルの更新（通常はBGP [Border Gateway Protocol]）がエッジルータによって要求されますが、ほかのトラフィックはすべてブロックされる必要があります。ISPでは、(D)DoS攻撃を軽減するために、「SAFEの原理」セクションで述べたレート制限を実装するほか、RFC1918およびRFC 2827によるフィルタリングも実装する必要があります。

企業の構内においては、最初のルータがISPへのインターフェイスとしての機能だけを持ちます。レイヤ3スイッチは、機能をハードウェアプロセッサに肩代わりしているため、すべてのネットワーク処理を行います。まず、特定のユーザーへの経路でどのISPのものが良いかを決めるために、完全BGPルーティング決定に関与します。また、前述したISPフィルタリングと共に妥当性検査フィルタリングを提供することで、セキュリティを二重化します。3つ目に、内蔵型のIDSモニタリングを提供します。インターネットへの接続がIDSラインカードの容量を超えた場合に、IDSラインカード上でインターネットからの受信Web要求だけを監視することが必要になります。これによって一部のhttpアラームのシグニチャ（約10パーセント）を見落とすことになりますが、両方向のストリーム全体を監視して多くのシグニチャが見落とされることに比べれば安全です。ファイアウォールのさまざまなインターフェイスの後方にあるほかのNIDS機器は、セグメントに最初の防御線を突破した攻撃がないかを監視します。たとえば、Webサーバが旧式のものである場合、ハッカーは、当然かいくぐることができると考えて、アプリケーションレイヤ攻撃によってHIDSに被害を与える可能性があります。企業インターネットモジュールと同様に、本当の攻撃の検知がすべて正しい優先度で処理されるように、偽陽性を排除する必要があります。実際、特定のセグメント上には特定の種類のトラフィックしか存在しないため、厳重にNIDSを調整することができます。

アプリケーションの面から、さまざまなレイヤ（web、apps、dbase）間において通信パスが暗号化され、処理を実行し、高度に認証される必要があります。たとえば、appsサーバが何らかの種類のスクリプトされた双方向セッション（SSH、FTP、Telnetなど）上でデータベースからデータを取得する場合、ハッカーがその双方向セッションを利用してアプリケーションレイヤ攻撃を開始する可能性があります。しかし、安全な通信を使用すれば、潜在的な脅威を制限することができます。

さまざまなファイアウォールセグメントをサポートするレイヤ2スイッチによってプライベートVLANの実装が可能になるため、特定のセグメント上における目的のトラフィック通信に対応してほかのトラフィックをすべて排除する信頼モデルが実装されます。たとえば、通常、1つのWebサーバが別のWebサーバと通信するための理由はありません。

モジュール全体の管理は、アーキテクチャのほかのモジュールと同様に、アウトバンドで完全に行われます。

代替案

この配置の主な代替案は、ISPにおいてシステム全体を共通配置することです。設計は同じですが、主に2つの点で異なります。1つ目は、一般にISPへの帯域幅が大きく、LAN接続が使用される点です。お勧めはできませんが、これにより、提案した設計においてエッジルータが不要になることがあります。また、追加の帯域幅により、(D)DoSを軽減するための別の要件が発生します。2つ目は、企業への接続を異なる方法で管理する必要がある点です。代替案には暗号化と専用回線が含まれるため、これらのテクノロジを使用することで、接続の場所やその用途によって追加のセキュリティを検討することが必要になります。

このモジュールは、主な何通りかの方法で設計されます。次に代替案をリストしますが、ここでは詳しい説明を省略します。

- 追加のファイアウォールを使用することが 1 つの代替案です。たとえば、エッジルーティング → ファイアウォール → Web サーバ → ファイアウォール → アプリケーションサーバ → ファイアウォール → データベースサーバ、というように通信します。これにより、各ファイアウォールは1つのプライマリシステムにおける通信だけを制御することができます。
- 負荷分散およびキャッシングテクノロジを、大幅な変更を伴わずにこのアーキテクチャに重ねることができます。この文書では具体的に説明していませんが、将来的に取り扱う予定です。
- 非常に高いセキュリティ要件の場合は、複数の種類のファイアウォールを使用することを検討できます。ただし、これによって異種のシステムでポリシーが2倍になるため、追加の管理オーバーヘッドが発生します。この設計の目的は、1つのファイアウォールにおける脆弱性によってシステム全体のセキュリティが低下するのを避けることです。この種の設計はファイアウォール中心になりがちであり、単一ファイアウォールによる脆弱性のリスクを軽減するためのIDSおよびその他のセキュリティテクノロジが十分に活かされなくなります。

エンタープライズオプション

設計プロセスは、多くの場合、トレードオフの連続となります。この短いサブセクションでは、ネットワーク設計者が予算面での厳しい制約に直面した際に実装することのできる高度なオプションについていくつか重点的に説明します。こうしたトレードオフは、モジュールレベルで行われるものもあれば、コンポーネントレベルで行われるものもあります。

1つ目のオプションは、ディストリビューションモジュールをコアモジュールにまとめることです。これにより、レイヤ3スイッチの数を50パーセント減らすことができます。この場合、コスト削減がトレードオフ（犠牲）となって、ネットワークのコアにおけるパフォーマンス要件、およびすべてのディストリビューションセキュリティフィルタリングを実装するための柔軟性が提供されます。

2つ目のオプションは、VPNおよびリモートアクセスモジュールの機能性を企業インターネットモジュールに統合することです。これらの構造は非常に似ており、モジュールの中心にある1組のファイアウォールがNIDS機器によって囲まれています。コンポーネントのパフォーマンスが両モジュールの統合されたトラフィック要件を満たす場合や、ファイアウォールが異なるサービスに対応するだけの十分なインターフェイスを持つ場合は、機能性を失うことなくこのオプションが可能になります。ただし、機能が単一のデバイスに集束されるにつれ、人為的ミスの可能性が増える点に注意してください。一部の組織では、さらに進んで、E-コマース機能を企業インターネット/VPNモジュールに組み込んでいます。著者は、これを行うにはリスクが伴いますが、E-コマースの必要性が最小でない限りはコスト削減を補ってなお余りあると考えています。一般的なインターネットトラフィックからE-コマーストラフィックを切り離せば、ISPはDDoS攻撃を軽減するためにより規制したフィルタリングおよびレート制限テクノロジを配置できるようになるため、E-コマース帯域幅のより優れた最適化が可能になります。

3つ目のオプションは、NIDS機器の一部を取り除くことです。運用する脅威対応戦略によっては、必要なNIDS機器がもっと少なくて済むことがあります。特定の場所でNIDSの必要性が少なくなる場合があるため、この数は配置されるホストIDSの量によっても左右されます。この内容については、特定のモジュールに関する説明で適宜取り扱います。

明らかに、ネットワーク設計は精密化学ではありません。常に、設計者の前に立ちはだかる特定の要件に基づいて選択する必要があります。設計者は、このアーキテクチャと全く同様に実装するのではなく、この実証済みの実装に裏づけされた知識を応用して、ネットワークセキュリティに関する賢明な選択を行うことをお勧めします。

移行戦略

SAFEは、エンタープライズネットワークにセキュリティを実装するための指針となるものです。エンタープライズネットワークにおけるセキュリティポリシーとして機能したり、すべての既存のネットワークに完全なセキュリティを提供するための包括的な設計として機能したりするものではありません。SAFEは、ネットワーク設計者がエンタープライズネットワークのセキュリティ要件を満たすためにどのように設計および実装するかを検討できるようにするためのテンプレートです。

ネットワークをセキュアなインフラストラクチャに移行する場合、まずセキュリティポリシーを設定する必要があります。セキュリティポリシーにおける基本的な推奨事項については、この文書の最後にある付録B「ネットワークセキュリティ入門」を参照できます。ポリシーを設定したら、ネットワーク設計者は、この文書の冒頭のセクションで述べたセキュリティの原理を考慮して、既存のネットワークインフラストラクチャ上にポリシーを位置付けるための詳細な方法を確認する必要があります。

アーキテクチャは十分な柔軟性を備え、その設計は詳細に検討されているため、SAFEアーキテクチャの要素は大部分のエンタープライズネットワークに適用することができます。たとえば、VPNおよびリモートアクセスモジュールでは、パブリックネットワークからのさまざまなトラフィックフローのそれぞれに対して、ファイアウォール上に1組の個別の終端デバイスと個別のインターフェイスを配置しています。VPNトラフィックは、負荷要件を満たす範囲で、かつ両方の種類のトラフィックにおけるセキュリティポリシーが同じであれば、ある1組のデバイスにまとめることができます。また、別のネットワークでは、従来のダイヤルインおよびリモートアクセスVPNユーザーが直接ネットワーク内に入れることがあります。これは、セキュリティポリシーが、ネットワークへの接続を許可する認証メカニズムにおいて、十分な信頼を第一にしているためです。

SAFEでは、設計者が各ネットワーク機能のセキュリティ要件をそれぞれ個別に取り組むことができます。各モジュールは一般に自己完結型であり、相互に接続したいずれのモジュールも基本的なセキュリティレベルに過ぎないことが想定されています。このため、ネットワーク設計者は、エンタープライズネットワークの安全確保に対して段階的なアプローチをとることができます。ネットワーク全体を設計し直さなくても、ポリシーで規定した最も重要なネットワーク機能の安全確保に取り組むことができます。ただし、管理モジュールは例外であり、最初にSAFEを実装する際、最初のモジュールと同時に管理モジュールを実装する必要があります。ネットワークのその他のモジュールが移行されると、管理モジュールを残りの場所に接続することができます。

SAFEアーキテクチャの最初のバージョンは、一般的なエンタープライズネットワークのセキュリティ実装に対応するという意図で設計されています。このため、さらに詳細な調査、研究、および改善を要する分野が多数残されています。こうした分野の一部を次に示します。

- セキュリティ管理の綿密な分析と実装
- 小規模ネットワーク専用の設計情報
- 自己証明、ディレクトリサービス、AAA　テクノロジ、および認証局の綿密な分析と実装
- VPNヘッドエンドおよびWAN設計の拡張版

付録 A：設定例

この文書で述べる機能性を検証するために、参照用のSAFEが実装されています。この付録では、通常のデバイス構成における総合ガイドラインや、各モジュールにおける特定のデバイスの構成について詳しく述べます。この実験で使用されているデバイスからの構成スナップショットを次に示しますが、これらの構成をそのまま実稼動ネットワークに適用することはお勧めできません。

総合ガイドライン

ここに示す構成は、一部、この文書の冒頭で述べたSAFEの原理に対応しています。

ルータ

SAFE実験のほとんどすべてのルータにおける基本的な構成オプションを次に示します。

```
! turn off unnecessary services
!
no ip domain-lookup
no cdp run
no ip http server
no ip source-route
no service finger
no ip bootp server
no service udp-small-s
no service tcp-small-s
!
!turn on logging and snmp
!
service timestamp log datetime localtime
logging 192.168.253.56
logging 192.168.253.51
snmp-server community Txo~QbW3XM ro 98
!
!set passwords and access restrictions
!
service password-encryption
enable secret %Z<)|z9~zq
no enable password
no access-list 99
access-list 99 permit 192.168.253.0 0.0.0.255
access-list 99 deny any log
no access-list 98
access-list 98 permit host 192.168.253.51
access-list 98 deny any log
line vty 0 4
access-class 99 in
login
password 0 X)[^j+#T98
exec-timeout 2 0
line con 0
login
password 0 X)[^j+#T98
exec-timeout 2 0
line aux 0
```

```
transport input none
password 0 X)[^j+#T98
no exec
exit
banner motd #

        This is a private system operated for and by Cisco VSEC BU.

        Authorization from Cisco VSEC management is required to use this system.

        Use by unauthorized persons is prohibited.

#
!
!Turn on NTP
!
clock timezone PST -8
clock summer-time PST recurring
ntp authenticate
ntp authentication-key 1 md5 -UN&/6[oh6
ntp trusted-key 1
ntp access-group peer 96
ntp server 192.168.254.57 key 1
access-l 96 permit host 192.168.254.57
access-l 96 deny any log
!
!Turn on AAA
!
aaa new-model
aaa authentication login default tacacs+
aaa authentication login no_tacacs line
aaa authorization exec tacacs+
aaa authorization network tacacs+
aaa accounting network start-stop tacacs+
aaa accounting exec start-stop tacacs+
tacacs-server host 192.168.253.54 single
tacacs-server key SJj)j~t]6-
line con 0
login authentication no_tacacs
```

次の構成スナップショットは、ネットワーク内のすべてのOSPFルータに対して、OSPF認証およびフィルタリングパラメータを定義しています。OOBネットワークを保証する配布リストと同様にMD5認証が公示されない点に注意してください。

```
interface Vlan13
  ip address 10.1.13.3 255.255.255.0
  ip ospf authentication message-digest
  ip ospf message-digest-key 1 md5 7 024D105641521F0A7E
  ip ospf priority 3
!
router ospf 1
  area 0 authentication message-digest
  network 10.1.0.0 0.0.255.255 area 0
```

```
  distribute-list 1 out
  distribute-list 1 in
!
access-list 1 deny 192.168.0.0 0.0.255.255
access-list 1 permit any
```

次の構成スナップショットは、ネットワーク全体のすべてのOOBインターフェイスにおけるアクセス制御を定義しています。これは管理対象ホストのIPアドレス間におけるアクセスをブロックするプライベートVLANへの追加である点に留意してください。

```
interface FastEthernet1/0
  ip address 192.168.254.15 255.255.255.0
  ip access-group 101 in
  ip access-group 102 out
  no cdp enable
!
access-list 101 permit icmp any any
access-list 101 permit tcp 192.168.253.0 0.0.0.255 host 192.168.254.15 established
access-list 101 permit udp 192.168.253.0 0.0.0.255 host 192.168.254.15 gt 1023
access-list 101 permit tcp 192.168.253.0 0.0.0.255 host 192.168.254.15 eq telnet
access-list 101 permit udp host 192.168.253.51 host 192.168.254.15 eq snmp
access-list 101 permit udp host 192.168.253.53 host 192.168.254.15 eq tftp
access-list 101 permit udp host 192.168.254.57 host 192.168.254.15 eq ntp
access-list 101 deny ip any any log
access-list 102 deny ip any any log
```

スイッチ

SAFE実験のほとんどすべてのCatalyst OSスイッチにおける基本的なセキュリティ構成を次に示します。IOSスイッチでは、ルータ構成とほとんど同じ構成が使用されます。

```
!
!Turn on NTP
!
set timezone PST -8
set summertime PST
set summertime recurring
set ntp authentication enable
set ntp key 1 trusted md5 -UN&/6[oh6
set ntp server 192.168.254.57 key 1
set ntp client enable
!
! turn off un-needed services
!
set cdp disable
set ip http server disable
!
!turn on logging and snmp
!
set logging server 192.168.253.56
set logging server 192.168.253.51
set logging timestamp enable
set snmp community read-only Txo~QbW3XM
set ip permit enable snmp
set ip permit 192.168.253.51 snmp
```

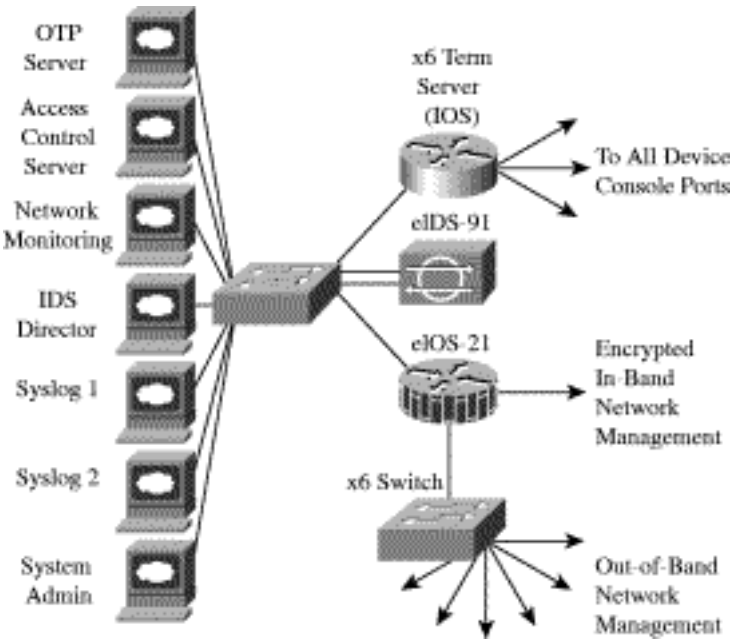
```
!
!Turn on AAA
!
set tacacs server 192.168.253.54 primary
set tacacs key SJj)j~t]6-
set authentication login tacacs enable telnet
set authentication login local disable telnet
set authorization exec enable tacacs+ deny telnet
set accounting exec enable start-stop tacacs+
set accounting connect enable start-stop tacacs+
!
!set passwords and access restrictions
!
set banner motd <c>
        This is a private system operated for and by Cisco VSEC BU.
        Authorization from Cisco VSEC management is required to use this system.
        Use by unauthorized persons is prohibited.
<c>
!console password is set by 'set password'
!enter old password followed by new password
!console password = X)[^j+#T98
!
!enable password is set by 'set enable'
!enter old password followed by new password
!enable password = %Z<)|z9~zq
!
!the following password configuration only works the first time
!
set password
X)[^j+#T98
X)[^j+#T98
set enable
cisco
%Z<)|z9~zq
%Z<)|z9~zq
!
!the above password configuration only works the first time
!
set logout 2
set ip permit enable telnet
set ip permit 192.168.253.0 255.255.255.0 telnet
```

ホスト

ホストは最新の修正版によってパッチが適用され、HIDSも同様に適用されました。研究所で使用されているHIDSアプリケーションは、ClickNetのEnterceptアプリケーションです。この製品の詳細については、http://www.clicknet.comを参照してください。

管理モジュール

図29 :管理モジュール(詳細)



使用した製品

Cisco Catalyst 3500XLレイヤ2スイッチ（すべてスイッチング）
Cisco 3640 IOS ルータFirewallフィーチャセット装備(eIOS-21)
Cisco 2511 IOSルータ(ターミナルサーバ)
Cisco Secure Intrusion Detection System(CSIDS)センサ
RSA SecureID OTP Server
Cisco Secure Access Control Server
CiscoWorks2000
Cisco Secure Policy Manager
netForensics syslog分析ツール
ClickNet Entercept HIDS

EIOS-21

次の構成は、デフォルトのIOSファイアウォールのパラメータを設定しています。

```
ip inspect audit-trail
ip inspect max-incomplete low 150
ip inspect max-incomplete high 250
ip inspect one-minute low 100
ip inspect one-minute high 200
ip inspect udp idle-time 20
ip inspect dns-timeout 3
ip inspect tcp idle-time 1800
ip inspect tcp finwait-time 3
ip inspect tcp synwait-time 15
ip inspect tcp max-incomplete host 40 block-time 0
ip inspect name mgmt_fw tcp timeout 300
ip inspect name mgmt_fw udp
ip inspect name mgmt_fw tftp
ip inspect name mgmt_fw http
ip inspect name mgmt_fw fragment maximum 256 timeout 1
ip audit notify log
ip audit po max-events 100
```

次の構成は、暗号化されたインバンドネットワーク管理を設定しています。

```
crypto isakmp policy 1
  encr 3des
  authentication pre-share
  group 2
crypto isakmp key A%Xr)7,_)address 172.16.224.24
crypto isakmp key A%Xr)7,_)address 172.16.224.23
!
crypto ipsec transform-set vpn_module_mgmt esp-3des esp-sha-hmac
!
crypto map mgmt1 100 ipsec-isakmp
  set peer 172.16.224.24
  set transform-set vpn_module_mgmt
  match address 111
crypto map mgmt1 200 ipsec-isakmp
  set peer 172.16.224.23
  set transform-set vpn_module_mgmt
  match address 110
access-list 110 permit ip 192.168.253.0 0.0.0.255 host 172.16.224.23
access-list 110 permit udp 192.168.254.0 0.0.0.255 host 172.16.224.23
access-list 111 permit ip 192.168.253.0 0.0.0.255 host 172.16.224.24
access-list 111 permit udp 192.168.254.0 0.0.0.255 host 172.16.224.24
```

次の構成は、管理対象ホストネットワークからの受信アクセス制御を定義しています。ポート45000はCSIDS用、ポート5000はClick NetのHIDS用です。

```
access-list 114 permit icmp 192.168.254.0 0.0.0.255 192.168.253.0 0.0.0.255 echo-reply
access-list 114 permit udp 192.168.254.0 0.0.0.255 host 192.168.253.56 eq syslog
access-list 114 permit udp 192.168.254.0 0.0.0.255 host 192.168.253.51 eq syslog
access-list 114 permit udp 192.168.254.0 0.0.0.255 host 192.168.253.50 eq 45000
access-list 114 permit tcp 192.168.254.0 0.0.0.255 host 192.168.253.50 eq 5000
access-list 114 permit udp 192.168.254.0 0.0.0.255 host 192.168.253.53 eq tftp
access-list 114 permit udp 192.168.254.0 0.0.0.255 host 192.168.254.57 eq ntp
access-list 114 permit tcp 192.168.254.0 0.0.0.255 host 192.168.253.54 eq tacacs
access-list 114 permit udp 192.168.254.0 0.0.0.255 host 192.168.253.54 eq 1645
access-list 114 permit udp 192.168.254.0 0.0.0.255 host 192.168.253.52 eq syslog
access-list 114 deny ip any any log
```

次の構成は、管理ホストネットワークからの受信アクセス制御を定義しています。

```
access-list 113 permit icmp 192.168.253.0 0.0.0.255 192.168.254.0 0.0.0.255
access-list 113 permit icmp 192.168.253.0 0.0.0.255 host 192.168.253.57
access-list 113 permit tcp 192.168.253.0 0.0.0.255 host 192.168.253.57 eq telnet
access-list 113 permit tcp 192.168.253.0 0.0.0.255 192.168.254.0 0.0.0.255 eq telnet
access-list 113 permit tcp 192.168.253.0 0.0.0.255 192.168.254.0 0.0.0.255 eq 443
access-list 113 permit tcp 192.168.253.0 0.0.0.255 192.168.254.0 0.0.0.255 eq 22
access-list 113 permit udp host 192.168.253.50 192.168.254.0 0.0.0.255 eq 45000
access-list 113 permit tcp host 192.168.253.50 192.168.254.0 0.0.0.255 eq 5000
access-list 113 permit udp host 192.168.253.51 192.168.254.0 0.0.0.255 eq snmp
access-list 113 permit udp host 192.168.253.53 gt 1023 host 192.168.253.57 gt 1023
access-list 113 permit udp 192.168.253.0 0.0.0.255 host 192.168.254.57 eq ntp
access-list 113 permit tcp host 192.168.253.54 eq tacacs host 192.168.253.57 gt 1023
access-list 113 permit icmp 192.168.253.0 0.0.0.255 host 172.16.224.23
```

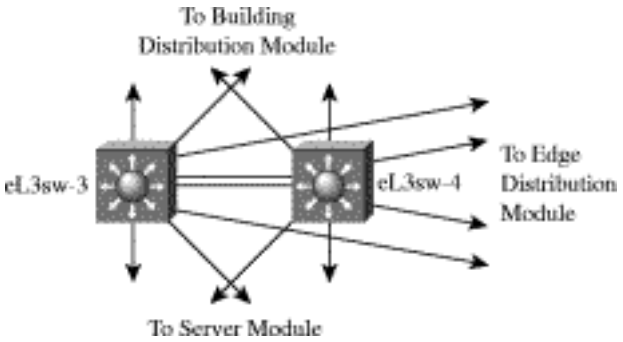
```
access-list 113 permit icmp 192.168.253.0 0.0.0.255 host 172.16.224.24
access-list 113 permit tcp 192.168.253.0 0.0.0.255 host 172.16.224.23 eq telnet
access-list 113 permit tcp 192.168.253.0 0.0.0.255 host 172.16.224.24 eq telnet
access-list 113 permit udp host 192.168.253.51 host 172.16.224.23 eq snmp
access-list 113 permit udp host 192.168.253.51 host 172.16.224.24 eq snmp
access-list 113 deny ip any any log
```

次の構成は、実稼動ネットワークからの受信アクセス制御を定義しています。実稼動ネットワークから管理モジュールに入れる唯一の通信であるため、暗号化されたトラフィックだけがこのアクセスを許可されます。最初の4行は、暗号化されたトラフィックのアクセスを定義しています。暗号化されたトラフィックは、管理モジュールに入るために、再びアクセスリストを通過する必要があります。

```
access-list 112 permit esp host 172.16.224.23 host 10.1.20.57
access-list 112 permit esp host 172.16.224.24 host 10.1.20.57
access-list 112 permit udp host 172.16.224.24 host 10.1.20.57 eq isakmp
access-list 112 permit udp host 172.16.224.23 host 10.1.20.57 eq isakmp
access-list 112 permit udp host 172.16.224.24 host 192.168.253.56 eq syslog
access-list 112 permit udp host 172.16.224.23 host 192.168.253.56 eq syslog
access-list 112 permit udp host 172.16.224.24 host 192.168.253.51 eq syslog
access-list 112 permit udp host 172.16.224.23 host 192.168.253.51 eq syslog
access-list 112 permit udp host 172.16.224.24 host 192.168.253.53 eq tftp
access-list 112 permit udp host 172.16.224.23 host 192.168.253.53 eq tftp
access-list 112 permit udp host 172.16.224.24 host 192.168.253.57 eq ntp
access-list 112 permit udp host 172.16.224.23 host 192.168.253.57 eq ntp
access-list 112 permit tcp host 172.16.224.24 host 192.168.253.54 eq tacacs
access-list 112 permit tcp host 172.16.224.23 host 192.168.253.54 eq tacacs
access-list 112 permit icmp host 172.16.224.24 192.168.253.0 0.0.0.255 echo-reply
access-list 112 permit icmp host 172.16.224.23 192.168.253.0 0.0.0.255 echo-reply
access-list 112 deny ip any any log
```

コアモジュール

図30: コアモジュール（詳細）

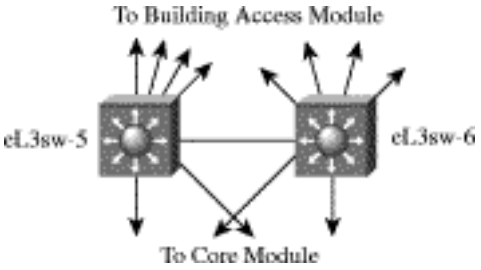


使用した製品

Cisco Catalyst 6500レイヤ3スイッチ

ビルディングディストリビューションモジュール

図31: ビルディングディストリビューションモジュール: 詳細



使用した製品

Cisco Catalyst 6500レイヤ3スイッチ

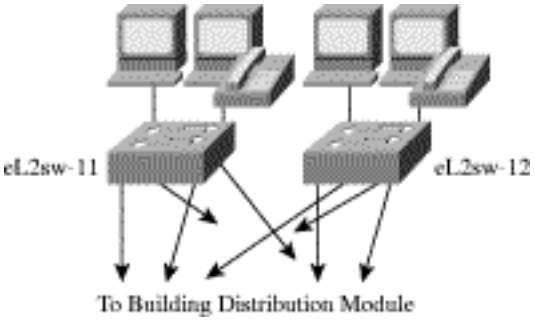
EL3SW-5

次の構成スナップショットは、このモジュールのサブネット間におけるレイヤ3アクセス制御を定義しています。VLAN 5はマーケティングサブネット、VLAN6はR&Dサブネット、VLAN 7はマーケティングのIP電話、VLAN 8はR&DのIP電話をそれぞれ定義しています。

```
interface Vlan5
  ip address 10.1.5.5 255.255.255.0
  ip access-group 105 in
!
interface Vlan6
  ip address 10.1.6.5 255.255.255.0
  ip access-group 106 in
!
interface Vlan7
  ip address 10.1.7.5 255.255.255.0
  ip access-group 107 in
!
interface Vlan8
  ip address 10.1.8.5 255.255.255.0
  ip access-group 108 in
!
access-list 105 deny ip 10.1.5.0 0.0.0.255 10.1.6.0 0.0.0.255
access-list 105 deny ip 10.1.5.0 0.0.0.255 10.1.7.0 0.0.0.255
access-list 105 deny ip 10.1.5.0 0.0.0.255 10.1.8.0 0.0.0.255
access-list 105 deny ip 10.1.5.0 0.0.0.255 10.1.16.0 0.0.0.255
access-list 105 permit ip 10.1.5.0 0.0.0.255 any
access-list 105 deny ip any any log
access-list 106 deny ip 10.1.6.0 0.0.0.255 10.1.5.0 0.0.0.255
access-list 106 deny ip 10.1.6.0 0.0.0.255 10.1.7.0 0.0.0.255
access-list 106 deny ip 10.1.6.0 0.0.0.255 10.1.8.0 0.0.0.255
access-list 106 deny ip 10.1.6.0 0.0.0.255 10.1.15.0 0.0.0.255
access-list 106 deny ip 10.1.6.0 0.0.0.255 10.1.16.0 0.0.0.255
access-list 106 permit ip 10.1.6.0 0.0.0.255 any
access-list 106 deny ip any any log
access-list 107 permit ip 10.1.7.0 0.0.0.255 10.1.8.0 0.0.0.255
access-list 107 permit ip 10.1.7.0 0.0.0.255 10.1.16.0 0.0.0.255
access-list 107 permit ip 10.1.7.0 0.0.0.255 host 10.1.11.50
access-list 107 deny ip any any log
access-list 108 permit ip 10.1.8.0 0.0.0.255 10.1.7.0 0.0.0.255
access-list 108 permit ip 10.1.8.0 0.0.0.255 10.1.16.0 0.0.0.255
access-list 108 permit ip 10.1.8.0 0.0.0.255 host 10.1.11.50
access-list 108 deny ip any any log
```

ビルディングアクセスモジュール

図32: ビルディングアクセスモジュール(詳細)

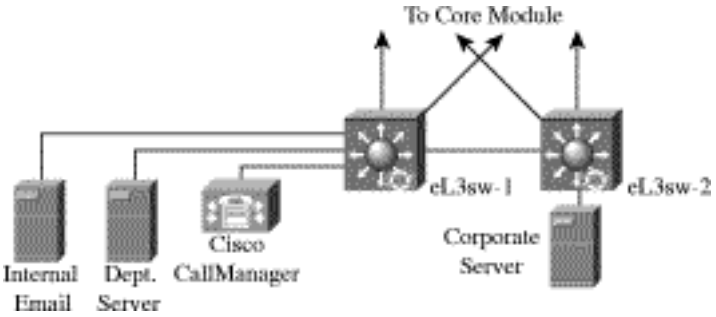


使用した製品

Cisco Catalyst 4003レイヤ2スイッチ
Cisco IP Phone

サーバモジュール

図33: サーバモジュール(詳細)



使用した製品

Cisco Catalyst 6500レイヤ3スイッチ
Cisco Catalyst 6500 Intrusion Detection Blade
Cisco Call Manager
ClickNet Entercept HIDS

EL3SW-1 および 2

次の構成は、同じVLANにおける一部のポートに対して、プライベートVLANのマッピングを設定しています。この構成により、内部の電子メールサーバが企業サーバと通信することを防止します。

```
! CAT OS Config
!
#private vlans
set pvlan 11 437
set pvlan 11 437 3/3-4,3/14
set pvlan mapping 11 437 15/1
!
! MSFC Config
!
interface Vlan11
  ip address 10.1.11.1 255.255.255.0
  ip access-group 111 in
  no ip redirects
```

EL2SW-11 および 12

次の構成スナップショットは、このモジュール内のレイヤ2スイッチにおけるVLAN設定の一部を示しています。不要なポートはディセーブルとされ、ルーティング不可能なVLANに設定されている点に注意してください。また、IP電話との接続で、電話とワークステーションの間のVLAN切り離しにトランキングが使用されている以外は、すべてのポート上でトランキングが無効になっています。

```
set vlan 5 2/5,2/17
set vlan 6 2/6,2/18
set vlan 99 2/34
set vlan 999 2/1-3,2/7-16,2/19-33
set port disable 2/7-33
set trunk 2/1-34 off
set trunk 2/4 on dot1q 1,5-8
```

次の構成は、このモジュール内の一部のインターフェイスにおけるインターフェイスフィルタリングを設定しています。RFC 2827フィルタリングも含まれています。

```
interface Vlan11
 ip address 10.1.11.1 255.255.255.0
 ip access-group 111 in
!
interface Vlan15
 ip address 10.1.15.1 255.255.255.0
 ip access-group 115 in
!
interface Vlan16
 ip address 10.1.16.1 255.255.255.0
 ip access-group 116 in
 ip access-group 126 out
!
access-list 111 permit ip 10.1.11.0 0.0.0.255 any
access-list 111 deny ip any any log
access-list 115 permit ip 10.1.15.0 0.0.0.255 any
access-list 115 deny ip any any log
```

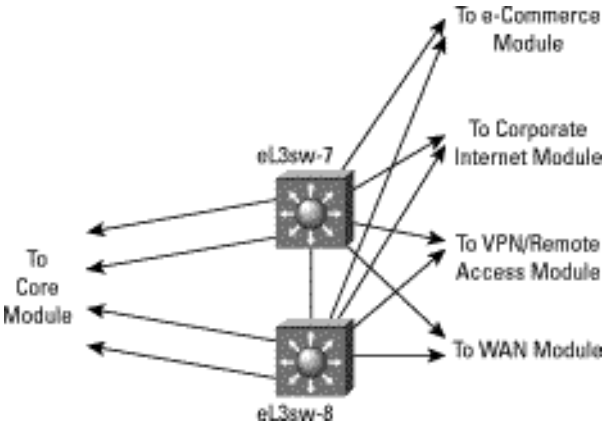
```
access-list 116 permit ip 10.1.16.0 0.0.0.255 10.1.7.0 0.0.0.255
access-list 116 permit ip 10.1.16.0 0.0.0.255 10.1.8.0 0.0.0.255
access-list 116 permit ip 10.1.16.0 0.0.0.255 10.1.11.0 0.0.0.255
access-list 116 deny ip any any log
access-list 126 permit ip 10.1.7.0 0.0.0.255 10.1.16.0 0.0.0.255
access-list 126 permit ip 10.1.8.0 0.0.0.255 10.1.16.0 0.0.0.255
access-list 126 permit ip 10.1.11.0 0.0.0.255 10.1.16.0 0.0.0.255
```

次の構成は、Cat 6000 IDSモジュールに対してキャプチャポートを設定しています。

```
#module 4 ：2-port Intrusion Detection System
set module name 4
set module enable 4
set vlan 1 4/1
set vlan 99 4/2
set port name 4/1 Sniff-4
set port name 4/2 CandC-4
set trunk 4/1 nonegotiate dot1q 1-1005,1025-4094
set security acl capture-ports 4/1
```

エッジディストリビューションモジュール

図34: エッジディストリビューションモジュール: 詳細

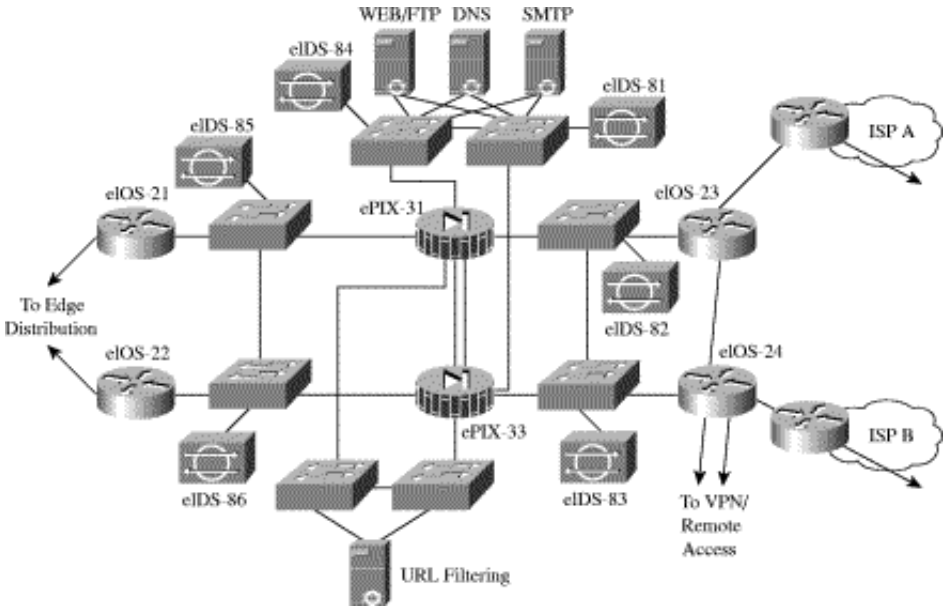


使用した製品

Cisco Catalyst 6500レイヤ3スイッチ

企業インターネットモジュール

図35: 企業インターネットモジュール(詳細)



使用した製品

Cisco Secure PIX Firewall
CSIDS Sensor
Catalyst 3500レイヤ2スイッチ
Cisco 7100 IOS Router
ClickNet Entercept HIDS
Websense URL Filtering Server

EPIX-31 および 33

この構成スナップショットは、PIX Firewall上におけるアクセス制御を詳しく示しています。アクセスリストの名前は、受信ACLが置かれる場所を示しています。「in」は受信、「out」は送信、「pss」はパブリックサービスセグメント（DMZ)、「url」はコンテンツフィルタリングセグメント、「mgmt」はOOBインターフェイスを示しています。

```
access-list out deny ip any 192.168.254.0 255.255.255.0
access-list out deny ip any 192.168.253.0 255.255.255.0
access-list out permit icmp any any echo-reply
access-list out permit tcp any host 172.16.225.52 eq www
access-list out permit tcp any host 172.16.225.52 eq ftp
access-list out permit tcp any host 172.16.225.50 eq smtp
access-list out permit udp any host 172.16.225.51 eq domain
access-list out permit esp host 172.16.224.23 host 172.16.224.57
access-list out permit esp host 172.16.224.24 host 172.16.224.57
access-list out permit udp host 172.16.224.23 host 172.16.224.57 eq isakmp
access-list out permit udp host 172.16.224.24 host 172.16.224.57 eq isakmp
access-list in deny ip any 192.168.254.0 255.255.255.0
access-list in deny ip any 192.168.253.0 255.255.255.0
access-list in permit icmp any any echo
access-list in permit udp host 10.1.11.50 host 172.16.225.51 eq domain
access-list in permit tcp 10.0.0.0 255.0.0.0 host 172.16.225.52 eq www
access-list in permit tcp 10.0.0.0 255.0.0.0 host 10.1.103.50 eq 15871
access-list in permit tcp host 10.1.11.51 host 172.16.225.50 eq smtp
access-list in permit tcp host 10.1.11.51 host 172.16.225.50 eq 20389
access-list in permit tcp 10.0.0.0 255.0.0.0 host 172.16.225.52 eq ftp
access-list in deny ip any 172.16.225.0 255.255.255.0
access-list in permit ip 10.0.0.0 255.0.0.0 any
access-list in permit esp host 10.1.20.57 host 172.16.224.23
access-list in permit esp host 10.1.20.57 host 172.16.224.24
access-list in permit udp host 10.1.20.57 host 172.16.224.23 eq isakmp
access-list in permit udp host 10.1.20.57 host 172.16.224.24 eq isakmp
access-list pss deny ip any 192.168.254.0 255.255.255.0
access-list pss deny ip any 192.168.253.0 255.255.255.0
access-list pss permit tcp host 172.16.225.50 host 10.1.11.51 eq 20025
access-list pss permit tcp host 172.16.225.50 host 10.1.11.51 eq 20389
access-list pss deny ip 172.16.225.0 255.255.255.0 10.0.0.0 255.0.0.0
access-list pss permit tcp host 172.16.225.50 any eq smtp
access-list pss permit udp host 172.16.225.51 any eq domain
access-list url permit udp host 10.1.103.50 host 172.16.225.51 eq domain
access-list url permit ip any any
access-list mgmt permit icmp 192.168.253.0 255.255.255.0 any
```

EIOS-23 および 24

この構成スナップショットは、高可用性のためにホットスタンバイルータプロトコル（HSRP）を使用する多くのルータにおけるHSRPコマンドを詳しく示しています。

```
interface FastEthernet0/0
  ip address 172.16.226.23 255.255.255.0
  standby 2 timers 5 15
  standby 2 priority 110 preempt delay 2
  standby 2 authentication k&>9NG@6
  standby 2 ip 172.16.226.100
  standby 2 track ATM4/0 50
```

次の構成は、暗号化されたインバンドネットワーク管理から管理モジュールへのリンクを設定しています。

```
crypto isakmp policy 1
  encr 3des
  authentication pre-share
  group 2
crypto isakmp key A%Xr)7,_)address 172.16.224.57
!
crypto ipsec transform-set vpn_module_mgmt esp-3des esp-sha-hmac
!
crypto map mgmt1 100 ipsec-isakmp
  set peer 172.16.224.57
  set transform-set vpn_module_mgmt
  match address 103

access-list 103 permit ip host 172.16.224.23 192.168.253.0 0.0.0.255
access-list 103 permit udp host 172.16.224.23 192.168.254.0 0.0.0.255
```

次のACLは、エンタープライズネットワークからの受信を設定しています。

```
access-list 112 permit udp host 172.16.224.57 host 172.16.224.23 eq isakmp
access-list 112 permit esp host 172.16.224.57 host 172.16.224.23
access-list 112 permit tcp 192.168.253.0 0.0.0.255 host 172.16.224.23 established
access-list 112 permit udp 192.168.253.0 0.0.0.255 host 172.16.224.23 gt 1023
access-list 112 permit tcp 192.168.253.0 0.0.0.255 host 172.16.224.23 eq telnet
access-list 112 permit udp host 192.168.253.51 host 172.16.224.23 eq snmp
access-list 112 permit udp host 192.168.254.57 host 172.16.224.23 eq ntp
access-list 112 permit icmp any any
access-list 112 deny ip any host 172.16.224.23 log
access-list 112 deny ip any host 172.16.226.23 log
access-list 112 deny ip any host 172.16.145.23 log
access-list 112 permit ip 172.16.224.0 0.0.0.255 any
access-list 112 permit ip 172.16.225.0 0.0.0.255 any
```

次のACLは、ISPからの受信を設定しています。これらのアドレスは研究所における実稼動アドレスとして使用されているため、RFC 1918フィルタリングは不完全である点に注意してください。実際のネットワークでは、完全なRFC 1918フィルタリングを実装する必要があります。

```
access-list 150 deny ip 10.0.0.0 0.255.255.255 any
access-list 150 deny ip 192.168.0.0 0.0.255.255 any
access-list 150 deny ip 172.16.224.0 0.0.7.255 any
access-list 150 permit ip any 172.16.224.0 0.0.7.255
access-list 150 permit ip any 172.16.145.0 0.0.0.255
access-list 150 permit esp any 172.16.226.0 0.0.0.255 fragments
access-list 150 deny ip any any fragments
access-list 150 deny ip any any log
```

次のフィルタリングは、RA & VPNモジュールに向けて実装されています。IKEとESPだけが許可されている点に注意してください。

```
access-list 160 permit esp any host 172.16.226.27
access-list 160 permit esp any host 172.16.226.28
access-list 160 permit esp any host 172.16.226.48
access-list 160 permit udp any host 172.16.226.27 eq isakmp
access-list 160 permit udp any host 172.16.226.28 eq isakmp
access-list 160 permit udp any host 172.16.226.48 eq isakmp
access-list 160 deny ip any any log
```

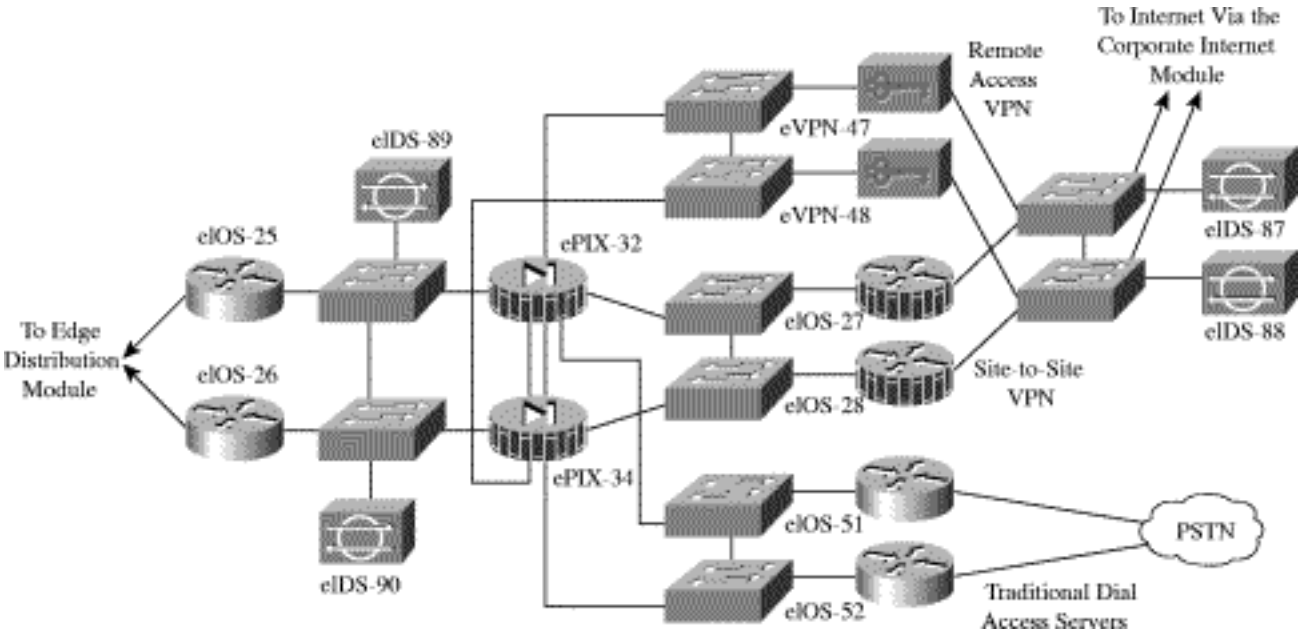
Catalyst 3500XL プライベート VLAN

この構成スナップショットは、パブリックサービスセグメントにおけるプライベートVLANの構成を詳しく示しています。

```
interface FastEthernet0/1
  port protected
!
interface FastEthernet0/2
  port protected
```

VPN およびリモートアクセスモジュール

図36: VPNおよびリモートアクセスモジュール（詳細）



使用した製品

- Cisco Secure PIX Firewall
- CSIDS Sensor
- Catalyst 3500レイヤ2スイッチ
- Cisco 7100 IOSルータ
- Cisco VPN 3060コンセントレータ
- Cisco IOSアクセスサーバ
- ClickNet Entercept HIDS
- Websense URLフィルタリングサーバ

EPIX-32 および 34

この構成スナップショットは、PIX Firewall上におけるアクセス制御を詳しく示しています。アクセスリストの名前は、受信ACLが置かれる場所を示しています。「in」は受信、「out」はサイト間VPN、「dun」はPSTNダイヤルアップ、「ra」はリモートアクセスVPN、「mgmt」はOOBインターフェイスを示しています。

```
access-list in deny ip any 192.168.253.0 255.255.255.0
access-list in deny ip any 192.168.254.0 255.255.255.0
access-list in permit icmp any any
access-list in permit tcp 10.0.0.0 255.0.0.0 10.0.0.0 255.0.0.0 eq smtp
access-list in permit tcp 10.0.0.0 255.0.0.0 10.0.0.0 255.0.0.0 eq pop3
access-list in permit tcp 10.0.0.0 255.0.0.0 10.0.0.0 255.0.0.0 eq www
access-list in permit tcp 10.0.0.0 255.0.0.0 10.0.0.0 255.0.0.0 eq ftp
access-list in permit udp 10.0.0.0 255.0.0.0 10.0.0.0 255.0.0.0 eq netbios-ns
access-list in permit udp 10.0.0.0 255.0.0.0 10.0.0.0 255.0.0.0 eq netbios-dgm
access-list in permit udp 10.0.0.0 255.0.0.0 10.0.0.0 255.0.0.0 eq domain
access-list out deny ip any 192.168.253.0 255.255.255.0
access-list out deny ip any 192.168.254.0 255.255.255.0
access-list out permit icmp any any
access-list out permit tcp 10.0.0.0 255.0.0.0 10.0.0.0 255.0.0.0 eq smtp
access-list out permit tcp 10.0.0.0 255.0.0.0 10.0.0.0 255.0.0.0 eq pop3
access-list out permit tcp 10.0.0.0 255.0.0.0 10.0.0.0 255.0.0.0 eq www
access-list out permit tcp 10.0.0.0 255.0.0.0 10.0.0.0 255.0.0.0 eq ftp
access-list out permit udp 10.0.0.0 255.0.0.0 10.0.0.0 255.0.0.0 eq netbios-ns
access-list out permit udp 10.0.0.0 255.0.0.0 10.0.0.0 255.0.0.0 eq netbios-dgm
access-list out permit udp 10.0.0.0 255.0.0.0 10.0.0.0 255.0.0.0 eq domain
access-list out permit tcp 10.0.0.0 255.0.0.0 172.16.255.0 255.255.255.0 eq www
access-list out permit tcp 10.0.0.0 255.0.0.0 172.16.255.0 255.255.255.0 eq ftp
access-list ra deny ip any 192.168.253.0 255.255.255.0
access-list ra deny ip any 192.168.254.0 255.255.255.0
access-list ra permit icmp any any
access-list ra permit tcp 10.1.198.0 255.255.254.0 10.0.0.0 255.0.0.0 eq smtp
access-list ra permit tcp 10.1.198.0 255.255.254.0 10.0.0.0 255.0.0.0 eq pop3
access-list ra permit tcp 10.1.198.0 255.255.254.0 10.0.0.0 255.0.0.0 eq www
access-list ra permit tcp 10.1.198.0 255.255.254.0 10.0.0.0 255.0.0.0 eq ftp
access-list ra permit udp 10.1.198.0 255.255.254.0 10.0.0.0 255.0.0.0 eq netbios-ns
access-list ra permit udp 10.1.198.0 255.255.254.0 10.0.0.0 255.0.0.0 eq netbios-dgm
access-list ra permit udp 10.1.198.0 255.255.254.0 10.0.0.0 255.0.0.0 eq domain
access-list ra deny ip 10.1.198.0 255.255.254.0 10.0.0.0 255.0.0.0
access-list ra permit tcp 10.1.198.0 255.255.254.0 172.16.225.0 255.255.255.0 eq www
access-list ra permit tcp 10.1.198.0 255.255.254.0 172.16.225.0 255.255.255.0 eq ftp
access-list ra deny ip 10.1.198.0 255.255.254.0 172.16.224.0 255.255.248.0
access-list ra permit ip 10.1.198.0 255.255.254.0 any
access-list dun deny ip any 192.168.253.0 255.255.255.0
access-list dun deny ip any 192.168.254.0 255.255.255.0
access-list dun permit icmp any any
access-list dun permit tcp 10.1.196.0 255.255.254.0 10.0.0.0 255.0.0.0 eq smtp
access-list dun permit tcp 10.1.196.0 255.255.254.0 10.0.0.0 255.0.0.0 eq pop3
access-list dun permit tcp 10.1.196.0 255.255.254.0 10.0.0.0 255.0.0.0 eq www
access-list dun permit tcp 10.1.196.0 255.255.254.0 10.0.0.0 255.0.0.0 eq ftp
access-list dun permit udp 10.1.196.0 255.255.254.0 10.0.0.0 255.0.0.0 eq netbios-ns
access-list dun permit udp 10.1.196.0 255.255.254.0 10.0.0.0 255.0.0.0 eq netbios-dgm
access-list dun permit udp 10.1.196.0 255.255.254.0 10.0.0.0 255.0.0.0 eq domain
access-list dun deny ip 10.1.196.0 255.255.254.0 10.0.0.0 255.0.0.0
access-list dun permit tcp 10.1.196.0 255.255.255.0 172.16.225.0 255.255.255.0 eq www
access-list dun permit tcp 10.1.196.0 255.255.255.0 172.16.225.0 255.255.255.0 eq ftp
access-list dun deny ip 10.1.196.0 255.255.254.0 172.16.224.0 255.255.248.0
access-list dun permit ip 10.1.196.0 255.255.254.0 any
access-list mgmt permit icmp 192.168.253.0 255.255.255.0 any
```

この構成スナップショットは、VPNトラフィックが企業インターネットモジュールを出てインターネットに到達するために必要な静的NAT変換を平文で詳しく示しています。

```
static（inside,ravpn）128.0.0.0 128.0.0.0 netmask 128.0.0.0 0 0
static（inside,ravpn）64.0.0.0 64.0.0.0 netmask 192.0.0.0 0 0
static（inside,ravpn）32.0.0.0 32.0.0.0 netmask 224.0.0.0 0 0
static（inside,ravpn）16.0.0.0 16.0.0.0 netmask 240.0.0.0 0 0
static（inside,ravpn）8.0.0.0 8.0.0.0 netmask 248.0.0.0 0 0
static（inside,ravpn）4.0.0.0 4.0.0.0 netmask 252.0.0.0 0 0
static（inside,ravpn）2.0.0.0 2.0.0.0 netmask 254.0.0.0 0 0
static（inside,ravpn）1.0.0.0 1.0.0.0 netmask 255.0.0.0 0 0
```

EIOS-27 および 28

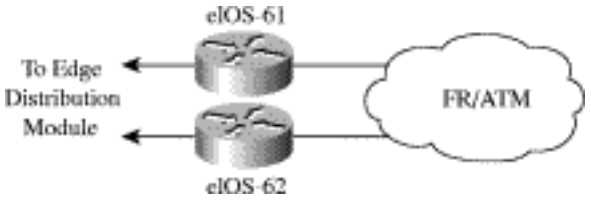
この構成スナップショットは、サイト間VPNにおける暗号化の構成を詳しく示しています。

```
!
! Basic Crypto Information
!
crypto isakmp policy 1
  encr 3des
  authentication pre-share
  group 2
crypto isakmp key 7Q!r$y$+xE address 172.16.132.2
crypto isakmp key 52TH^m&^qu address 172.16.131.2
!
!
crypto ipsec transform-set smbranch esp-3des esp-sha-hmac
  mode transport
!
crypto map secure1 100 ipsec-isakmp
  set peer 172.16.132.2
  set transform-set smbranch
  match address 105
crypto map secure1 300 ipsec-isakmp
  set peer 172.16.131.2
  set transform-set smbranch
  match address 107
!
!
! GRE Tunnel Information
!
interface Tunnel0
  ip address 10.1.249.27 255.255.255.0
  tunnel source 172.16.226.27
  tunnel destination 172.16.132.2
  crypto map secure1
!
interface Tunnel1
  ip address 10.1.247.27 255.255.255.0
  tunnel source 172.16.226.27
  tunnel destination 172.16.131.2
  crypto map secure1
!
!
! EIGRP Routing to keep links up
!
```

```
router eigrp 1
  redistribute static
  passive-interface FastEthernet0/1
  passive-interface FastEthernet4/0
  network 10.0.0.0
  distribute-list 2 out
  distribute-list 2 in
!
! Crypto ACLs
!
access-list 105 permit gre host 172.16.226.27 host 172.16.132.2
access-list 107 permit gre host 172.16.226.27 host 172.16.131.2
!
! Inbound ACLs from Internet
!
access-list 110 permit udp 172.16.0.0 0.0.255.255 host 172.16.226.27 eq isakmp
access-list 110 permit esp 172.16.0.0 0.0.255.255 host 172.16.226.27
access-list 110 permit gre 172.16.0.0 0.0.255.255 host 172.16.226.27
access-list 110 deny ip any any log
```

WAN モジュール

図37: WANモジュール(詳細)



使用した製品

Cisco 3640 IOSルータ

EIOS-61

次の構成は、WANモジュール内のルータにおけるアクセス制御を詳しく示しています。

```
!
! Inbound from the WAN
!
access-list 110 deny ip any 192.168.253.0 0.0.0.255 log
access-list 110 deny ip any 192.168.254.0 0.0.0.255 log
access-list 110 permit ospf any any
access-list 110 permit ip 10.2.0.0 0.0.255.255 10.1.0.0 0.0.255.255
access-list 110 permit ip 10.2.0.0 0.0.255.255 10.3.0.0 0.0.255.255
access-list 110 permit ip 10.2.0.0 0.0.255.255 10.4.0.0 0.0.255.255
access-list 110 permit ip 10.2.0.0 0.0.255.255 172.16.224.0 0.0.7.255
access-list 110 deny ip any any log
!
! Inbound from the Campus
!
access-list 111 deny ip any 192.168.253.0 0.0.0.255 log
access-list 111 deny ip any 192.168.254.0 0.0.0.255 log
access-list 111 permit ospf any any
access-list 111 permit ip 10.1.0.0 0.0.255.255 10.2.0.0 0.0.255.255
access-list 111 permit ip 10.3.0.0 0.0.255.255 10.2.0.0 0.0.255.255
access-list 111 permit ip 10.4.0.0 0.0.255.255 10.2.0.0 0.0.255.255
access-list 111 permit ip 172.16.224.0 0.0.7.255 10.2.0.0 0.0.255.255
access-list 111 deny ip any any log
```

付録 B：ネットワークセキュリティ入門

ネットワークセキュリティの必要性

インターネットによって、仕事、暮らし、遊び、学習の手段は変化しつつあります。こうした変化は、現在経験している手段（E-コマース、情報へのリアルタイムアクセス、E-ラーニング、拡張された通信オプションなど）、およびまだ経験していない手段の両方において始まっています。企業がインターネット上で電話を無料で利用できる日を想像してみてください。あるいは、個人的な例になるかもしれませんが、託児所のWebサイトにログオンして、子供の様子を1日中確認できることを考えてみてください。社会的には、インターネットの潜在能力がまさに開花し始めていますが、あまりに急速なインターネットの成長によって、パーソナルデータ、企業のクリティカルなリソース、政府機密などが前例のない脅威にさらされています。こういったものに対してハッカーは毎日のようにさまざまな攻撃によって脅威をもたらしており、その数は増加の一途をたどっています。次のセクションで概説するこうした攻撃は、種類がますます増えると共に、より簡単に実行できるようになっています。この問題には、主に2つの原因があります。

1つ目は、インターネットが偏在していることです。現在、無数のデバイスがインターネットに接続され、その数はさらに増え続けているため、ハッカーによる脆弱なデバイスへのアクセスは増加する一方です。そればかりか、インターネットの偏在は、ハッカーが世界規模で知識を共有することも可能にしています。「ハック」、「クラック」、または「フリーク」のキーワードで簡単なインターネット検索を行うと、多数のサイトが見つかり、その多くには悪意のあるコードや、そのコードを使用するための手段が掲載されています。

2つ目は、使いやすいオペレーティングシステムと開発環境が普及したことです。この要因により、ハッカーに必要とされる創意工夫や知識は全体的に少なくて済むようになりました。本当に並外れたハッカーは、使いやすいアプリケーションを開発して一般大衆に配布することができます。パブリックドメインで入手可能なこうしたハッカーツールの中には、IPアドレスかホスト名さえわかれば、マウスボタンをクリックするだけで攻撃を実行できるものもあります。

ネットワーク攻撃の分類

ネットワーク攻撃は、ハッカーが侵入しようとするシステムと同じぐらい、その種類が豊富です。攻撃には、精巧で複雑なものもあれば、悪意のないデバイスオペレータによって知らぬ間に行われるものもあります。攻撃の種類を評価するには、TCP/IPプロトコルのいくつかの固有の限界を理解しておくことが重要です。インターネットは、形成された当初、学習や調査を容易にするという明確な目的でさまざまな政府機関や大学を相互にリンクするものでした。最初のインターネット考案者らは、インターネットが今日のように広く普及するなど夢にも思わなかったため、当初のインターネットプロトコル（IP）にはセキュリティが明確に設計に組み込まれていませんでした。こうした理由から、ほとんどのIP実装は本質的に安全とは言えません。時を経て、多数のRFC（Requests for Comment）が提案された今になってようやく、IPを安全に配置するためのツールが提供されるようになりました。特定のIPセキュリティ対策は初めから設計されていないため、IPの実装をネットワークセキュリティの慣行、サービス、および製品で補うことで、インターネットプロトコルに伴うリスクを軽減することが重要となります。以下に、IPネットワークにおける一般的な攻撃の種類、および攻撃を軽減する方法について簡単に説明します。

パケットスニファ

パケットスニファは、ネットワークアダプタカードを無差別モード（ネットワークアダプタカードが物理的なネットワークワイヤ上で受信したすべてのパケットをアプリケーションに送信して処理させるモード）で使用して、特定の衝突ドメインで送信されるすべてのネットワークパケットを捕捉するソフトウェアアプリケーションです。スニファは、今日では、トラブルシューティングやトラフィック分析を支援するためにネットワーク内で正当に使用されています。しかし、一部のネットワークアプリケーションではデータが平文（telnet、FTP、SMTP、POP3など）で送信されるため、パケットスニファによって、ユーザー名やパスワードなど、重要で時には機密を扱った情報までが提供されてしまいます。

ユーザー名とパスワードを取得する際の重大な問題の1つに、多くの場合、ユーザーがログイン名とパスワードを複数のアプリケーションおよびシステムで再使用することがあります。実際、多くのユーザーが、すべてのアカウントおよびアプリケーションへのアクセスに1つのパスワードを使用しています。アプリケーションがクライアントサーバモードで実行され、かつ認証情報がネットワーク中を平文で送信される場合は、この同じ認証情報を使用してほかの企業または外部のリソースにアクセスできる可能性が高くなります。ハッカーは、複数のアカウントに1つのパスワードを使用するといった人間の性質を心得てそれを利用する（総称してソーシャルエンジニアリング攻撃として知られる攻撃手段）ことで、機密を扱った情報へのアクセスにたびたび成功しています。最悪の事態になると、ハッカーは、システムレベルのユーザーアカウントにアクセスし、そのアカウントを利用して、ネットワークとそのリソースに侵入するための裏口としていつでも使用できる新しいアカウントを作成します。

次に示す方法によって、パケットスニファの脅威を軽減することができます。

- **認証** --- 強固な認証の使用は、パケットスニファから防御するための最初の選択肢です。強固な認証は、容易に侵入できないユーザー認証手段として広く定義することができます。強固な認証の一般的な例は、ワンタイムパスワード（OTP）です。OTPは2ファクタ認証の一種であり、2ファクタ認証では、何か知っているものと組み合わせたものが使用されます。現金自動預け払い機（ATM）ではこの2ファクタ認証が使用され、カスタマは処理するためにATMカードと個人識別番号（PIN）の両方が必要になりま

す。OTPでは、デバイスまたはソフトウェアアプリケーションへの認証にPINとトークンカードが必要です。トークンカードは、一見してランダムな新しいパスワードを指定の間隔(通常は60秒)で生成するハードウェアまたはソフトウェアデバイスです。ユーザーは、そのランダムなパスワードとPINを組み合わせて、一度限りの認証に使用される一意のパスワードを作成します。ハッカーがパケットスニファを使用してパスワードを入手しても、そのパスワードはすでに失効しているため、この情報は役に立ちません。ただし、この軽減手段が効果を上げるのは、パスワードを盗むことを目的としたスニファが実装された場合だけであり、機密を扱った情報(メールのメッセージなど)を知るために配置されるスニファに対しては効果がありません。

- **スイッチ型インフラストラクチャ** --- 現在の環境でパケットスニファの使用に反撃するための別の方法は、スイッチ型インフラストラクチャを配置することです。たとえば、組織全体にスイッチ型イーサネットを配置すると、ハッカーは自身が接続する特定のポートを流れるトラフィックにしかアクセスできません。スイッチ型インフラストラクチャは、パケットスニファの脅威を明らかになくすことはできませんが、その効果を大幅に減らすことができます。
- **アンチスニファツール** --- スニファ対策に使用される3つ目の方法は、ネットワーク上のスニファの使用を検知するように設計されたソフトウェアとハードウェアを使用することです。これらのソフトウェアおよびハードウェアは、脅威を完全になくすとは限りませんが、多くのネットワークセキュリティツールと同様に、システム全体において重要な要素となります。このいわゆる「アンチスニファ」は、ホストの応答時間における変化を検知して、ホストが必要以上に多くのトラフィックを処理しているかどうかを判断します。こうしたネットワークセキュリティソフトウェアツールの1つに、LOpht Heavy Industriesから提供されるAntiSniffと呼ばれる製品があります。詳細については、次のURLを参照してください。

  http://www.l0pht.com/antisniff/

- **暗号技術** --- パケットスニファに対処するために最も効果的なこの方法は、パケットスニファを防御または検知するのではなく不適切とします。通信チャネルが暗号上安全である場合、パケットスニファが検知するデータは暗号文(一見してランダムなビット文字列)だけであり、元のメッセージではありません。シスコでは、IP Security(IPSec)に基づいたネットワークレベルの暗号技術を実装しています。IPSecは、ネットワーキングデバイスがIPを使用してプライベートに通信するための標準的な手段です。ネットワーク管理の暗号プロトコルには、ほかにSSH(Secure Shell)とSSL(Secure Sockets Layer)があります。

IP スプーフィング

IPスプーフィング攻撃は、ネットワークの内部または外部のハッカーが信頼できるコンピュータになりすました場合に発生します。ハッカーがこれを行うには2通りの方法があります。ハッカーは、ネットワークの信頼できるIPアドレスの範囲内にあるIPアドレスか、信頼され、かつネットワーク上の指定のリソースにアクセスする権限のある外部IPアドレスのいずれかを使用します。IPスプーフィング攻撃は、ほかの攻撃の開始ポイントになる場合もあります。典型的な例では、ハッカーの正体を隠すために、スプーフィングした送信元アドレスを使用してDoS攻撃を開始するものがあります。

通常、IPスプーフィング攻撃は、クライアントサーバ間やピアツーピアのネットワーク接続間で受け渡される既存のデータストリームに、悪意のあるデータまたはコマンドを挿入することに限定されています。両方向通信を可能にするには、ハッカーはスプーフィングしたIPアドレスを指すすべてのルーティングテーブルを変更する必要があります。そのほか、単にアプリケーションからの応答の受信を気にかけないことも、ハッカーがとることのあるアプローチの1つです。ハッカーが機密を扱ったファイルをシステムから入手しようとする場合、アプリケーションの応答は重要でないからです。

しかし、ハッカーがスプーフィングしたIPアドレスを指すようにルーティングテーブルをなんとか変更した場合、ハッカーは、スプーフィングしたアドレスにアドレス指定されたネットワークパケットをすべて受信し、信頼できるユーザーと全く同様に応答することができます。

次の方法によってIPスプーフィングの脅威を減らすことができますが、なくすことはできません。

- **アクセス制御** --- IPスプーフィングを防ぐための最も一般的な方法は、アクセス制御を正しく構成することです。IPスプーフィングの効果を減らすには、内部ネットワークにある必要がある送信元アドレスを持った外部ネットワークからのトラフィックをすべて拒否するようにアクセス制御を構成してください。ただし、この方法によってスプーフィング攻撃を防御できるのは、内部アドレスだけが信頼できるアドレスである場合です。外部アドレスに信頼できるアドレスがある場合、この方法は効果がありません。
- **RFC 2827フィルタリング** --- 送信元アドレスが組織固有のIP範囲内にないネットワーク上の送信トラフィックを防ぐことで、ネットワークユーザーがほかのネットワークをスプーフィングできないようにする(と同時に優れた「ネット市民」になる)こともできます。ISPでもこの種のフィルタリングを実装することができ、総称してRFC 2827フィルタリングと呼ばれています。このフィルタリングにより、特定のインターフェイスで期待された送信元アドレスを持たないすべてのトラフィックが拒否されます。たとえば、ISPは、IPアドレス 15.1.1.0/24 への接続を提供する場合、トラフィックをフィルタリングして、アドレス 15.1.1.0/24 から送信されたトラフィックだけが

そのインターフェイスからISPルータに入れるようにすることができます。ただし、すべてのISPでこの種のフィルタリングを実装しない限り、その効果は大幅に小さくなります。また、フィルタリングするデバイスからのトラフィックが多くなればなるほど、細かいレベルでのフィルタリングが困難になります。たとえば、インターネットへのアクセスルータでRFC 2827フィルタリングを実行するには、メジャーネットワーク番号全体(つまり、10.0.0.0/8)がアクセスルータを通過できることが要求されます。このアーキテクチャ内のディストリビューションレイヤでフィルタリングを実行すれば、より限定したフィルタリング(つまり、10.1.5.0/24)を実現することができます。

IPスプーフィングの脅威を軽減するための最も効果的な方法は、パケットスニファの脅威を軽減するための最も効果的な方法と同じで、つまり、その効果をなくすことです。IPスプーフィングが正しく機能するのは、デバイスがIPアドレスに基づいた認証を使用するときだけです。このため、追加の認証方法を使用すると、IPスプーフィング攻撃は不適切になります。暗号認証は追加認証の最良の形態ですが、不可能な場合は、OTPを使用する強固な2ファクタ認証も有効です。

サービス拒否

最もよく知られる攻撃形態であるサービス拒否（DoS）攻撃は、完全に排除することが最も困難な攻撃の1つです。ハッカー集団の間でさえ、DoS攻撃は取るに足らないものとみなされ、実行するための労力をほとんど必要としないために低レベルな攻撃であるとされています。しかし、DoS攻撃は、簡単に実行に移せるにもかかわらず大きな被害を与える可能性を秘めているため、セキュリティ管理者は特に注意することが必要です。DoS攻撃について詳しく知りたい場合は、よく知られる攻撃の一部で使用されている手段を調査すると役に立ちます。これらの攻撃には、次のものがあります。

- TCP SYN Flood
- Ping of Death
- Tribe Flood Network(TFN)とTribe Flood Network 2000(TFN2K)
- Trinco
- Stacheldraht
- Trinity

そのほかにセキュリティのトピックを扱った優れた出典の1つに、CERT（Computer Emergency Response Team）があります。DoS攻撃への対応に関する優れた資料が発行されており、次のURLで参照することができます。

http://www.cert.org/tech_tips/denial_of_service.html

DoS攻撃は、一般にネットワークやネットワーク上の情報へのアクセスを目的としていないため、ほかのほとんどの攻撃と異なります。DoS攻撃の狙いは、サービスを通常通りに使用できなくすることであり、一般にネットワーク上やオペレーティングシステムまたはアプリケーション内の一部のリソース制限を使い果たすことで行われます。

WebサーバやFTPサーバなどの特定のネットワークサーバアプリケーションがターゲットになる場合、この攻撃は目的のサーバでサポートされる使用可能な接続をすべて獲得してオープンな状態に維持することに照準を定めることができ、そのサーバまたはサービスの有効なユーザーを効果的にロックアウトします。DoS攻撃には、TCPやICMP（Internet Control Message Protocol）などの一般的なインターネットプロトコルが使用される可能性もあります。DoS攻撃の大部分は、ソフトウェアバグやセキュリティホールではなく、攻撃対象のシステムのアーキテクチャ全体における弱点につけこむものです。一方、ネットワークのパフォーマンスを脅かすために、望ましくない、また時には役に立たないネットワークパケットでネットワークをフラッディングしたり、ネットワークリソースの状態に関する誤った情報を提供したりする攻撃もあります。この種の攻撃を防止することは、アップストリームネットワークプロバイダとの連携を必要とするため、最も困難です。使用可能な帯域幅を消費する意図のあるトラフィックがそこで阻止されなければ、ネットワークに侵入した時点でそれを拒否してもほとんど効果はありません。使用可能な帯域幅はすでに消費されているからです。この種の攻撃が多くの異なるシステムで同時に発生すると、分散型サービス拒否攻撃(DDoS)と呼ばれることがあります。

DoS攻撃の脅威は、次の3つの方法によって減らすことができます。

- **アンチスプーフ機能** --- ルータとファイアウォールにアンチスプーフ機能を正しく構成することにより、リスクを減らすことができます。この機能として、最小でRFC 2827フィルタリングが使用されます。ハッカーは、自分の正体を隠すことができなければ、なかなか攻撃しません。
- **アンチDoS機能** --- ルータとファイアウォールにアンチDoS機能を正しく構成することにより、攻撃の効果を制限することができます。これらの機能では、任意の時間にシステムをオープンにできる半オープン接続の量が制限されます。
- **トラフィックレート制限** --- 企業は、ISPと共にトラフィックレート制限を実装することができます。この種のフィルタリングは、ネットワークセグメントを通る不要なトラフィックの量を一定のレートに制限します。一般的な例は、診断の目的でしか使用されないため、ネットワーク内に入れるICMPトラフィックの量を制限することです。ICMPベースの(D)DoS攻撃は一般的です。

パスワード攻撃

ハッカーがパスワード攻撃を実行するには、ブルートフォース攻撃、トロイの木馬プログラム、IPスプーフィング、パケットスニファといった方法が使用されます。パケットスニファとIPスプーフィングはユーザーアカウントとパスワードを手に入れることができますが、パスワード攻撃は、通常、ユーザーアカウントとパスワード、または

そのいずれかを識別するために繰り返される試行を指しています。この繰り返される試行は、ブルートフォース攻撃と呼ばれます。

多くの場合、ブルートフォース攻撃は、ネットワーク内で実行されるプログラムを使用して実行され、サーバなどの共有リソースにログインしようと試みます。リソースへのアクセスに成功したハッカーは、そのリソースにアクセスするために被害を与えたアカウントの持ち主であるユーザーと同じ権利を持ちます。被害を受けたアカウントが十分な特権を持っていれば、ハッカーは、ステータスや被害を受けたユーザーアカウントに対するパスワード変更を気にすることなく、将来のアクセスに備えて裏口を作成することができます。

もう1つの問題は、ユーザーが接続するすべてのシステムで同じ（おそらく強固な）パスワードを持つことによって生じます。多くの場合、個人システム、企業システム、およびインターネット上のシステムがこれに含まれます。このようなパスワードのセキュリティは、管理が最も脆弱なホストと同程度でしかないため、そのホストが被害を受けると、ハッカーはホストの全範囲にわたって同じパスワードを試すことができるのです。

まず平文のパスワードを避けることで、最も簡単にパスワード攻撃をなくすことができます。OTPと暗号認証、またはそのいずれかを使用すれば、事実上、パスワード攻撃の脅威をなくすことができます。しかし、残念なことに、すべてのアプリケーション、ホスト、およびデバイスがこれらの認証方法をサポートしているわけではありません。このため、標準パスワードを使用する場合は、推測しづらいパスワードを選ぶことが重要です。パスワードは、8文字以上で、大文字小文字のアルファベット、数字、特殊文字（#%$ など）で構成されます。最も良いパスワードはランダムに作成されたものですが、これは非常に覚えにくいため、多くの場合、ユーザーがパスワードを書き留めることになります。

ユーザーと管理者の両方におけるパスワード保持については、さまざまな進歩があります。今では、ハンドヘルドコンピュータに保存するためにパスワードリストを暗号化するソフトウェアアプリケーションを使用することができます。これにより、ユーザーは、複雑なパスワードを1つだけ覚えておいて、残りのパスワードはアプリケーション内に安全に保存しておくことができます。管理者の観点から、管理下のユーザーパスワードをブルートフォース攻撃する方法がいくつかあります。このような方法の1つに、ハッカー集団が使用するL0phtCrackと呼ばれるツールがあります。L0phtCrackは、Windows NTのパスワードをブルートフォース攻撃して、ユーザーがいつ推測しやすいパスワードを選んだのかを特定することができます。詳細については、次のURLを参照してください。

http://www.l0pht.com/l0phtcrack/

Man-in-the-Middle 攻撃

man-in-the-middle攻撃では、ネットワークを通るネットワークパケットにハッカーがアクセスできることが必要です。このような構成の例としてISPで勤務する人が挙げられ、勤務先のネットワークとそれ以外のネットワークの間で送信されるネットワークパケットのすべてにアクセスすることができます。このような攻撃は、多くの場合、ネットワークパケットスニファや、ルーティグおよびトランスポートプロトコルを使用して実行されます。このような攻撃の用途として、情報の盗用、進行中のセッションのハイジャックによるプライベートネットワークリソースへのアクセス、トラフィック分析によるネットワークとそのユーザーに関する情報収集、サービス拒否、送信データの破壊、およびネットワークセッションへの新しい情報の挿入といったことが考えられます。

Man-in-the-middle攻撃は、暗号化技術を使用することによってのみ効果的に軽減することができます。暗号化されたプライベートセッションの最中に何者かがデータをハイジャックした場合、ハッカーが見ることのできるのはすべて暗号文であり、元のメッセージではありません。ただし、ハッカーが暗号セッションに関する情報（セッションキーなど）を知ることができれば、man-in-the-middle攻撃は可能になります。

アプリケーションレイヤ攻撃

アプリケーションレイヤ攻撃は、いくつかの方法によって実行されます。最も一般的な方法の1つは、sendmail、HTTP、FTPなどのサーバで一般に見られるソフトウェアの周知の弱点につけこむことです。ハッカーは、こうした弱点につけこむことで、通常は特権システムレベルのアプリケーションを実行するアカウントの許可により、コンピュータにアクセスすることができます。このアプリケーションレイヤ攻撃は、管理者がパッチを使用して問題を修正できるように、たいていは広く公表されています。しかし、残念ながら多くのハッカーも同じメーリングリストに加入しているため、（まだ発見していない場合は）この攻撃について同時に知ることになります。

アプリケーションレイヤ攻撃に関する主な問題は、ファイアウォールの通過を許可されているポートがよく使用されることです。たとえば、Webサーバに対して既知の脆弱性につけこむハッカーは、攻撃によくTCPポート80を使用します。Webサーバはページをユーザーに提供しているため、ファイアウォールはそのポート上でのアクセスを許可する必要があります。ファイアウォールの面からは、それは標準のポート80トラフィックに過ぎません。

アプリケーションレイヤ攻撃を完全になくすことはできません。常に新しい脆弱性が発見され、インターネット界に公表されているからです。リスクを減らすための最も効果的な方法は、適切なシステム管理を実践することです。次に、リスクを減らすために使用できる方法をいくつか示します。

- OS およびネットワークログファイルを読み取り、ログ解析アプリケーションによって分析します。

- Bugtraq（http://www.securityfocus.com/）やCERT（http://www.cert.org）など、脆弱性を公開しているメーリングリストに加入します。
- OS　とアプリケーションを、最新のパッチによって常に最新の状態にします。
- 適切なシステム管理のほかに、侵入検知システム（IDS）を使用します。補足する2つのIDSテクノロジがあります。
- ネットワークベースの　IDS（NIDS）は、特定の衝突ドメインを介するすべてのパケットを監視することによって機能します。NIDSは、既知または疑わしい攻撃に一致するパケットまたは一連のパケットを検知すると、アラームにフラグを立てるか、セッションを終了することができます。
- ホストベースの　IDS（HIDS）は、エージェントをホストに挿入して保護することによって機能し、そのホストに対して生成された攻撃だけに対応します。
- IDS　システムは、攻撃のシグニチャを使用することによって機能します。攻撃のシグニチャは、特定の攻撃または攻撃の種類のプロファイルであり、トラフィックが攻撃であると思われる前に満たす必要のある特定の条件を規定しています。物理的には、IDSはアラームシステムやセキュリティカメラに最もよく似ています。IDSシステムでは、特定のシステムで生成される偽陽性アラームの量を主に制限します。IDSがネットワーク内で正しく機能するためには、IDSを調整してこうした誤ったアラームを避けることが重要です。

ネットワーク偵察

ネットワーク偵察とは、公的に使用可能な情報およびアプリケーションを使用してターゲットのネットワークに関する情報を得るという行為全体を指しています。ハッカーが特定のネットワークに侵入しようとする場合、攻撃を開始する前にそのネットワークに関する情報をできるだけ多く知っておく必要があります。これは、DNSクエリー、pingスイープ、ポートスキャンといった形態をとります。DNSクエリーによって、特定のドメインの所有者、そのドメインに割り当てられているアドレスなどの情報を漏らすことができます。DNSクエリーによって漏れたアドレスをpingスイープすることで、特定の環境で稼動中のホストの状態がわかります。このリストが生成されると、ポートスキャンツールによって周知のポートをすべて巡回し、pingスイープによって発見されたホストで実行中のすべてのサービスの完全なリストが提供されます。最後に、ハッカーはアプリケーションの特性がホスト上で実行されていることを調べることができます。これにより、ハッカーはそのサービスに被害を与えようとする際に役立つ特定の情報を得ることができます。

ネットワーク偵察を完全に防ぐことはできません。たとえば、ICMPエコーとエコー応答がエッジルータで無効になっている場合、pingスイープを阻止することはできますが、ネットワーク診断データが犠牲になります。ただし、存在していないかもしれないIPアドレスをスキャンする必要があるため時間は長くかかりますが、完全なpingスイープがなくてもポートスキャンは簡単に実行できます。ネットワークレベルおよびホストレベルでのIDSは、通常、偵察集中攻撃が始まると管理者に知らせることができます。管理者は、これから起こる攻撃に十分に備えるか、偵察プローブを始動したシステムのホスティングであるISPに知らせることができます。

信用詐欺

信用詐欺とは、それ自体は攻撃ではありませんが、個人がネットワーク内における信頼関係を利用した攻撃を指します。典型的な例として、企業からの周辺ネットワーク接続があります。これらのネットワークセグメントは、多くの場合、DNS、SMTP、およびHTTPサーバ上にあります。これらはすべて同じセグメントにあり、1つのシステムが被害を受けると、同じネットワークに接続したほかのシステムを信頼している可能性があるため、別のシステムも被害を受けることがあります。ほかの例は、ファイアウォールの内側にあるシステムと信頼関係を持った、ファイアウォールの外側にあるシステムです。被害を受けた外側のシステムは、その信頼関係を利用して内部ネットワークを攻撃することができます。

信用詐欺に基づいた攻撃は、ネットワーク内の信頼レベルを厳しく制約することによって軽減することができます。ファイアウォールの内側にあるシステムは、外側にあるシステムを全面的に信頼すべきではありません。こうした信頼は特定のプロトコルに限定し、できるだけIPアドレス以外のもので認証される必要があります。

ポート転送

ポート転送攻撃は、信用詐欺攻撃の一種であり、被害を受けたホストを使用して、通常であればドロップされるはずのトラフィックがファイアウォールを通過します。3つのインターフェイスのそれぞれにホストが実装されたファイアウォールを考えてみてください。外側にあるホストはパブリックサービスセグメント（一般にDMZと呼ばれる）上のホストに到達できますが、内側にあるホストには到達できません。パブリックサービスセグメント上にあるホストは、外側と内側の両方のホストに到達することができます。ハッカーがパブリックサービスセグメントのホストに被害を与えることができた場合、ソフトウェアをインストールしてトラフィックを外側のホストから内側のホストへ直接転送できることになります。いずれの通信もファイアウォールで実施される規則に違反しませんが、現在、パブリックサービスホストのポート転送プロセスによって、外側のホストが内側のホストと接続できるようになりました。この種のアクセスを提供できるアプリケーションの例として、netcatがあります。詳細については、次のURLを参照してください。

http://www.avian.org

ポート転送は、主に、適切な信頼モデル（前述のとおり）を使用することによって軽減することができます。システムが攻撃を受けていると想定して、ホストベースのIDSは、このようなユーティリティをホスト上にインストールしているハッカーを検知して防御することができます。

不正アクセス

特定の種類の攻撃ではありませんが、不正アクセス攻撃とは、今日、ネットワーク内で実行される大多数の攻撃を指します。誰かがtelnetログインをブルートフォースするためには、まずシステム上のtelnetプロンプトを取得する必要があります。telnetポートに接続したとたん、「このリソースを使用するには権限が必要です」というメッセージが表示されることがありますが、ハッカーがアクセスの試みを続ければ、その行為は「不正」となります。この種の攻撃は、ネットワークの内部と外部の両方で発生します。

不正アクセス攻撃を軽減するための手段は非常に単純であり、ハッカーが不正なプロトコルを使用してシステムにアクセスできることを減らす、または排除することが必要です。たとえば、Webサービスを外部に提供する必要のあるサーバ上のtelnetポートにハッカーがアクセスすることを防ぎます。ハッカーがそのポートに到達できなければ、攻撃はとても困難になります。ネットワークにおけるファイアウォールの主な機能は、単純な不正アクセス攻撃を防ぐことです。

ウイルスおよびトロイの木馬アプリケーション

エンドユーザーワークステーションにおける主な脆弱性は、ウイルスおよびトロイの木馬攻撃です。ウイルスとは、ほかのプログラムに添付されてユーザーのワークステーション上で特定の望ましくない機能を実行する悪意のあるソフトウェアのことです。ウイルスの例として、command.com（windowsシステムの主要インタープリタ）に付いて特定のファイルを削除し、検出可能なほかのすべてのバージョンのcommand.comに感染させるプログラムがあります。トロイの木馬は、実際は攻撃ツールでありながら、アプリケーション全体が別のものであるかのように記述されているという点でのみ異なります。トロイの木馬の例として、ユーザーのワークステーション上で簡単なゲームを実行するソフトウェアアプリケーションがあります。ユーザーがゲームに夢中になっている間、そのユーザーのアドレス帳にあるユーザー全員にトロイの木馬のコピーがメール送信されます。そして、ほかのユーザーがそのゲームを受け取ってプレーする、というようにしてトロイの木馬が広がっていきます。

この種のアプリケーションは、アンチウイルスソフトウェアを効果的に使用することで、ユーザーレベル、および潜在的にネットワークレベルでくい止めることができます。アンチウイルスソフトウェアは、大部分のウイルスと多くのトロイの木馬アプリケーションを検知し、これらがネットワーク内に広がることを防止することができます。この種の攻撃における最新の開発に関して情報を常に得ることも、攻撃に対するより効果的な対策となります。新しいウイルスまたはトロイの木馬アプリケーションがリリースされるため、企業では、最新のアンチウイルスソフトウェアとアプリケーションのバージョンに関する情報を常に得ることが必要です。

「セキュリティポリシー」とは

セキュリティポリシーは、ネットワークリソースの許容される使用に関するポリシーと同じぐらい単純なものもあれば、数百ページにもわたって接続のすべての要素と関連するポリシーを詳しく規定したものもあります。いくらか範囲が狭まっていますが、RFC 2196でセキュリティポリシーを次のように適切に定義しています。

「セキュリティポリシーとは、企業のテクノロジおよび情報資産へのアクセス権を与えられた者が従う必要のある規則を正式に規定したものである。」

この文書では、セキュリティポリシーの開発について詳しく説明しません。RFC 2196でこのテーマに関する正確な情報を一部入手できるほか、Web上の多くの場所にポリシーおよびガイドラインの例が掲載されています。セキュリティポリシーについて関心がある場合は、次のWebページを参照してください。

- RFC 2196「Site Security Handbook」
  http://www.ietf.org/rfc/rfc2196.txt
- イリノイ州立大学のセキュリティポリシー例
  http://www.aits.uillinois.edu/security/securestandards.html
- 企業セキュリティポリシーの設計と実施
  http://www.knowcisco.com/content/1578700434/ch06.shtml

セキュリティポリシーの必要性

ネットワークセキュリティが進化の過程であることを理解することが重要です。組織を「セキュア」にできる製品は1つもありません。本当のネットワークセキュリティは、製品とサービスの組み合わせに、包括的なセキュリティポリシーと、組織においてトップダウンでそのポリシーに従う義務をすべて兼ね備えることによって実現します。実際、企業資産に対する脅威を軽減するという点では、関連するポリシーを実施しないで包括的なセキュリティ製品を実装するより、専用のセキュリティハードウェアがなくてもセキュリティポリシーを正しく実施することの方が効果的です。

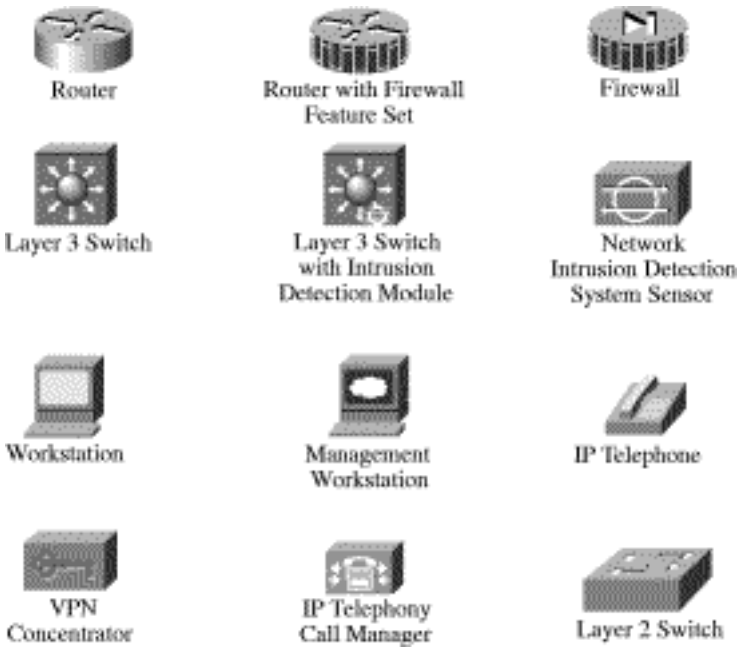
付録 C：アーキテクチャの分類

- **アプリケーションサーバ** --- アプリケーションサービスを直接または間接に企業のエンドユーザーに提供します。サービスには、ワークフロー、一般的なオフィス業務、およびセキュリティアプリケーションが含まれます。
- **ファイアウォール（ステートフル）** --- IPベースプロトコルのステートテーブルを維持するステートフルパケットフィルタリングデバイスです。トラフィックは、定義済みのアクセス制御フィルタに一致する場合、またはステートテーブルにおいてすでに確立されたセッションの一部である場合だけ、ファイアウォールを通ることができます。
- **ホストIDS** --- ホスト侵入検知システムは、個々のホストでアクティビティを監視するソフトウェアアプリケーションです。監視技術には、オペレーティングシステムや

アプリケーションの呼び出しの妥当性検査、およびログファイル、ファイルシステム情報、ネットワーク接続のチェックが含まれます。

- **ネットワークIDS** --- ネットワーク侵入検知システム。通常は非破壊的な方法で使用されるこのデバイスは、LANセグメント上におけるトラフィックをキャプチャし、リアルタイムのトラフィックを既知の攻撃シグニチャと突き合わせます。シグニチャには、アトミック(単一パケットおよび方向)シグニチャから、ステートテーブルとレイヤ7アプリケーショントラッキングが必要なコンポジット(マルチパケット)シグニチャまであります。
- **IOSファイアウォール** --- Cisco IOS(Internetwork Operating System)で固有に動作するステートフルパケットフィルタリングファイアウォール。
- **IOSルータ** --- すべてのパフォーマンス要件に対して多くのルーティングおよびセキュリティサービスを幅広く提供する、柔軟なネットワークデバイス。デバイスの大部分はモジュラ型であり、LANおよびWAN物理インターフェイスがあります。
- **レイヤ2スイッチ** --- 帯域幅およびVLANサービスをイーサネットレベルでネットワークセグメントに提供します。通常、このデバイスは、10/100の各スイッチドポート、ギガビットイーサネットアップリンク、VLANトランキング、およびL2フィルタリング機能を備えています。
- **レイヤ3スイッチ** --- レイヤ2スイッチと同様の高スループット機能を提供しながら、ルーティング、QoS、セキュリティの各機能が追加されます。このスイッチは、多くの場合、特殊機能プロセッサの機能を持ちます。
- **管理サーバ** --- ネットワーク管理サービスをエンタープライズネットワークのオペレータに提供します。サービスには、一般構成管理、ネットワークセキュリティデバイスの監視、およびセキュリティ機能の操作が含まれます。
- **SMTPコンテンツフィルタリングサーバ** --- 通常、外部のSMTPサーバで実行されるアプリケーション。着信メールや発信メールの内容(添付ファイルを含む)を監視して、そのメールがそのまま転送、変更して転送、またはドロップされることを許可されているかを決定します。
- **URLフィルタリングサーバ** --- 通常、スタンドアロン型のサーバで実行されるアプリケーション。ネットワークデバイスから転送されるURL要求を監視し、その要求をインターネットに転送する必要があるかどうかをネットワークデバイスに通知します。これにより、企業はインターネットサイトのどのカテゴリが不正であるかを要求するセキュリティポリシーを実施することができます。
- **VPN終端デバイス** --- サイト間またはリモートアクセスのいずれかのVPN接続におけるIPSecトンネルを終端させます。典型的なWANまたはダイヤルイン接続と同じネットワーク機能性を実現するには、追加のサービスを提供する必要があります。
- **ワークステーションまたはユーザー端末** --- エンドユーザーによって直接使用される、ネットワーク上のすべてのデバイス。PC、IP電話、ワイヤレスデバイスなどがあります。

図の凡例



参考文献

RFC

RFC 2196「Site Security Handbook」--- http://www.ietf.org/rfc/rfc2196.txt
RFC 1918「Address Allocation for Private Internets」--- http://www.ietf.org/rfc/rfc1918.txt
RFC 2827「Network Ingress Filtering：Defeating Denial of Service Attacks which employ IP Source Address Spoofing」--- http://www.ietf.org/rfc/rfc2827.txt

その他の参考文献

「Improving Security on Cisco Routers」--- http://www.cisco.com/warp/public/707/21.html
「VLAN Security Test Report」--- http://www.sans.org/newlook/resources/IDFAQ/vlan.htm
「AntiSniff」--- http://www.l0pht.com/antisniff/
「L0phtCrack」--- http://www.l0pht.com/l0phtcrack/
「Denial of Service Attacks」--- http://www.cert.org/tech_tips/denial_of_service.html
「Computer Emergency Response Team」--- http://www.cert.org
「Security Focus（Bugtraq）」--- http://www.securityfocus.com
「Avian Research（netcat）」--- http://www.avian.org
「University of Illinois Security Policy」--- http://www.aits.uillinois.edu/security/securestandards.html
「Design and Implementation of the Corporate Security Policy」--- http://www.knowcisco.com/content/1578700434/ch06.shtml

パートナー製品の参考文献

ClickNet Entercept Host-Based IDS --- http://www.clicknet.com
RSA SecureID OTP System --- http://www.rsasecurity.com/products/securid/
Content Technologies MIMESweeper Email Filtering System --- http://www.contenttechnologies.com
Websense URL Filtering --- http://www.websense.com/products/integrations/ciscopix.cfm
netForensics Syslog Analysis --- http://www.netforensics.com/

謝辞

この場を借りて、SAFE アーキテクチャおよびこの文書の執筆に貢献していただいたすべての方々に感謝いたします。まさに、本社および現場の全シスコ社員による貴重なアドバイスと再調査のフィードバックなくしては、このアーキテクチャを無事に完成させることは不可能だったことでしょう。さらに、たくさんの方々が、このアーキテクチャを研究所に実装して検証することに貢献してくださいました。このグループの中心となったRoland Saville 氏、Floyd Gerhardt 氏、Majid Saee 氏、Mark Doering 氏、Charlie Stokes 氏、Tom Hunter 氏、Kevin McCormick 氏、および Casey Smith 氏を含む、皆様の多大なる努力に感謝いたします。

お問い合せ先

シスコシステムズ株式会社
URL:http://www.cisco.com/jp/
問合せ URL:http://www.cisco.com/jp/service/contactcenter/
〒107-0052 **東京都港区赤坂** 2-14-27 **国際新赤坂ビル東館**
TEL:03-6655-4433
電話でのお問合せは、以下の時間帯で受付けております。
平日 10:00 ～ 12:00 および 13:00 ～ 17:00