SAFE：
小規模、中規模、およびリモートユーザ ネットワークへのセキュリティ ブループリントの適用

筆者について

この文書の筆者である Sean Convery および Roland Saville は、シスコ本社（米国カリフォルニア州サンノゼ）におけるこのアーキテクチャの参照実装でリーダーを努めました。この 2 人は、VPN およびセキュリティ問題を専門とするネットワーク設計者です。

概要

本文書の最大の目的は、安全なネットワークの設計および実装に携わる各関係者に対し、ベストプラクティスについての情報を提供することにあります。SAFE ホワイトペーパーの基本文書は、http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safe_wp.htm から参照できます。この文書は、大規模な企業ネットワークのセキュリティ設計に関するベストプラクティスをまとめたものです。

本文書は基本文書と同じ原則を、大企業のブランチ オフィスや、スタンドアロンあるいは中小規模の企業など、より小規模なネットワークに合わせて適用することを目的としています。テレワーカー（在宅勤務者）やモバイルワーカーなどのリモートユーザ ネットワークに関する情報も含んでいます。本文書には、基本文書の内容の中で適切と思われるものをすべて掲載しているため、本文書の前に SAFE 基本文書を読んでおく必要はありません。

SAFE は、自社ネットワークにおけるセキュリティ要件を検討するネットワーク設計者のための指針となる文書です。SAFE は、ネットワークセキュリティ設計において深さを備えた防御アプローチをとります。これは、「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」といったことではなく、どんな脅威が予測されるか、その軽減策は何かに重点を置く設計手法です。この戦略は重層的なセキュリティ対策につながり、セキュリティシステムの 1 つに障害が生じても、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。

本文書は、まずアーキテクチャの概要に触れてから、個々の設計の詳細について解説します。各モジュールの最初の 2 セクションでは、主要機器について解説し、予測される脅威とその基本的な軽減方法を説明します。続いて、技術面からこの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しく解説します。付録 A では、SAFE の検証テストについて詳しく説明し、設定スナップショット（設定例）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読者は、最初にこのセクションを読んでから他のセクションを読むことをお勧めします。付録 C には、本文書で使用する技術用語の定義一覧を掲載します。

本文書は、今日のネットワークが直面する脅威に大きな重点を置いています。このような脅威を理解するネットワーク設計者であれば、軽減手段としての技術を配置する場所とその方法について、より適切に判断できます。ネットワークセキュリティに伴う脅威が完全に理解されないと、セキュリティ配備の構成が不適切となったり、セキュリティデバイスばかりが強調されたり、脅威に対して取るべき措置の種類が不足しがちとなります。本文書は、脅威の軽減措置を取り上げることで、ネットワーク設計者がネットワークセキュリティの選択肢を的確に判断するための情報を提供します。

対象読者

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であれば、各分野の冒頭のセクションを読むことによって、ネットワークセキュリティの設計戦略および考察点の全体像を明確に把握できます。ネットワークエ

ンジニアや設計者であれば、本文書全体を読み、必要なデバイスの実際の設定スナップショットに裏付けられた、設計情報や脅威分析の詳細を知ることができます。本文書は、SAFE の基本文書をすでに読んでいて、基本文書で取り上げられているアーキテクチャより小規模のネットワーク設計に関心を持つ読者に対しても有益です。まず本文書の導入セクションを読んでから、配置を検討しているネットワークの種類のセクションに直接移動してもよいでしょう。

注意事項

この文書は、すでにセキュリティポリシーが整備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、ポリシーを策定せずにセキュリティ技術を配置することを推奨していません。本文書は、中小規模およびリモートユーザ ネットワークのニーズに直接応えるものです。大規模な企業ネットワーク設計に関心のある読者は、SAFE ホワイトペーパーの基本文書（http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safe_wp.htm）を参照してください。

この文書のガイドラインに従うだけで、あらゆる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てコンクリート詰めにし、連邦金塊貯蔵庫の地下にでも保管するしかありません。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策定し、本文書のガイドラインに従い、ハッカーやセキュリティコミュニティにおける最新情報を常に把握し、正しいシステム管理手法に基づいて全システムを保守および維持することで、適度のセキュリティを実現することは可能です。そのほか、この文書では包括的に扱いませんが、アプリケーションのセキュリティ問題に対する認識も必要となります。

このアーキテクチャには VPN（仮想プライベートネットワーク）も含まれますが、ここでは詳細な解説を省略します。規模拡張方法に関する詳細や復元力維持のための戦略、その他の VPN 関連の問題は、本文書には含まれません。これらの問題に関心のある読者は、SAFE VPN ホワイトペーパー（http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safev_wp.htm）を参照してください。VPN と同じく、本人確認戦略（認証局［CA］を含む）についても、本文書では詳細に取り上げません。同様に、CA についても、本文書の提供しない詳細レベルの解説が必要ですが、ネットワークセキュリティの他のあらゆる関連分野については十分に検証します。完全機能を備える CA 環境を整備したネットワークはまだ少ないため、CA を使わない状況で、どのように安全にネットワークを展開するかを検討することも重要です。E コマース（電子商取引）も、本文書では扱わない分野の 1 つです。E コマース関連のネットワークに関する推奨事項は、小規模組織と大規模組織ではほとんど違いがありません。したがって、この点については SAFE 基本文書で十分対応できます。最後に、特定の高度なネットワーク アプリケーションおよび技術（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、本文書では扱いません。これらが SAFE 内で使用されることは予想されますが、それぞれに固有のセキュリティ要件については本文書の対象外となります。

SAFE には、シスコおよびシスコの各パートナー企業の製品を使用します。ただし、この文書では特に製品名を挙げていません。文書内で各コンポーネントは、モデルの型番や名前ではなく、その機能目的で示されています。SAFE の検証作業では、実際の製品を、本文書で説明されているとおりのネットワーク実装に設定しました。付録 A「検証テスト」には、検証テストとその結果、および設定スナップショットを掲載しました。

本文書全体で使用する「ハッカー」という用語は、悪意を持って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ます。このような人物をより正確に表現するには、一般に「クラッカー」という用語が使用されますが、ここでは分かりやすく「ハッカー」を使用します。

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、今日のネットワークにおける機能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方法は異なりますが、SAFE では、優先順に挙げた以下の設計目標に従って意思決定が行われました。

- ポリ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機器だけでなく）インフラ全体におけるセキュリティの実装
- 費用効率の高い配置
- 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する、ユーザ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

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、貴重なネットワークリソースに影響を与えようとするほとんどの攻撃を防ぐ必要があります。最初の防御線の突破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食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、ネットワークは安全性を保ちながら、ユーザ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。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手法ではなく、ネットワークをセキュアにするためのブループリントに過ぎません。

中小規模、およびリモートネットワーク向けの SAFE アーキテクチャは、復元性を除外して設計されています。復元性を備えたセキュアなネットワーク設計に関心のある読者は、SAFE 基本文書（以降『SAFE エンタープライズ』と表記）を参照してください。

ネットワーク設計プロセスにおける多くの場面で、ネットワーク機器に統合された機能を使用するか、または専用機能を持つアプライアンスを使用するかを選択する必要があります。統合機能は、既存の機器に実装できるため、あるいは他の機器と相互に作用させ、より優れた機能ソリューションを提供できるため、しばしば魅力的な選択肢となります。これに対してアプライアンス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、性能的なニーズによって専用のハードウェアが必要とされる場合です。この判断は、アプライアンスの処理能力と機能性を取るか、デバイスの統合性におけるメリットを取るかを考慮した上で行ってください。たとえば、小型の IOS ルータに別個のファイアウォールを組み合わせるのではなく、処理能力の高い統合的な Cisco IOS(R) ルータと IOS ファイアウォール ソフトウェアの方が好ましい場合もあります。このアーキテクチャでは、両方のシステムが使用されます。しかし、設計要件によって選択肢が決まらない場合、ソリューションの全体的な費用を削減するため、統合機能が採用されています。

モジュールの概要

ほとんどのネットワークは、組織の IT 要件の拡大に合わせて進化しますが、SAFE アーキテクチャでは、新規構築型のモジュラ型アプローチを採用しています。モジュラ型アプローチには、主に 2 つの利点があります。まず、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のセキュリティ関係に対応できる点です。もう 1 つの利点は、一括的に完全なアーキテクチャを設計しようとしなくても、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ことにあります。各モジュールのセキュリティ設計はそれぞれ個別に行われますが、全体設計の一部として評価されます。

ほとんどのネットワークが、明確なモジュール単位に簡単に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、様々なセキュリティ機能をネットワークのあらゆる場所に実装することが可能になります。この文書では、ネットワークエンジニアが SAFE 実装と同一のネットワークを設計するのではなく、以下に述べる各モジュールを組み合わせ、既存のネットワークに組み込むことを期待しています。

SAFE の原則

ルータはターゲットとなる

ルータは、あらゆるネットワークからあらゆるネットワークへのアクセスを制御します。ルータはネットワークを広告し、ネットワークを使用可能なユーザをフィルタリングする機能を持ちますが、このため、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。ルータのセキュリティは、すべてのセキュリティ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、直接的に被害を受ける可能性を減らすことが必要です。ルータのセキュリティに関しては、以下の項目について他の文書で詳しく解説しています。

- ルータへの Telnet アクセスの禁止
- ルータへの SNMP（Simple Network Management Protocol）アクセスの禁止
- TACACS+（Terminal Access Controller Access Control System Plus）を使用した、ルータへのアクセス制御
- 不要なサービスの停止
- 適切なレベルでのログ記録
- 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

スイッチはターゲットとなる

ルータと同様、スイッチ（レイヤ 2 およびレイヤ 3）にも、セキュリティに関する一連の考慮事項があります。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の手段についての情報は、それほど多く公開されていません。先の「ルータはターゲットとなる」のセクションで示したセキュリティ技術のほとんどは、スイッチにも適用できます。さらに、あらかじめ以下の対策を取る必要があります。

- トランク接続の不要なポートは、すべてのトランク接続設定を「自動」ではなく「オフ」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、通常トランクポートに送られるすべてのトラフィックを受信してしまうことを防止します。
- イーサネットスイッチに使用するソフトウェアのバージョンが古い場合は、トランクポートに使用する VLAN（仮想 LAN）番号が、このスイッチの他のポートで使用されていないことを確認します。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 デバイスを通過せずに他の VLAN に到達することを防止します。この詳細については、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は、すべて使用不可（Disable）に設定します。これにより、ハッカーが未使用ポートに接続して、ネットワークの他の部分と通信することを防止します。
- 2 つのサブネット間のアクセスを安全にする唯一の手段として VLAN を使用することは避けてください。人為的ミスの可能性が生じる上、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、機密を扱う環境で VLAN を使用することは推奨できません。セキュリティの配備に VLAN が必要となる場合は、前述の設定方法とガイドラインに対して十分な注意が必要です。

既存の VLAN 内では、プライベート VLAN によって、特定のネットワークアプリケーションに対して何らかの付加的なセキュリティ機能を提供できます。プライベート VLAN は、同じ VLAN 内の他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、同じコミュニティ内の他のポート、および無差別ポートとだけ通信でき、無差別ポートはどのポートとも通信できます。これは、被害を受けた単一ホストからの影響を軽減するための効果的な方法です。Web サーバ、FTP（File Transfer Protocol）サーバ、および DNS（Domain Name System）サーバで構成される、標準的な公開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、他の 2 台のホストを追跡できます。しかしプライベート VLAN が配置されていれば、システムの 1 つが被害を受けても、このシステムは他のシステムと通信できません。したがって、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。プライベート VLAN はレイヤ 2 接続を制限するため、ネットワーク問題のトラブルシューティングがより困難となります。プライベートVLANは、現在市販されているすべてのイーサネットスイッチがサポートするわけではない点に注意してください。特にローエンドのスイッチは、ほとんどがこの機能をサポートしていません。

ホストはターゲットとなる

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を生じさせます。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、そのすべてに対し、それぞれ異なるタイミングでアップデート版、パッチ、および修正版が公開されます。ホストは、要求を出す他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、ネットワーク内で極めて視認性の高い存在となっています。たとえば、ホストである www.whitehouse.gov にアクセスしたことのある人は大勢いても、ルータである 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。こうした視認性の高さのため、ホストはネットワークへのあらゆる不正侵入の試みにおいて、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、ホストは最も被害を与えやすい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 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、さらに別のベンダ製のオペレーティングシステムを使用し、その Webサーバ自身もオープンソースであるか、さらに別のベンダ製であることがあります。さらにこの Web サーバは、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たり、以上の多様性を一からすべて繰り返すデータベースサーバと通信するかもしれません。これらすべてにおけるマルチソース的な性質が、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、むしろ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、システム内の各コンポーネントに十分な注意を払う必要があります。また、すべてのシステムを、最新のパッチや修正版などによって常に最新の状態に保ちます。特に、これらのパッチが、他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する必要があります。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。

ネットワークはターゲットとなる

ネットワーク攻撃は、最も対処の難しい攻撃の 1 つです。一般にこの攻撃は、それぞれのネットワーク運用の本質的な性質を悪用するものであるためです。これには ARP（Address Resolution Protocol）や MAC（Media Access Control）に基づくレイヤ 2 攻撃、盗聴、分散型サービス妨害（DDoS）攻撃などがあります。ARP および MAC に基づくレイヤ2攻撃の一部は、スイッチおよびルータに対するベストプラクティスの実施によって軽減できます。盗聴については、本文書の付録 B「ネットワークセキュリティ入門」で解説します。しかし DDoS は、特別な注意が必要となる独特の攻撃です。

最悪の攻撃は、阻止の不可能な攻撃です。正常に実行される場合、DDoS はまさにこうした攻撃となります。付録 B で概説するとおり、DDoS はある 1 つの IP アドレス宛に、何十台または何百台ものマシンから疑似データを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。一般にこうした攻撃の目的は、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、インターネットに DS1（1.5 Mbps）接続して、E コマースサービスを Web サイトユーザに提供している組織があるとします。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、ハッカーが DDoS 攻撃を成功させた場合、残念ながら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 DSL（500 Kbps）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れば、不正データで DS1 回線を容易にフラッディングできます。個々のホストは 100 Kbps のトラフィックしか生成できないとしても（研究所のテストによると、1 台のストック PC は一般的な DDoS ツールによって 50 Mbps を容易に生成可能）、その合計量は、この E コマースサイトが処理可能なトラフィック量のほぼ 10 倍にもなります。この結果、正規の Web 要求が失われ、ほとんどのユーザから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が不正データをすべて破棄したときには、トラフィックはすでに WAN 接続を介してリンクを満たしているため、被害が及んだ後となります。

この架空の E コマース企業は、インターネット サービス プロバイダ（ISP）との協力によってのみ、こうした攻撃の防御を期待できます。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できます。このレート制限により、事前に指定された有効帯域幅の容量を超えた時点で、最も不要なトラフィックを破棄できます。この場合、不要なトラフィックに対して正しくフラグを設定することが鍵となります。

DDoS 攻撃の一般的な形態は、ICMP（Internet Control Message Protocol）フラッド、TCP SYN フラッド、または UDP（User Datagram Protocol）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の分類はかなり簡単です。管理者はポート　80（HTTP［Hypertext　Transfer Protocol］）に対する TCP SYN 攻撃を制限する場合に限り、攻撃を受ける間、正規ユーザまでロックアウト（締め出し）してしまうというリスクを負います。この場合でも、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、一時的に新規の正規ユーザをロックアウトして、ルーティングおよび管理接続を保持する方が得策です。

より高度な攻撃になると、ACK（確認応答）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、トラフィックが正規の 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、まさにネットワークへの受け入れを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分類できる見込みはありません。

この種の攻撃を制限する手段の 1 つとして、RFC 1918 および RFC 2827 の規定する、ネットワークフィルタリングに関す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された、パブリックインターネット上で公開し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 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「IP スプーフィング」のセクションで説明しています。たとえば、インターネットに接続したルータへの受信トラフィックに対しては、RFC 1918 および 2827 の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できます。このフィルタリングを ISP 側で実装した場合、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できるので、万が一攻撃を受けたとしても、帯域幅を節約できる可能性があります。総合的に、世界中の ISP が RFC 2827 のガイドラインを実施したとすると、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。この戦略によって DDoS 攻撃を直接防御でき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。契約先の ISP が顧客に提供している DDoS 軽減手法を確認してみてください。

アプリケーションはターゲットとなる

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、数々のエラーが発生する可能性があります。こうしたエラーには、文書を不正確に印刷するなどのあまり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など、極めて悪質なものもあります。一般的な他のセキュリティ脆弱性に加え、このような悪質な問題に注意を払う必要があります。商用アプリケーション、パブリックドメイン（無償公開）アプリケーションのどちらについても、最新のセキュリティ修正版によって、常に最新の状態に保つように注意する必要があります。パブリックドメインアプリケーションや独自に開発したアプリケーションは、貧弱なプログラミングが原因となるどのようなセキュリティリスクも招き入れることがないように、コードを再検証する必要があります。たとえば、アプリケーションが他のアプリケーションや OS 自身を呼び出す方法、アプリケーションが実行される権限レベル、アプリケーションの周囲のシステムへの信頼レベル、そして最後に、データをネットワーク上で伝送するためにアプリケーションが採用する方式などのプログラミングを検証します。次のセクションでは、侵入検知システム（IDS）の概要と、ネットワーク内のアプリケーションや他の機能を対象とした攻撃のいくつかを、IDS がどのように軽減するかについて解説します。

侵入検知システム

侵入検知システム（Intrusion Detection System：IDS）は、物理的な世界でのアラームシステムと同様の機能を持ちます。IDS は攻撃とみなすものを検知した場合、自ら適切に対処するか、管理システムに通知して、管理者に対処してもらうことができます。一部のシステムには、こうした攻撃に対応して防御するための機能が多かれ少なかれ装備されています。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へのコールをいったん代行受信することによって機能させるほか、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させることもできます。前者の方法では、より効果的に攻撃を防御できるのに対し、後者の方法は、より受動的に攻撃に対応する役割を意味します。ホストベース IDS（HIDS）システムはこうした専門的な役割を持つため、通常は攻撃の発見時に警報を発するだけのネットワーク IDS（NIDS）より、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、この専門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。残念ながら、どの技術を使うかに関する選択は、IT 予算に依存することがよくあります。この場合は、個々の技術、監視すべきデバイスの数、および攻撃に対処する人員に対する総合的な費用を、十分に考慮する必要があります。

いったん配置した IDS は、その効果を高め、「偽陽性（Fault Positive）」を排除できるように調整する必要があります。偽陽性は、正常なトラフィックやアクティビティに対してアラームを発生してしまうことです。一方偽陰性は、IDS システムが検知できない攻撃です。IDS は調整することによって、脅威を軽減する役割を果たせるよう、より明確に設定できます。前述のとおり、HIDS には特定のアクティビティが実際にセキュリティへの脅威であることを判断する力に優れているため、もっとも影響のある脅威については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 における脅威軽減の役割を決定する場合、主に 2 つの選択肢があります。ただし、脅威へのどのような対応策を実装するのであっても、まず最初にすべきことは、正しい脅威だけを検知できるように NIDS を適切に調整することです。

1 つ目の選択肢であり、正しく配置しないと潜在的に最も被害の大きくなる方法は、ルータとファイアウォールにアクセス制御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）」する方法です。NIDS は、特定のプロトコルによる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、事前に定義した期間だけブロックできます。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支援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。攻撃とみなされるトラフィックが NIDS によって検知され、そのアラームによって排除が行われると、NIDS はそのデバイスにアクセスリストを配置します。しかし、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、攻撃の始点とはまったく無関係のアドレスをロックアウトしてしまいます。また、ハッカーが使用した IP アドレスが、たまたま大手 ISP の送信 HTTP プロキシサーバの IP アドレスだった場合、膨大な数のユーザがロックアウトされる可能性があります。これ自体、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。

有害な排除リスクを軽減するには、一般に、スプーフィングが UDP よりはるかに困難な TCP トラフィックにだけ排除を使用する必要があります。排除は、脅威が現実的であり、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。排除期間をごく短く設定することも考える必要があります。この場合は、ユーザがこの IP アドレスを使ってどのようなアクションを実行しようとしているかを管理者が判断するのに十分な時間だけ、このユーザを排除します。一方、ネットワーク内部には、より多くの選択肢があります。RFC 2827 フィルタリングが効果的に実行されていれば、スプーフィングされたトラフィックが大幅に制限できているはずです。また、通常は顧客が内部ネットワーク上にいることはないため、内部から試みられる攻撃に対しては、より厳しい立場をとることができます。また、内部ネットワークには、インターネットとの境界部分と同レベルのステートフルフィルタリングが実装されない場合が多いことも考える必要があります。したがって内部ネットワークでは、外部環境よりも大きく IDS に依存する必要があります。

NIDS による脅威軽減の 2 つ目の選択肢は、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、攻撃する側とされる側のホストに 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 トラフィックはスプーフィングがより困難なため、排除より TCP リセットを多用することを検討するべきです。スイッチ型の環境では、SPAN（スイッチ型ポートアナライザ）またはミラーポートを使用しない限り、全ポートの全トラフィックを把握することはできません。したがって、標準的なハブを使用した環境より TCP リセットが困難になることに注意してください。また、このミラーポートが双方向のトラフィックフローに対応し、SPAN ポートの MAC アドレス学習機能を無効にできることを確認してください。

いずれの脅威軽減手法を採用する場合でも、担当者が IDS コンソールを 365 日 24 時間監視する必要があります。IT 担当者は仕事量が過度に多くなる傾向にあるので（特に小企業）、社内の IDS 管理を第三者にアウトソースすることも検討してください。

性能面から見ると、NIDS は回線上のパケットを監視します。NIDS はデータの流れの中に直接存在するわけではないため、NIDS の処理能力を超える速度でパケットが送信されてきた場合でも、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、パケットが失われる可能性もあり、偽陰性や偽陽性の原因となります。IDS の利点を活かすには、IDS の処理能力を超えないように注意してください。ルーティングの面から見ると、IDS は多くの状態認識エンジンと同様、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たパケットが、別の組み合わせから戻されると、IDS はトラフィックの半分しか監視できないため、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

「ログは採るだけでなく、読まなければならない」というのはとても単純なことです。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いうことを言ったことがあるでしょう。しかし、多数のデバイスから情報を記録し、そのすべてを読むことは、非常に骨の折れる仕事となる可能性があります。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一のアラームを報告する場合に、互いのタイムスタンプを一致させ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。攻撃を受けたシステムから大量に生成されるメッセージをどのように処理するのか。ログファイルを効果的に管理しようと考えるなら、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、また別の問いに答える必要があります。デバイスを安全に管理するにはどうするのか。コンテンツを公開サーバに送信する際、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、デバイス上の変更をどのように突き止めれば問題解決につながるのか、といった問題です。

『SAFE エンタープライズ』で解説しているアウトバンド（OOB）管理アーキテクチャは、最高レベルのセキュリティを実現しますが、本文書の目的は費用効率の高いセキュリティ配備なので、ここではこのアーキテクチャを推奨しません。OOB 環境では、各ネットワークデバイスおよびホストはそれぞれ専用の管理インターフェイスを持ちます。そしてこのインターフェイスは、プライベート管理ネットワークに接続されます。この構成により、安全性の低い管理プロトコル（Telnet、TFTP［Trivial File Transfer Protocol］、SNMP など）やシステムログが実稼働ネットワーク上に流れ、これらが捕捉されたり変更されたりするリスクを軽減できます。しかし、本文書で解説するアーキテクチャでは、管理トラフィックをどのような場合でも「インバンド」で送信し、トン

ネリングプロトコルや、安全性の低いプロトコルの代わりに安全なプロトコルを使用して、管理トラフィックを可能な限り安全に保ちます。たとえば、Telnet の代わりに、可能な限り常に SSH（Secure Shell Protocol）を使用します。実稼働ネットワーク上を管理トラフィックが「インバンド」で流れるため、前述の原則により忠実に従うことが重要となります。

ファイアウォール外部のデバイス管理が必要とされる場合、確認すべき要因がいくつかあります。まず、このデバイスはどの管理プロトコルをサポートするのか。IPSec（IP セキュリティ）が実装されたデバイスは、管理ネットワークからデバイスへのトンネルを構築するという、単純な方法で管理すべきです。これにより、安全性の低い多数の管理プロトコルを、1 つの暗号化トンネル内で伝送できるようになります。デバイスが未対応のために IPSec を使用できない場合は、安全性の劣る代替策を選択するしかありません。デバイスの設定では多くの場合、Telnet の代わりに SSH または SSL（Secure Sockets Layer）を使用して、デバイスに対するあらゆる設定変更を暗号化できます。これらのプロトコルは、TFTP、FTP などの安全性の低いプロトコルの代わりとして、デバイスとのデータのやり取りに使用することもできます。しかしシスコの機器では、設定のバックアップやソフトウェアバージョンのアップデートを実行するために、しばしば TFTP が必要とされます。ここで、2 つ目の問いが生じます。この管理チャネルは、常にアクティブにしておく必要があるのかどうか。そうでない場合、管理機能が実行され、その後削除される間、ファイアウォールに一時的な穴を空けることができます。しかし、デバイスが多数の場合には、これに対応できる拡張性がありません。SNMP を使用する場合など、チャネルを常時アクティブにする必要があるなら、次の問いについて検討します。この管理ツールは、本当に必要なのかどうか。SNMP マネージャはしばしば、問題解決や設定を容易にするためにネットワーク内部で使用されます。しかし、レイヤ 2 サービスを 2 つか 3 つのサーバに提供するだけの DMZ スイッチにとって、この機能は本当に必要でしょうか。必要なければ、この機能は無効にします。必要だと判断した場合は、これによってネットワーク環境に潜在的な脆弱性が導入されることを意識してください。以降の数段落にわたり、具体的な管理の種類について詳しく解説します。

レポートの点から見ると、ほとんどのネットワークデバイスは、ネットワーク問題やセキュリティの脅威の解決において非常に貴重なシステムログデータを提供できます。ログを参照したいあらゆるデバイスが生み出すこうしたデータを、システムログ分析ホストに送るようにしてください。このデータは、リアルタイムで、または必要に応じたスケジュール型のレポートの形で閲覧できます。適切な量のデータがログ分析ホストに送られるように、対象となるデバイスの種類に応じてさまざまなログのレベルを選択できます。また、きめ細かい閲覧およびレポート作成が行えるように、分析ソフトウェアでデバイスログデータにフラグを設定することも必要です。たとえば攻撃を受けている間、レイヤ 2 スイッチから送られるログデータは、IDS から送られるデータほどには重要でないこともあります。ログメッセージの時刻を相互に同期させるには、ホストとネットワークデバイスの両方のクロックを同期させる必要があります。デバイスがサポートしているならば、NTP（Network Time Protocol）を使用することで、全デバイスが正確な時刻を維持することを保証できます。攻撃への対処においては、特定の攻撃が発生する順序の識別が重要となるため、数秒の差が意味を持ちます。

安全性管理においては、設定変更の管理も課題の 1 つです。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、最後に確認された設定変更日時を把握することは重要です。変更管理のスケジュール作成は、包括的なセキュリティポリシーの一環とすべきですが、最低限、認証システムを使用してデバイスに加えられた変更を記録し、FTP または TFTP 経由で設定を保存する必要があります。

ヘッドエンドとブランチの比較

以下に説明する小規模および中規模の設計は、2 つの設定での使用が考えられます。1 つは、組織のネットワークの「ヘッドエンド」としての設計です。このヘッドエンドは、同組織の他のオフィスと VPN で接続される場合もあります。たとえばある大きな法律事務所では、ヘッドエンドに中規模ネットワーク設計を採用し、他の拠点にはいくつかの小規模ネットワーク設計を採用するかもしれません。フルタイムの在宅勤務者は、リモートネットワーク設計のセクションで検証するいくつかのオプションによって、ヘッドエンドに接続するかもしれません。もう 1 つは、より大規模な組織のブランチとして機能する設計であり、『SAFE エンタープライズ』で解説する設定に基づいて構築されます。

さらに別の例を挙げると、大手の自動車メーカーは、企業本社に『SAFE エンタープライズ』の設計を使用し、リモート拠点と在宅勤務者向けには本文書で解説する設計を使用するかもしれません。必要となる特定の設計変更については、各セクションで必要に応じて解説します。

予測される脅威

脅威の観点から見ると、中小規模のネットワークは、インターネットに接続している大半のネットワークと同様です。つまり、外部へのアクセスを必要とする内部ユーザが存在し、内部へのアクセスを必要とする外部ユーザが存在します。ネットワークに侵入し、二次的な不正利用を仕掛ける足がかりとするために、次に述べるようないくつかの一般的な脅威を適用し、最初の侵害を発生させます。

1 つは、内部ユーザからの脅威です。調査によって数字が異なりますが、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。

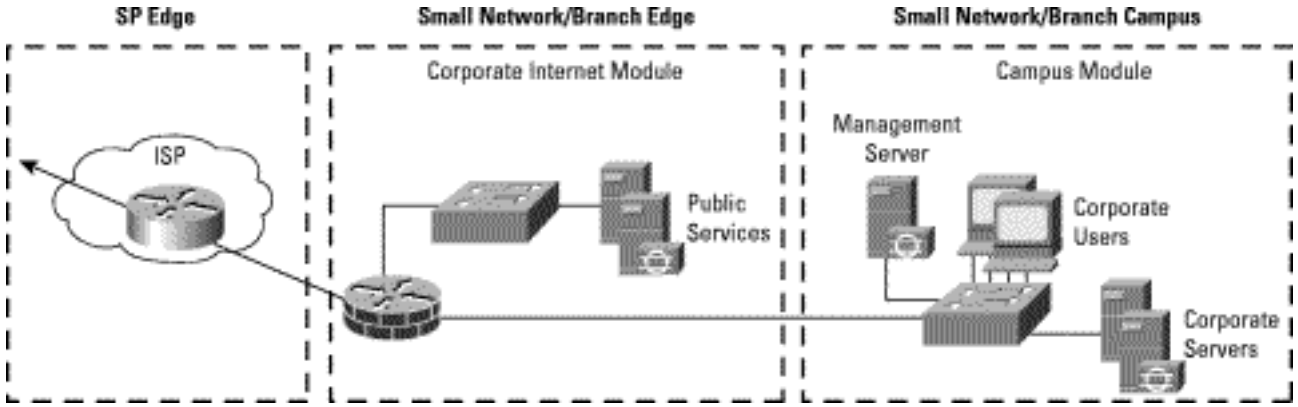
2 つ目は、インターネットに接続した、アドレス指定可能なホストに対する脅威です。こうしたシステムは、アプリケーションレイヤの脆弱性と DoS 攻撃によって攻撃される可能性が高くなります。

これらの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。

小規模ネットワークの設計

小規模ネットワーク設計は 2 つのモジュール、すなわち企業インターネットモジュールとキャンパスモジュールから構成されます。企業インターネットモジュールは、インターネットへの接続を保持すると同時に、VPN および公開サービス（DNS、HTTP、FTP、SMTP）トラフィックを終端します。キャンパスモジュールは、レイヤ 2 スイッチとすべてのユーザ、および管理サーバとイントラネットサーバで構成されます。この設計に関する議論のほとんどは、企業のヘッドエンドとして機能する小規模ネットワークを想定していますが、ブランチとして使用する場合の設計変更についても併せて解説します。

図 1 :小規模ネットワークの詳細



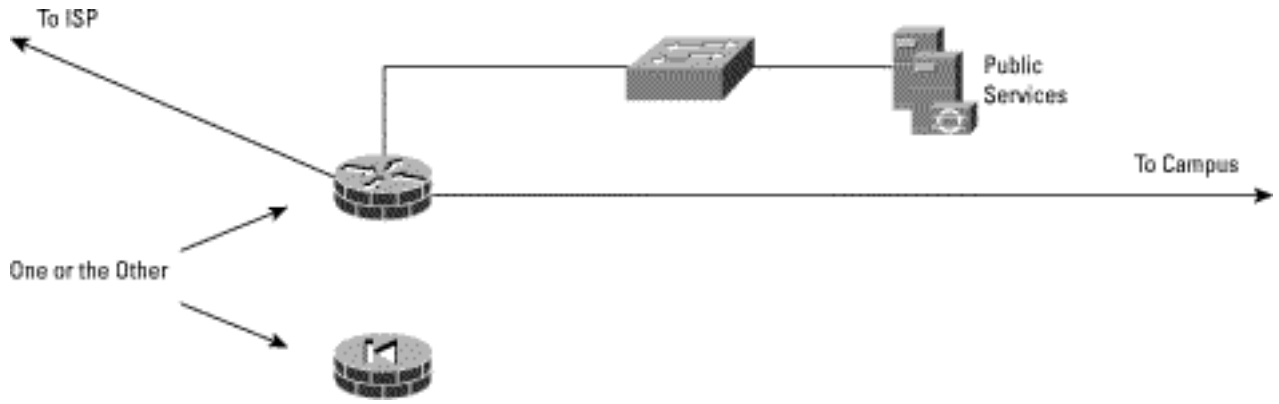
企業インターネットモジュール

企業インターネットモジュールは、内部ユーザにはインターネットサービスへの接続を提供し、インターネットユーザには公開サーバ上の情報へのアクセスを提供します。また、リモート拠点や在宅勤務者には VPN アクセスも提供します。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を提供している場合の詳細については、『SAFE エンタープライズ』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。

主要デバイス

- SMTP サーバ - インターネットとイントラネット メールサーバの間の中継装置として動作
- 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、内部からインターネットへの要求を中継
- FTP/HTTP サーバ - 組織の公開情報を提供
- ファイアウォールまたはファイアウォール ルータ - ネットワークレベルのリソース保護、トラフィックのステートフル フィルタリング、およびリモート拠点とユーザに対する VPN 終端機能を提供
- レイヤ 2 スイッチ（プライベート VLAN 対応） - 管理対象デバイスからのデータが IOS ファイアウォールだけを直接通過することを保証

図 2 :小規模ネットワークにおける企業インターネットモジュールの詳細

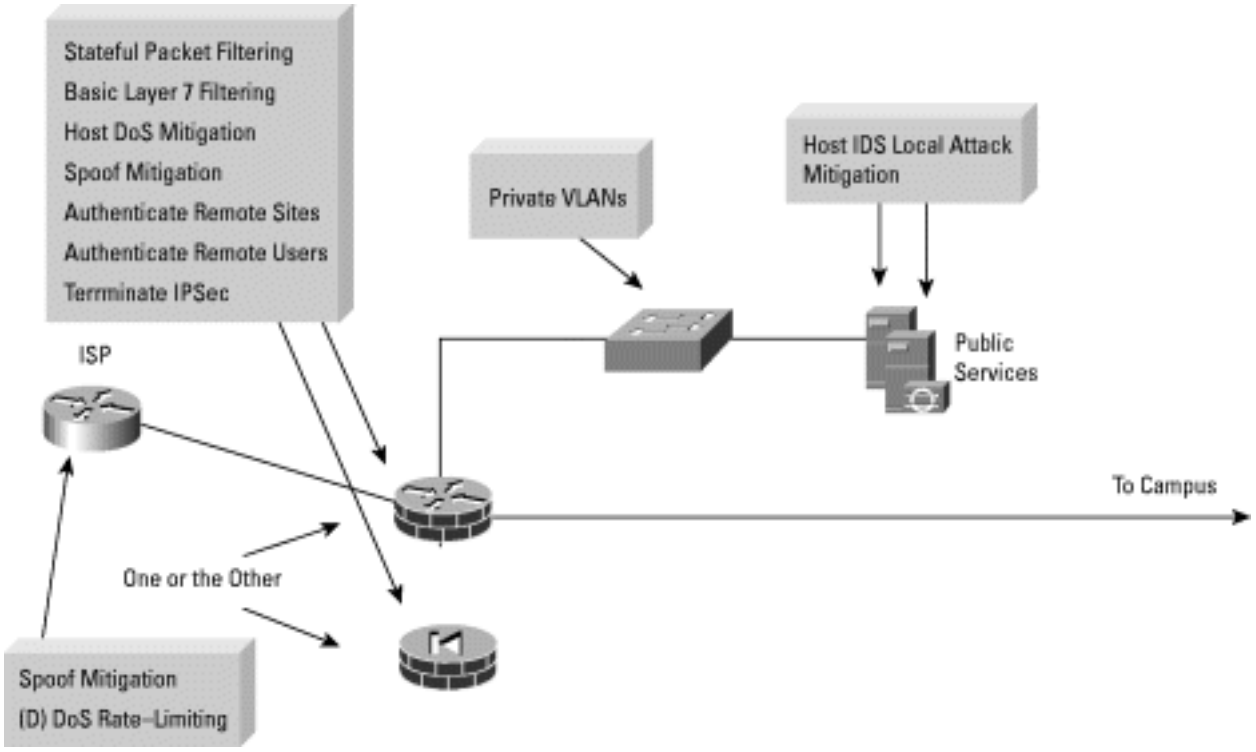


脅威の軽減

このモジュールにおいて攻撃対象となる可能性が最も高いのは、外部からアドレス指定可能なサーバです。予測される脅威は以下のとおりです。

- **不正アクセス** - 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** - 公開サーバの HIDS によって軽減
- **ウィルスとトロイの木馬** - ホストレベルのウィルススキャンによって軽減
- **パスワード攻撃** - ブルートフォース攻撃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 エッジでの CAR(Committed Access Rate)の適用、ファイアウォールでの TCP 設定制御による露出の制限
- **IP スプーフィング** - ISP エッジおよびローカルファイアウォールでの 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と HIDS によって露出を制限
- **ネットワーク偵察** - HIDS 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 HIDS によって攻撃を制限

図 3:企業インターネットモジュールにおける小規模ネットワークの攻撃軽減の役割



設計ガイドライン

このモジュールは、あらゆるセキュリティおよび VPN サービスを 1 つのボックス（デバイス）内に収めており、セキュリティを意識した小規模ネットワーク設計の最終形を表します。この機能の実装方法を決める上で、2 つの主要な選択肢があります。1 つは、ファイアウォールと VPN 機能を備えたルータの使用です。ルータは今日のネットワークで必要と思われるあらゆる高度なサービス（QoS、ルーティング、マルチプロトコルのサポートなど）に対応するため、この構成では、小規模ネットワークにとって最大限の柔軟性が得られます。ルータの代わりに、専用のファイアウォールを使用することもできます。これには、いくつかの配置上の制限が伴います。まず、ファイアウォールは一般にイーサネットだけに対応するものであり、適切な WAN プロトコルへの何らかの変換が必要となります。現在の環境では、ケーブルや DSL（デジタル加入者線）に対応したルータ／モデムの大半はサービスプロバイダから提供され、イーサネット経由でファイアウォールに接続できます。WAN 接続がデバイスに必要となる場合（通信事業者の提供する DS1 回線を接続する場合など）は、ルータを使用する必要があります。専用ファイアウォールを使用すれば、セキュリティサービスを簡単に設定できるという利点が得られ、ファイアウォール機能の実行においてより高い性能が期待できます。どのデバイスを選択するにしても、ステートフル インスペクションによってあらゆる方向のトラフィックを検査し、正規のトラフィックだけがファイアウォールを通過するようにします。さらに、トラフィックがファイアウォールに到達する以前にも、ISP 側に何らかのセキュリティフィルタリングが実装されていると理想的です。初期設定では、ルータはトラフィックを許可し、ファイアウォールはトラフィックを拒否する傾向にあることに注意してください。

ISP 内の顧客エッジルータから始まり、ISP からの出口では、事前に定義したしきい値を超える不要なトラフィックをレート制限することで、DDoS 攻撃を軽減します。また、ISP ルータの出口では RFC 1918 および RFC 2827 フィルタリングを実施することで、ローカルネットワークやプライベートアドレスレンジを使用した送信元アドレスのスプーフィングを軽減できます。

ファイアウォールの入口では、ISP によるフィルタリングの確認として、まず RFC 1918 および RFC 2827 フィルタリングを実施します。さらに、断片化パケットが引き起こす巨大なセキュリティ脅威に備え、インターネット上の標準的なトラフィックタイプには一般に存在するはずのない断片化パケットのほとんどを破棄するように、ファイアウォールを設定します。このフィルタリングによって正規トラフィックが失われることになっても、こうした不正トラフィックを招き入れるリスクに比べれば許容範囲です。外部からファイアウォール自身に宛てられたトラフィックは、IPSec トラフィック、およびルーティングに必要なプロトコルに限定します。

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。外部からアドレス指定可能なサーバについては、ファイアウォールにハーフオープン接続制限などの仕組みを実装すれば、TCP SYN フラッドをある程度防御できます。フィルタリングの面からは、公開サービスセグメント上のトラフィックを関連アドレスおよびポートだけに制限するほか、反対方向のフィルタリングも行います。ファイアウォールおよび HIDS を巧みに回避した攻撃によって公開サーバの 1 つが被害を受けた場合でも、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には、特定のフィルタリングを使用して、公開サーバが他の場所に向けて不正な要求を発行することを防止します。たとえば Web サーバであれば、Web サーバ自身の要求を発行させず、クライアントからの要求に応答するだけに留めるようにフィルタリングする必要があります。これにより、ハッカーが最初の攻撃で被害を与えたホストに、ユーティリティをダウンロードすることを防止できます。また、一次的な攻撃の間に、ハッカーが不要なセッションを発生させることも防止できます。こうした攻撃の例は、たとえば、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向けに xterm を生成するような攻撃です。さらに、DMZ スイッチにプライベート VLAN を配置すれば、被害を受けた公開サーバが同セグメント上の他のサーバを攻撃することも防止できます。こうしたトラフィックはファイアウォールでさえも検知できないため、プライベート VLAN は極めて重要です。

ホストの観点では、公開サービスセグメント上の各サーバにはそれぞれホスト侵入検知ソフトウェアを実装し、OS レベルの不正なアクティビティ、および共通サーバアプリケーション（HTTP、FTP、SMTP など）でのアクティビティを監視します。DNS ホストは、必要なコマンドだけに応答するようにロックダウンし、ハッカーのネットワーク偵察を支援しかねない不要な応答を排除する必要があります。これには、正規のセカンダリ DNS サーバ以外の場所からのゾーン転送の防止も含まれます。メールサービスに対しては、ファイアウォール自身がレイヤ 7 で SMTP メッセージをフィルタリングするようにし、必要なコマンドだけをメールサーバに送信させます。

一般にファイアウォールやファイアウォール ルータは、セキュリティ機能の一部として、何らかの制限付きの NIDS 機能を備えています。この機能はデバイスの性能に影響を与えますが、攻撃を受ける場合に、さらなる攻撃を検知しやすくなります。つまり、攻撃視認性が性能の犠牲の上に成り立つ点に注意します。このような攻撃の多くは IDS を使用しなくても防止できますが、これから仕掛けられようとしている個々の攻撃については、監視ステーションでも検知できません。

VPN 接続は、ファイアウォールまたはファイアウォール ルータを介して提供されます。各リモート拠点は事前共有キーで相互に認証し合い、リモートユーザはキャンパスモジュール内のアクセス制御サーバによって認証を受けます。

代替案

この設計から派生するすべての代替案は、ネットワーク容量の拡大や、さまざまなセキュリティ機能をデバイスごとに分割することを目的としたものです。これにより、この設計の外観は、本文書で後述する中規模ネットワークに限りなく近づきます。中規模設計を丸ごと適用するのではなく、最初の段階としては、専用のリモートアクセス VPN コンセントレータを追加し、リモートユーザ コミュニティの管理性を高めることです。

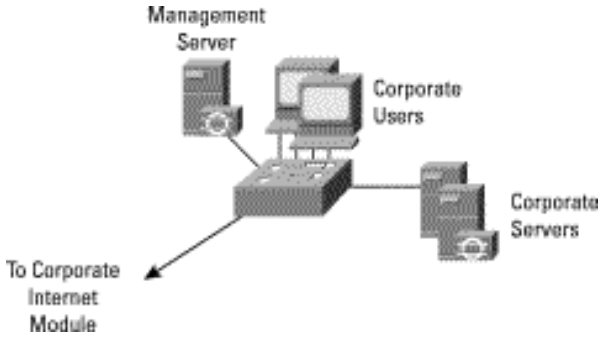
キャンパスモジュール

キャンパスモジュールは、エンドユーザのワークステーション、企業のイントラネットサーバ、管理サーバ、および各デバイスの支援に必要となるレイヤ 2 インフラで構成されます。このレイヤ 2 機能は、小規模ネットワーク設計では 1 つのスイッチ内に組み込まれます。

主要デバイス

- **レイヤ 2 スイッチ（プライベート VLAN 対応）** - ユーザのワークステーションにレイヤ 2 サービスを提供
- **企業サーバ** - 内部ユーザに電子メールサービス（SMTP、POP3）を提供し、ワークステーションにファイル、印刷、および DNS サービスを提供
- **ユーザのワークステーション** - ネットワーク上の認可ユーザにデータサービスを提供
- **管理ホスト** - HIDS、システムログ、TACACS+/RADIUS（Remote Access Dial-In User Service）の各機能、および全般的な設定管理機能を提供

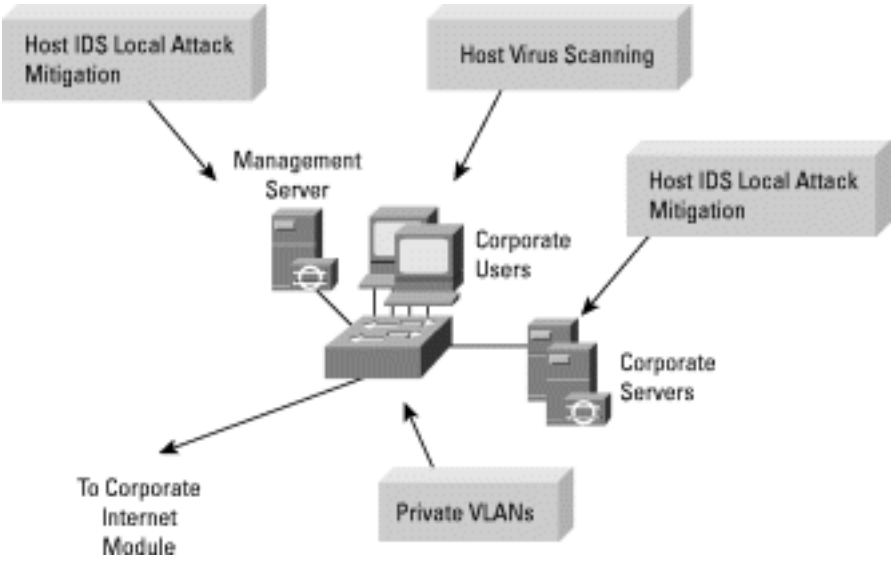
図 4: 小規模ネットワークにおけるキャンパスモジュールの詳細



脅威の軽減

- **パケットスニファ** - スイッチ型インフラによってスニファの効果を制限
- **ウィルスおよびトロイの木馬アプリケーション** -ホストベースのウィルススキャンにより、大部分のウィルスと多くのトロイの木馬を防止
- **不正アクセス** - ホストベースの侵入検知とアプリケーション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最新のセキュリティ修正版によって常に最新の状態に保ち、HIDS で保護
- **信用詐欺** - プライベート VLAN により、同一サブネット内のホストからの不要な通信を防止
- **ポート転送** - HIDS 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 5: キャンパスモジュールにおける小規模ネットワークの攻撃軽減の役割



設計ガイドライン

キャンパススイッチの主な機能は、実稼働および管理トラフィックをスイッチし、企業サーバと管理サーバ、およびユーザに接続性を提供することです。スイッチ内でプライベート VLAN を有効にすると、デバイス間の信用詐欺を軽減できます。たとえば、企業ユーザは企業サーバと通信する必要があるにしても、ユーザどうしでは通信の必要性がない場合もあります。

キャンパスモジュール内には、レイヤ 3 デバイスが何も存在しません。したがって、この設計では内部ネットワークのオープン性のため、アプリケーションとホストのセキュリティを重視していることに注意してください。このため、キャンパス内の主要システム（企業サーバ、管理システムなど）には HIDS も実装します。

代替案

管理ステーションとネットワークの他の部分との間に、小型のフィルタリングルータまたはファイアウォールを設定することで、全体的なセキュリティを向上できます。これにより、管理者が必要とみなした特定方向にだけ、管理トラフィックが流れることになります。組織内の信用度が高い場合は HIDS を外すこともできますが、これは推奨できません。

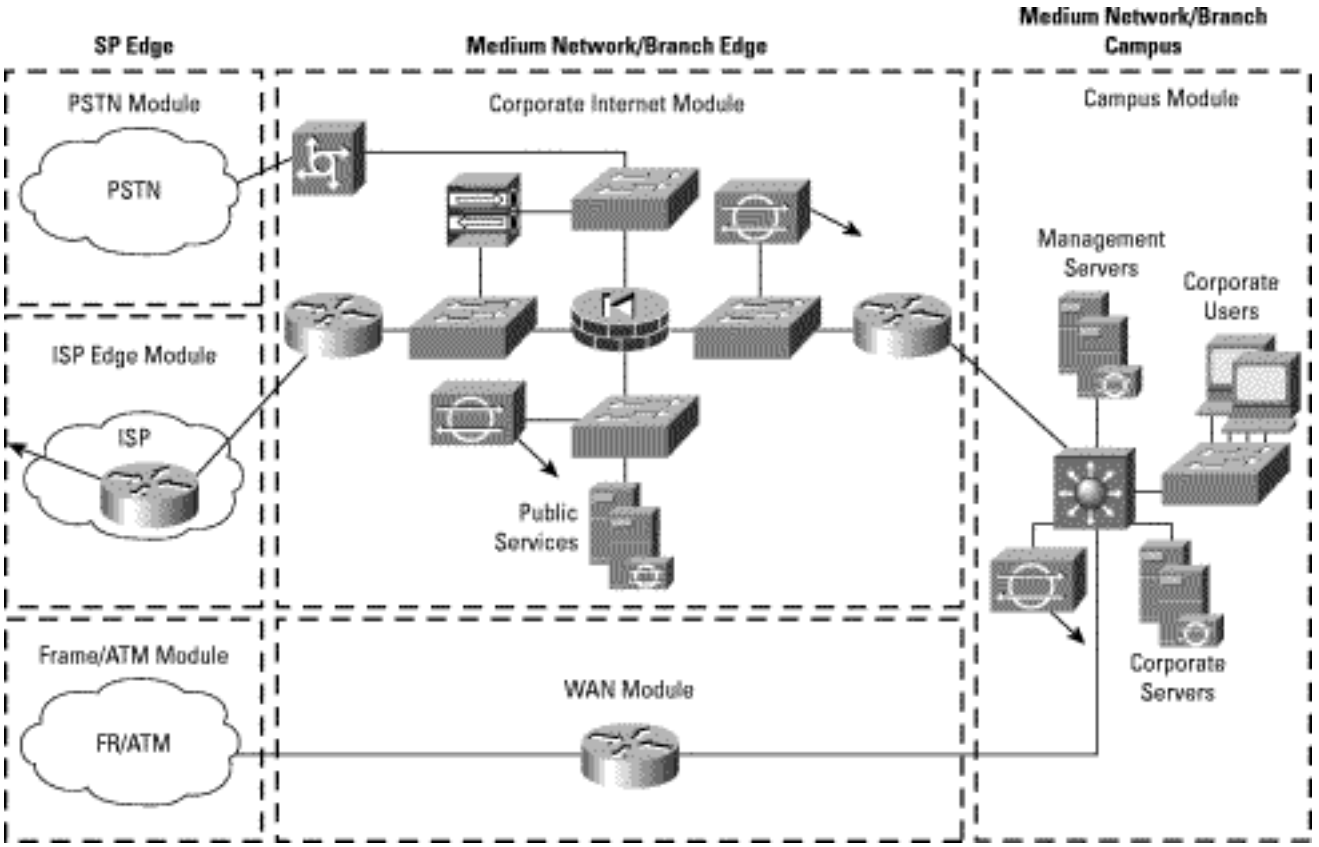
ブランチとスタンドアロンの比較

ブランチとして構成する場合、リモートアクセス VPN 機能は通常は企業本社から提供されるため、実装の必要はありません。さらに、管理ホストは中央拠点に置かれるのが一般的です。この場合、管理トラフィックは拠点間 VPN 接続によって、企業本社まで伝送する必要があります。

中規模ネットワーク設計

SAFE の中規模ネットワーク設計は 3 つのモジュール、すなわち企業インターネットモジュール、キャンパスモジュール、および WAN モジュールで構成されます。小規模ネットワーク設計と同様、企業インターネットモジュールはインターネットに接続され、VPN および公開サービス（DNS、HTTP、FTP、SMTP）のトラフィックを終端します。ここでは、ダイヤルイン トラフィックも終端されます。キャンパスモジュールは、レイヤ 2 および 3 スイッチングインフラのほか、すべての企業ユーザ、管理サーバ、およびイントラネットサーバを収容します。WAN の観点から見ると、中規模設計に接続されるリモート拠点には、2 つのオプションがあります。1 つは WAN モジュールを使用したプライベート WAN 接続であり、もう 1 つは企業インターネットモジュールにつながる IPSec VPN です。この設計に関する議論のほとんどは、企業のヘッドエンドとして機能する中規模ネットワークを想定していますが、ブランチとして使用する場合の特定の設計変更についても併せて解説します。

図 6：中規模ネットワークの詳細



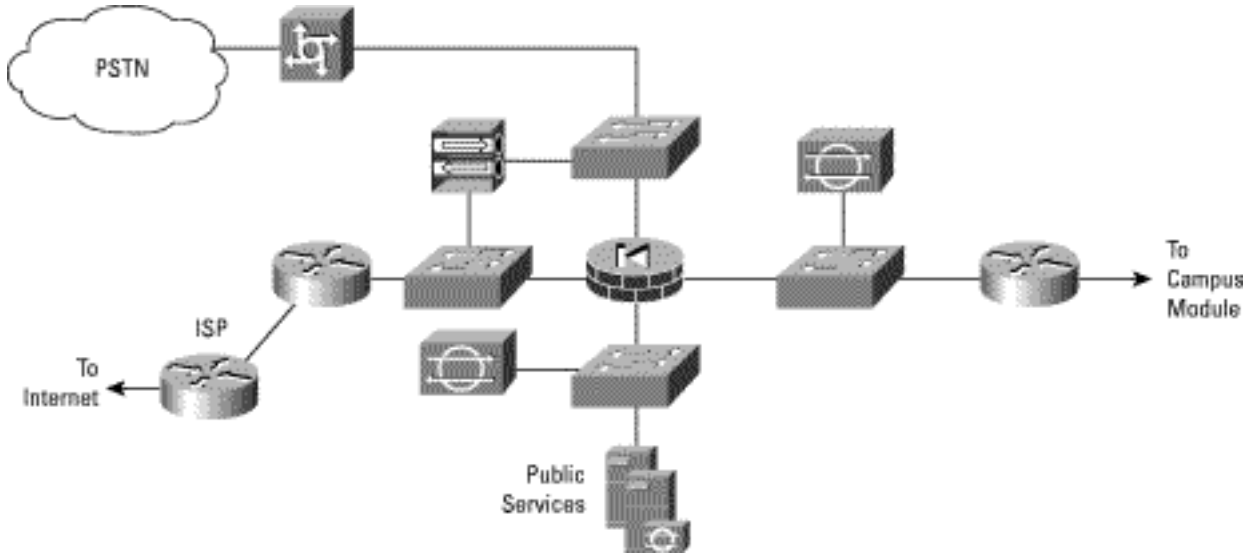
企業インターネットモジュール

企業インターネットモジュールの目的は、内部ユーザにはインターネットサービスへの接続、インターネットユーザには公開サーバ（HTTP、FTP、SMTP、DNS）上の情報へのアクセスを提供することです。また、このモジュールはリモートユーザおよびリモート拠点からの VPN トラフィックや、従来のダイヤルインユーザからのトラフィックを終端します。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を提供している場合の詳細については、『SAFE エンタープライズ』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。

主要デバイス

- **ダイヤルインサーバ** - 個々のリモートユーザを認証し、このユーザのアナログ接続を終端
- **DNS サーバ** - 中規模ネットワークにおける権威ある外部 DNS サーバとしての役割を果たし、内部からインターネットへの要求を中継
- **FTP/HTTP サーバ** - 組織の公開情報を提供
- **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。差異化したセキュリティをリモートアクセスユーザに提供。信頼されたリモート拠点を認証し、IPSec トンネルを使用した接続を提供
- **レイヤ 2 スイッチ（プライベート VLAN 対応）** - 各デバイスにレイヤ 2 接続を提供
- **NIDS アプライアンス** - モジュール内の主要なネットワークセグメントに対し、レイヤ 4～7 の監視機能を提供
- **SMTP サーバ** - インターネットとイントラネット メールサーバの間の中継装置として動作し、メールの内容を検査
- **VPN コンセントレータ** - 個々のリモートユーザを認証し、IPSec トンネルを終端
- **エッジルータ** - 基本的なフィルタリングとインターネットへのレイヤ 3 接続を提供

図 7：中規模ネットワークにおける企業インターネットモジュールの詳細



脅威の軽減

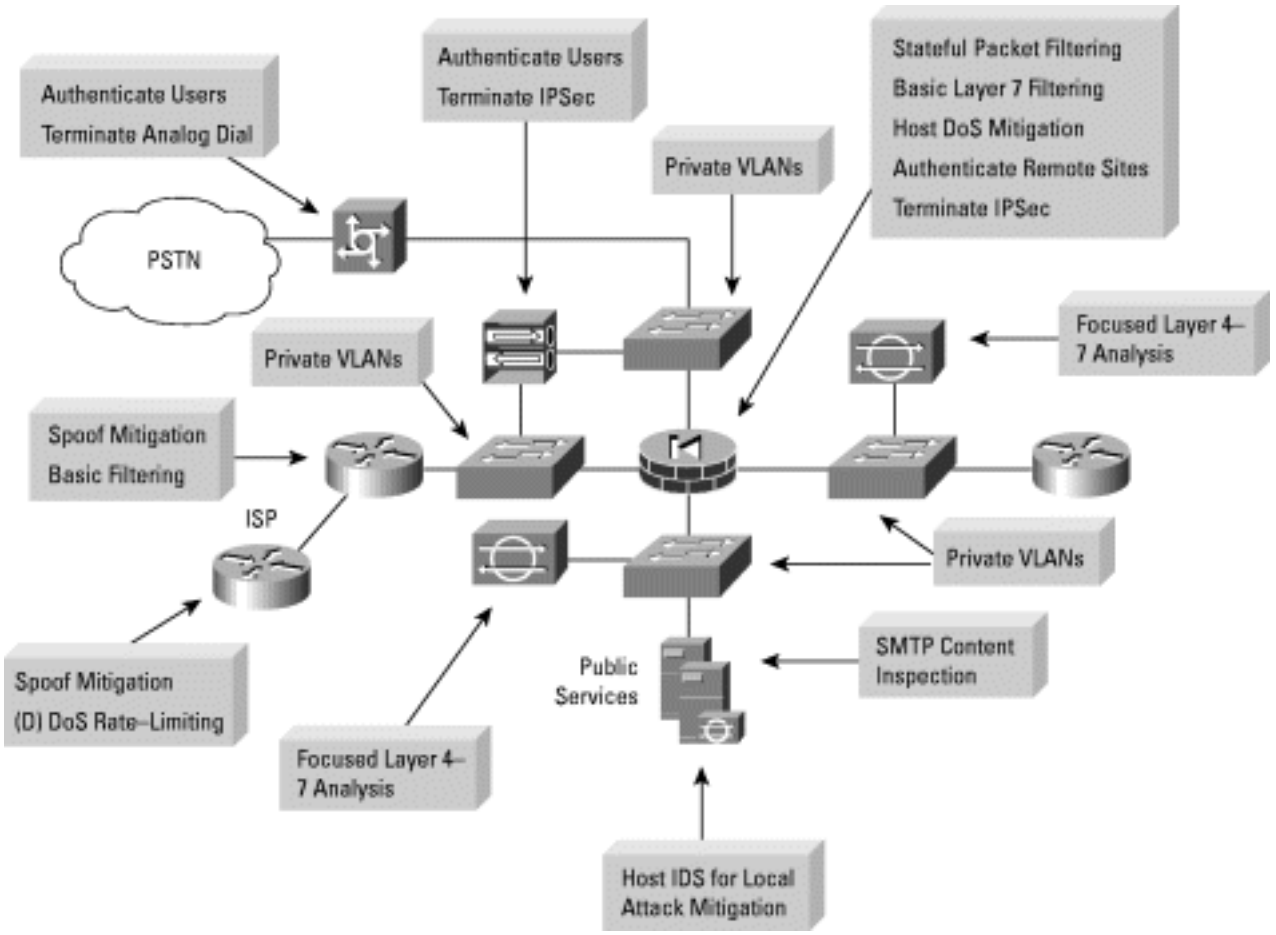
このモジュールで攻撃対象となる可能性が高いのは、外部からアドレス指定可能なサーバです。予測される脅威は以下のとおりです。

- **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の IDS によって軽減
- **ウィルスおよびトロイの木馬アプリケーション** - 電子メール内容のフィルタリング、HIDS、およびホストベースのウィルススキャンにより軽減
- **パスワード攻撃** - ブルートフォース攻撃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** - ISP エッジでの CAR の適用、およびファイアウォールでの TCP 設定制御
- **IP スプーフィング** - ISP エッジおよび中規模ネットワーク エッジルータでの 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および HIDS による露出の制限
- **ネットワーク偵察** - IDS による偵察の検知、プロトコルフィルタリングによる偵察効果の制限
- **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 HIDS によって攻撃を制限

リモートアクセス VPN および拠点間 VPN サービスも、このモジュールにおける攻撃対象です。予測される脅威は以下のとおりです。

- **ネットワークトポロジの発見** - 入口のルータにアクセス制御リスト（ACL）を設定し、インターネットから VPN コンセントレータおよびファイアウォールへのアクセスを、IKE（Internet Key Exchange）および ESP（Encapsulating Security Payload）だけに制限
- **パスワード攻撃** - ワンタイム パスワード（OTP）によりブルートフォース パスワード攻撃を軽減
- **不正アクセス** - パケット復号化後にファイアウォール サービスを適用することにより、権限のないポートへのトラフィックを防止
- **中間者による偽装攻撃（Man-in-the-middle attacks）** - リモートトラフィックの暗号化により軽減
- **パケットスニファ** - スイッチ型インフラによってスニファの効果を制限

図 8:企業インターネットモジュールにおける小規模ネットワークの攻撃軽減の役割



設計ガイドライン

以降のセクションでは、企業インターネットモジュール内の各デバイスの機能について詳述します。

ISP ルータ

ISP 内の顧客エッジルータの主な機能は、インターネットまたは ISP ネットワークへの接続の提供です。ISP ルータの出口では、事前に定義したしきい値を超える不要なトラフィックをレート制限することで、DDoS 攻撃を軽減します。最後に、ISP ルータの出口で RFC 1918 および RFC 2827 フィルタリングを設定し、ローカルネットワークとプライベートアドレス範囲を使用した送信元アドレスのスプーフィングを軽減します。

エッジルータ

中規模ネットワークでのエッジルータの機能は、ISP ネットワークと中規模ネットワークとの間に境界点を設けることです。中規模ネットワークのエッジルータ入口では、基本的なフィルタリングを使用して、予測される IP トラフィックだけにアクセスを限定し、基本的な攻撃のほとんどを排除する目の粗いフィルタの役割を持たせます。ここでは ISP フィルタリングの確認として、RFC 1918 および RFC 2827 フィルタリングも実施します。さらに、断片化パケットが引き起こす巨大なセキュリティ脅威に備え、インターネット上の標準的なトラフィックタイプには一般に存在するはずのない断片化パケットの大部分を破棄するように、ファイアウォールを設定します。このフィルタリングによって正規トラフィックが失われることになっても、こうした不正トラフィックを招き入れるリスクに比べれば許容範囲です。最後に、VPN コンセントレータまたはファイアウォール宛のすべての IPSec トラフィックも通過を許可します。ルータのフィルタリングは、IKE および IPSec トラフィックだけが VPN コンセントレータまたはファイアウォールに到達するように設定します。リモートアクセス VPN では、リモートシステムの IP アドレスが一般に知られることはないため、リモートユーザと通信するヘッドエンド ピア（VPN コンセントレータ）だけにフィルタリングを限定できます。拠点間 VPN では、リモート拠点の IP アドレスは一般に公開されます。したがって、フィルタリングは両方のピア間の双方向のトラフィックに設定する必要があるでしょう。

ファイアウォール

ファイアウォールの主な機能は、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実施することです。また、ファイアウォールは、リモート拠点の実稼働および管理トラフィックに対する拠点間 IPSec VPN トンネルの終端点でもあります。ファイアウォールの外側には、複数のセグメントが存在します。1 つは公開サービスセグメントであり、このセグメント内のホストはすべて、公的にアドレス指定が可能です。もう 1 つはリモートアクセス VPN およびダイヤルイン用のセグメントであり、詳細については後述します。外部からアドレス指定可能なサーバは、ファイアウォールにハーフオープン接続制限などの仕組みを実装すれば、TCP SYN フラッドをある程度防御できます。フィルタリングの点では、公開サービスセグメントのトラフィックを関連アドレスおよびポートに限定するだけでなく、逆方向のフィルタリングも行います。（ファイアウォール、HIDS、NIDS を巧みに回避した）攻撃によって公開サーバの 1 つが被害を受けた場合でも、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には、フィルタリングを使用して、公開サーバが他の場所に向けて不正な要求を発行することを防止します。たとえば Web サーバであれば、Web サーバ自身の要求を発行させず、クライアントからの要求に応答するだけに留めるようにフィルタリングする必要があります。これにより、ハッカーが最初の攻撃で被害を与えたホストに、新たにユーティリティをダウンロードすることを防止できます。また、一次的な攻撃の間に、ハッカーが不要なセッションを発生させることも防止できます。こうした攻撃の例は、たとえば、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向けに xterm を生成するような攻撃です。さらにプライベート VLAN を使用すれば、被害を受けた公開サーバが同セグメント上の他のサーバを攻撃することも防止できます。こうしたトラフィックはファイアウォールでさえも検知できないため、プライベート VLAN は極めて重要です。

侵入検知

公開サービスセグメントには、NIDS アプライアンスを設置します。この主な機能は、ファイアウォール設定によって許可されたポートに対する攻撃の検知です。最も多い例が、特定サービスに対するアプリケーションレイヤ攻撃です。NIDS で一致するシグネチャは、すでにファイアウォール突破に成功したパケットを意味します。したがって、公開サービスセグメントの NIDS は、制限を厳しく設定する必要があります。さらに、各サーバにはそれぞれ HIDS を実装します。HIDS の主な機能は、OS レベル、および共通サーバアプリケーション（HTTP、FTP、SMTP など）で生じた不正な動作の監視です。DNS は、必要なコマンドだけに応答するようにロックダウンし、ハッカーのネットワーク偵察を支援しかねない不要な応答を排除する必要があります。これには、正規のセカンダリ DNS サーバ以外の場所からのゾーン転送防止も含みます。SMTP サーバにはメールの内容検査サービスを実装し、ウィルスやトロイの木馬型の攻撃を軽減します。この種の攻撃は内部ネットワークを対象とし、通常はメールシステム全般に蔓延します。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、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プライベートインターフェイスと内部ルータとの間に設置される NIDS アプライアンスで、攻撃に対する最終的な分析を行います。このセグメント内部への通過を許可されるのは、発行された要求に対する応答、公開サービスセグメントから選択された少数のポート、およびリモートアクセスセグメントからのトラフィックだけなので、このセグメントで検知される攻撃はほとんどないはずです。このセグメントで検知されるのは、高度な攻撃だけとなります。こうした攻撃は通常、公開サービスセグメント上のシステムの 1 つが被害を受け、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します。たとえば、公開 SMTP サーバが被害を受けた場合、ハッカーは 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 から、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、すでに被害が発生している可能性があるため、他のセグメントで検知された場合より厳重に対処する必要があります。たとえば、前述の TCP リセットや排除を使用して 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。

リモートアクセス VPN

リモートアクセス VPN コンセントレータの主な機能は、中規模ネットワークへの安全な接続をリモートユーザに提供することです。VPN コンセントレータは、内部ネットワークのアクセス制御サーバとのセッションを開始し、ユーザを認証してから、ネットワークへのアクセス権限を与えます。次に、アクセス制御サーバはワンタイムパスワード（OTP）システムに問い合わせ、ユーザの認証情報を評価します。コンセントレータからクライアントに送られる IPSec ポリシーに基づき、ユーザによるトンネル分割が無効になるので、ユーザは企業経由の接続でしかインターネットに接続できないようになります。使用される IPSec パラメータは、暗号化には 3DES（Triple Data Encryption Standard）、データの完全性には SHA/HMAC（Secure Hash Algorithm/Hash-Based Message Authentication Code）が使用されます。VPN トンネルが終端した後に、トラフィックはファイアウォールを介して送信されるので、VPN ユーザに適切なフィルタリングが適用されます。こうした構成より、IDS からファイアウォールに対し、特定のトラフィック排除を指示することも可能です。このシナリオは、VPN デバイスの前にファイアウォールを設置する、最近よく見られる配置形態とは逆です。VPN デバイスの前にファイアウォールを設置すると、ファイアウォール内のトラフィックが暗号化されたままになるので、ユーザトラフィックの個々の種類が判別できなくなります。

ダイヤルイン アクセス ユーザ

従来のダイヤルインユーザは、モデム内蔵のアクセスルータによって終端されます。ユーザとサーバの間でレイヤ 2 接続が確立されると、ユーザは 3 方向 CHAP（Challenge Handshake Authentication Protocol）によって認証されます。リモートアクセス VPN サービスと同様、認証には AAA（認証、認可、アカウンティング）サーバが使用されます。認証されたユーザには、IP プールから IP アドレスが付与されます。

レイヤ 2 スイッチ

企業インターネットモジュール内のスイッチの主な機能は、モジュール内のさまざまなデバイス間に、レイヤ 2 接続を提供することです。外部セグメント、公開サービスセグメント、VPN セグメント、および内部セグメント間を物理的に分割するため、複数の VLAN を 1 台のスイッチに設定するのではなく、個別の複数のスイッチを使用しています。これにより、1 台のスイッチの設定ミスによってセキュリティが損なわれる可能性を軽減します。さらに、各スイッチがプライベート VLAN 機能を実行するので、信用詐欺に基づく攻撃の軽減に役立ちます。

内部ルータ

内部ルータの主な役割は、企業インターネットモジュールとキャンパスモジュール内をレイヤ 3 分割し、ルーティング機能を提供することです。このデバイスはあくまでもルータとして機能し、どちらのインターフェイス上のトラフィックをも制限するアクセスリストを持ちません。ルーティング情報自体が DoS 攻撃に使用されることもあるので、こうした攻撃に備え、デバイス間のルーティング情報の更新を認証することもあります。このルータは、ルーティングされるイントラネットと外部ネットワークとの最終的な境界点となります。ほとんどのファイアウォールはルーティングプロトコルを使用せずに設定されているので、企業インターネットモジュール内に、ネットワークの他の部分に依存しないルーティングポイントを提供することは重要です。

代替案

このモジュールには、いくつかの代替的な設計があります。ネットワーク管理者は、中規模ネットワークにつながるエッジルータに基本的なフィルタリング機能を実装するより、このデバイスへのステートフル ファイアウォールの実装を選択する場合もあります。ステートフル ファイアウォールを 2 台用意することは、モジュール内のセキュリティに対するより徹底した防御策となります。攻撃に対するネットワーク管理者の意識の高さによっては、ファイアウォールの前に NIDS アプライアンスを設置することも考えられます。基本的なフィルタ機能を適切に実装すれば、ファイアウォール外部の IDS は、通常であればファイアウォールが破棄しかねない重要なアラーム情報を提供できます。このセグメントで生成されるアラームの量は恐らく膨大なので、この位置でのアラームは、ファイアウォール背後で生成されるアラームより重要度を低く設定するべきです。また、このセグメントから発せられたアラームを、このセグメントから切り離した管理ステーションへログ記録することも検討してください。これにより、他のセグメントからの正規のアラームに、適切な注意を払うことができます。このように、ファイアウォール外側の NIDS が提供する視認性により、組織が受けやすい攻撃の種類を評価しやすくなります。さらに、ISP や企業のエッジフィルタの効果も評価できます。

このほか、2 つの代替案があります。1 つは、ファイアウォールとキャンパスモジュールとの間のルータを除去することです。この場合、ルータの機能はキャンパスモジュールのレイヤ 3 スイッチに統合できますが、企業インターネットモジュールは、ネットワークの他の領域からのレイヤ 3 サービスに依存せずに機能することができなくなってしまいます。もう 1 つは、すでに設定したメールの内容検査に加え、さらに内容検査を追加することです。たとえば、公開サービスセグメントに URL フィルタリングサーバを設置し、従業員がアクセス可能な Web ページの種類をフィルタリングします。

キャンパスモジュール

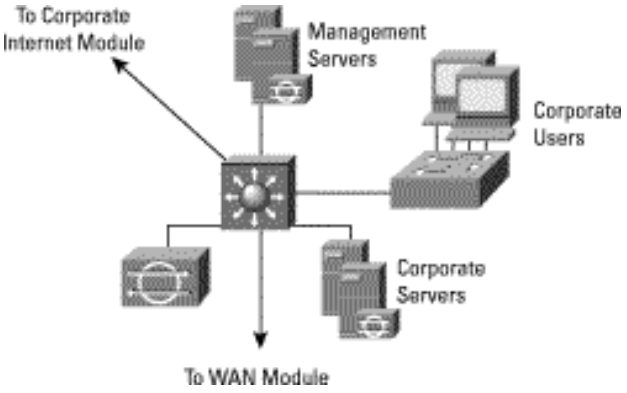
キャンパスモジュールは、エンドユーザのワークステーション、企業イントラネットサーバ、および管理サーバのほか、これらのデバイスの支援に必要となるレイヤ 2 および 3 インフラで構成されます。『SAFE エンタープライズ』のすべてのキャンパスモジュールは、1 つのモジュールに統合されます。この構成は、中規模ネットワークのサイズをより正確に反映し、設計にかかる総費用を削減します。

企業インターネットモジュールと同様、中規模ネットワーク設計では、企業設計に通常採用される冗長性を考慮していません。

主要デバイス

- **レイヤ 3 スイッチ** - キャンパスモジュール内の実稼働および管理トラフィックのルーティングとスイッチ、ビルディングスイッチへの分散レイヤサービス提供、トラフィックフィルタリングなどの高度なサービスをサポート
- **レイヤ 2 スイッチ（プライベート VLAN対応）** - ユーザのワークステーションにレイヤ 2 サービスを提供
- **企業サーバ** - 内部ユーザに E メール（SMTP、POP3）サービスを提供し、ワークステーションにはファイル、印刷、および DNS サービスを提供
- **ユーザのワークステーション** - ネットワーク上の認可ユーザにデータサービスを提供
- **SNMP 管理ホスト** - 各デバイスに SNMP 管理機能を提供
- **NIDS ホスト** - ネットワーク内の全 NIDS デバイスからのアラームを集約
- **·Syslog ホスト** - ファイアウォールと NIDS ホストのログ情報を集約
- **アクセス制御サーバ** - ネットワークデバイスに認証サービスを提供
- **ワンタイムパスワード（OTP）サーバ** - アクセス制御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
- **システム管理者ホスト** - デバイスの設定、ソフトウェア、およびコンテンツを変更
- **NIDS アプライアンス** - モジュール内の主なネットワークセグメントに対するレイヤ 4～レイヤ 7 での監視を実施

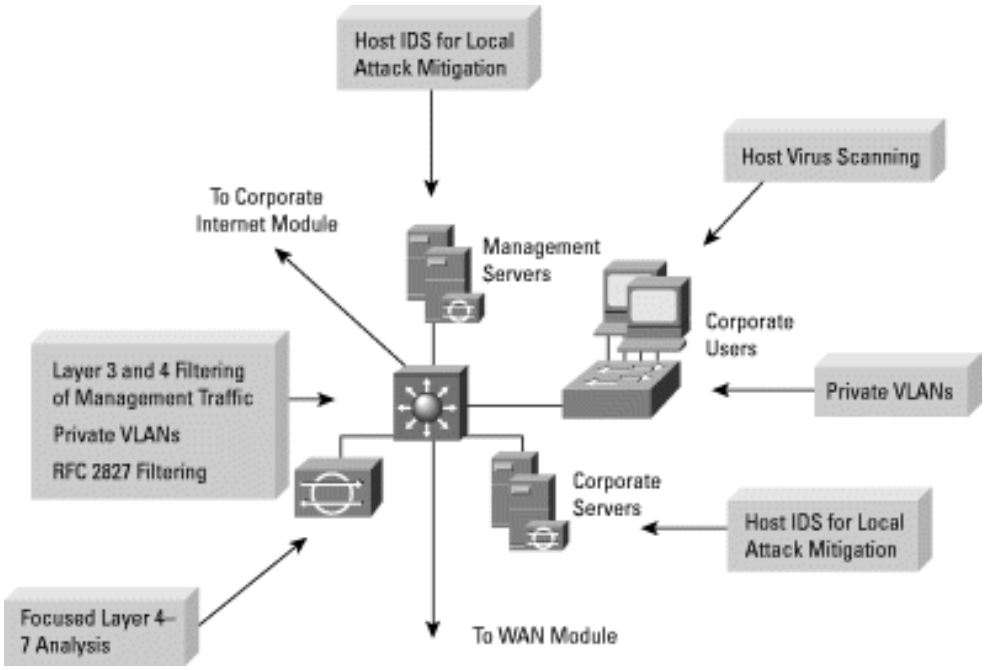
図 9：中規模ネットワークにおけるキャンパスモジュールの詳細



脅威の軽減

- **パケットスニファ** - スイッチ型インフラによってスニファの効果を制限
- **ウィルスおよびトロイの木馬アプリケーション** - ホストベースのウィルススキャンにより、ほとんどのウィルスおよび多数のトロイの木馬を軽減
- **不正アクセス** - ホストベースの侵入検知およびアクセス制御によって軽減
- **パスワード攻撃** - アクセス制御サーバにより、主要アプリケーションに対し強力な 2 要素認証を実行
- **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最新のセキュリティ修正版によって常に最新の状態に保ち、HIDS で保護
- **IP スプーフィング** - RFC 2827 フィルタリングによる送信元アドレスのスプーフィング防止
- **信用詐欺** - 信用の取り決めを明確にしておき、同じサブネット内のホストが不要な通信を行うことをプライベート VLAN によって防止
- **ポート転送** - HIDS 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 10: キャンパスモジュールにおける中規模ネットワークの攻撃軽減の役割



設計ガイドライン

以降のセクションでは、キャンパスモジュール内の各デバイスの機能を詳しく解説します。

コアスイッチ

コアスイッチの主な機能は、実トラフィックと管理トラフィックのルーティングとスイッチング、ビルディングスイッチへの分散レイヤサービス（ルーティング、QoS、アクセス制御）、企業サーバおよび管理サーバへの接続提供、およびサブネット間のトラフィックフィルタリングなどの高度な機能の提供です。企業サーバセグメント、管理サーバセグメント、および企業ユーザセグメントに個別の VLAN を提供し、WAN モジュールと企業インターネットモジュールへの接続を提供するため、レイヤ 2 スイッチではなくレイヤ 3 スイッチを採用しています。レイヤ 3 スイッチは、内部から仕掛けられた攻撃に対する一連の防御と保護機能を実行します。レイヤ 3 スイッチはアクセス制御の実行により、ある部署内から他の部署内のサーバ上の機密情報にアクセスできる可能性を軽減します。たとえば、マーケティング部と研究開発部を包含するネットワークがあるとします。このネットワークでは、研究開発部のサーバを特定の VLAN セグメントに切り離し、研究開発部の人員だけがアクセスできるようにこのセグメントへのアクセスをフィルタリングできます。性能面での理由から、このアクセス制御は、フィルタリングしたトラフィックをほぼワイヤスピードで送信できるようなハードウェアプラットフォームに実装することが重要です。このような構成では一般的に、従来的な専用ルーティング機器の数を増やすのではなく、レイヤ 3 スイッチの使用が必要となります。このアクセス制御により、RFC 2827 フィルタリングを実施することで、ローカルな送信元アドレスのスプーフィングも防止できます。RFC 2827 フィルタリングは、企業ユーザおよび企業イントラネットサーバの VLAN に対して適用する必要があります。

各 VLAN 内では、プライベート VLAN を使用することで、デバイス間の信用詐欺攻撃を軽減できます。たとえば企業サーバセグメントにおいて、個々のサーバが互いに通信し合う必要性はまったくないはずです。これらのサーバは、企業ユーザセグメントに接続されたデバイスとだけ通信できればいいのです。

管理サーバに対してさらに防御機能を強化するには、管理サーバセグメントに接続された VLAN インターフェイスに対し、拡張的なレイヤ 3 およびレイヤ 4 フィルタリングを送信方向に設定します。アクセス制御リスト（ACL）により、管理サーバに出入りする接続は、管理下にあるデバイス（IP アドレスで識別）だけ、および必要なプロトコルとサービスだけ（ポート番号で識別）に限定されます。これには、リモート拠点のデバイスに向けた管理トラフィックのアクセス制御も含まれます。このトラフィックはファイアウォールによって暗号化されてから、リモート拠点に送信されます。ACL 経由で確立された接続だけを許可することで、管理対象デバイスへのアクセス管理をさらに強化できます。

ビルディングスイッチ

キャンパスモジュールにおけるビルディングスイッチの主な機能は、企業ユーザのワークステーションにレイヤ 2 サービスを提供することです。エンドユーザの個々のワークステーションは、通常は互いに通信し合う必要性はありません。したがって、信用詐欺攻撃を軽減するため、ビルディングスイッチには VLAN を実装します。スイッチのセキュリティ原則のセクションで解説したネットワークセキュリティ ガイドラインに加え、ホストベースのウィルススキャン機能もワークステーションレベルで実行する必要があります。

侵入検知

キャンパスモジュールには、NIDS アプライアンスも含まれます。NIDS アプライアンスに接続するスイッチポートは、監視の必要なすべての VLAN からのトラフィックが、アプライアンスのモニタリングポートにミラーリングされるように設定します。この NIDS アプライアンスが分析する攻撃は、キャンパスモジュール自身の内部で発生したと言えるため、ここで検知される攻撃はほとんどないはずです。たとえば、未知のモデムからの接続によってユーザのワークステーションが被害にあった場合、NIDS はキャンパス内で発生した不審な動作を検出します。これ以外にも、不満を持つ従業員、権限のないユーザがアクセスできる状態に放置されたワークステーション、不注意からポータブル PC にロードされたトロイの木馬アプリケーションなどが、内部攻撃の起点となる可能性があります。HIDS は、個々の企業イントラネットサーバおよび管理サーバにもインストールします。

代替案

ネットワークの規模がある程度小さければ、ビルディングスイッチの機能をコアスイッチに統合し、ビルディングスイッチを省くこともできます。この場合、エンドユーザのワークステーションはコアスイッチに直接接続されます。信用詐欺攻撃を軽減するには、コアスイッチにプライベート VLAN 機能を実装します。内部ネットワークの性能要件がそれほど高くない場合は、高性能のレイヤ 3 スイッチの代わりに、コアと分散拠点に個別のルータとレイヤ 2 スイッチを使用できます。

必要であれば、個々の NIDS アプライアンスを、コアスイッチに適した統合 IDS モジュールに置き換えることができます。これにより、NIDS モジュールに流れるトラフィックには高いスループットを期待できます。NIDS モジュールは、1 つの 10/100 Mbps イーサネットポート経由で接続されるのではなく、スイッチのバックプレーン上に位置するためです。スイッチの ACL を使用すれば、IDS モジュールに送られるトラフィックの種類を制御できます。

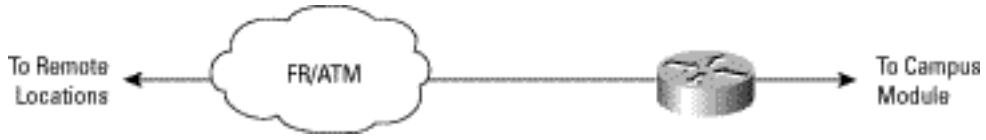
WAN モジュール

WAN モジュールは、プライベートネットワークからリモート拠点に接続する必要がある場合だけに組み込みます。こうした必要性が生じるのは、厳格な QoS 要件が IPSec VPN では満たせない場合や、IPSec への移行を経済的に正当化できず、レガシー WAN 接続が使用されている場合です。

主要デバイス

IOS ルータ - リモート拠点へのルーティング、アクセス制御、および QoS メカニズムを提供

図 11: 中規模ネットワークにおける WAN モジュールの詳細



脅威の軽減

- IP スプーフィング - レイヤ 3 フィルタリングにより軽減
- 不正アクセス - ルータ上の単純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限定

図 12: WAN モジュールの攻撃軽減の役割

設計ガイドライン

WAN モジュールに設定するセキュリティのレベルは、接続するリモート拠点および ISP に対する信頼度に応じて異なります。セキュリティの実装には、IOS セキュリティ機能を使用します。この設計では、シリアルインターフェイスに適用する受信方向のアクセスリストを使用して、不要なトラフィックが中規模ネットワークにアクセスすることを防止します。さらにイーサネットインターフェイスに受信方向のアクセスリストを適用すると、中規模ネットワークからリモート拠点に戻るトラフィックの種類も制限できます。

代替案

情報の機密性への関心が極めて高い組織では、従来の WAN リンクを流れるトラフィックを暗合化することもあります。拠点間 VPN と同様、IPSec を使用しても、こうしたレベルの情報機密性を実現できます。また、WAN ルータ上でファイアウォールを実行すれば、SAFE 設計で使用する基本的な ACL と比べ、さらに多くのアクセス制御オプションを利用できます。

ブランチとヘッドエンドの比較

ブランチとして構成する場合、中規模設計のいくつかの構成要素を省略できます。まず考慮すべきは、その組織が、プライベート WAN リンクまたは IPSec VPN によって企業本社に接続する必要があるのかどうかということです。プライベート WAN を選択する理由には、よりきめ細かい QoS サポート、マルチキャスト サポート、ネットワークインフラの信頼性、あるいは IP 以外のトラフィックの必要性などがあります。『SAFE エンタープライズ』で解説した GRE（Generic Routing Encapsulation）による IPSec を使用する場合は、VPN 環境内でもマルチキャストおよび非 IP トラフィックを使用できることに注意してください。プライベート WAN 接続ではなく、IPSec VPN を選択する理由はいくつかあります。まず、インターネット上で IPSec VPN を使用すると、すべてのリモート拠点がインターネットにローカルにアクセスできるようになるので、ヘッドエンドの帯域幅（およびその費用）を節約できます。また、多くの国内アプリケーションやほとんどの国際的アプリケーションでは、IPSec VPN を使用することで、プライベート WAN 接続より大幅に費用を削減できます。

ブランチとして運用する中規模ネットワークに対してプライベート WAN リンクを選択した場合は、企業インターネットモジュール全体が不要になります（ブランチからローカルなインターネットアクセスが必要となる場合を除く）。一方、IPSec VPN モジュールを選択した場合は、WAN モジュールが不要になります。ブランチの中規模設計において、サービスが企業本社から提供される場合は、WAN モジュールだけでなく、リモートアクセス サービス用の VPN コンセントレータまたはダイヤルアクセスルータも不要になります。

管理の面から見ると、中規模ネットワークの設定およびセキュリティ管理は、企業本社の管理モジュールから実行されます（IT リソースが一元管理される場合）。拠点どうしの接続にプライベート WAN リンクを選択すると、管理トラフィックは、管理の必要なデバイスに対して WAN モジュール上をスムーズに送信されるようになります。拠点どうしの接続に IPSec VPN を選択すると、ほとんどの管理トラフィックは、プライベート WAN リンクの使用時と同様に送信されます。ファイアウォール外部のエッジルータなど、いくつかのデバイスは IPSec トンネルの対象外となるので、別途管理が必要です。この場合は、各デバイスに個別の IPSec

トンネルを提供したり、アプリケーションレイヤの暗号化（SSH）を利用してデバイスを設定変更することもできます。原則のセクションで述べたように、すべての管理プロトコルに安全性を確保するプロトコルが関連付けられているわけではありません。

リモートユーザ設計

このセクションでは、SAFE 設計においてリモートユーザ接続を提供するための、4 種類の手法について解説します。リモート接続は、モバイルワーカーと在宅勤務者の両方に適用されます。こうした設計の主な狙いは、リモート拠点から企業本社への接続、また、何らかの手段によるインターネットへの接続を提供することです。次の 4 つの手法は、ソフトウェアのみ、ソフトウェアとハードウェアの組み合わせ、およびハードウェアのみのソリューションを表します。

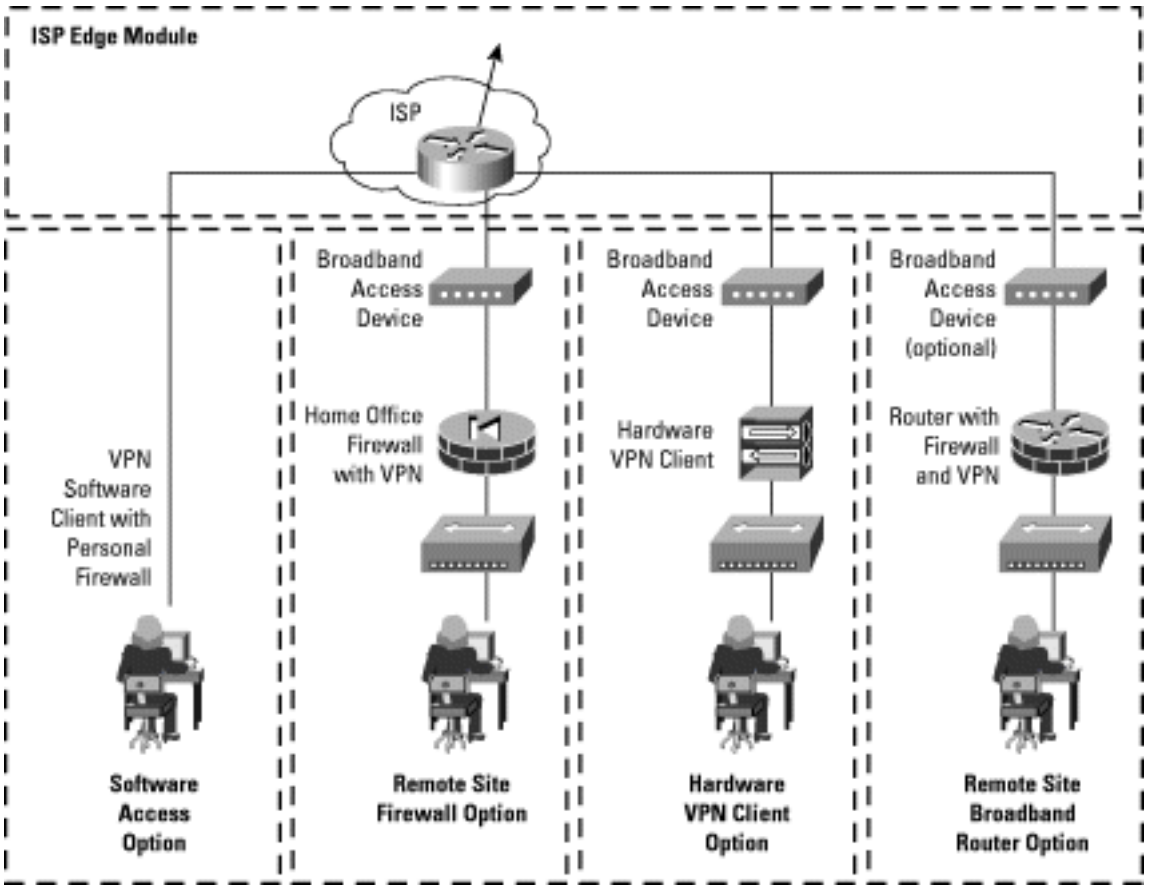
- **ソフトウェアアクセス** - リモートユーザは、ソフトウェア VPN クライアントおよびパーソナルファイアウォール ソフトウェアを PC に実装
- **リモート拠点のファイアウォール オプション** - ファイアウォール機能と企業本社への IPSec VPN 接続を提供する専用ファイアウォールによって、リモート拠点を保護。ISP の提供するブロードバンド アクセスデバイス（DSL モデム、ケーブルモデムなど）経由の WAN 接続を提供
- **ハードウェア VPN クライアントオプション** - リモート拠点において、企業本社への IPSec VPN 接続を提供する専用ハードウェア VPN クライアントを使用。ISP の提供するブロードバンド アクセスデバイス経由の WAN 接続を提供
- **リモート拠点ルータオプション** - リモート拠点において、ファイアウォール機能と企業本社への IPSec VPN 接続の両方を提供するルータを使用。このルータがブロードバンドアクセスを直接提供するか、あるいは ISP の提供するブロードバンド アクセスデバイスを経由する

以上の各設計については、以降の設計ガイドラインのセクションで詳しく解説します。これらの解説ではすべて、接続がインターネット経由であることを前提とします。この代わりにプライベート WAN 接続（ISDN、プライベート DSL など）を使用する場合は、トラフィックの暗号化は必ずしも必要ではありません。どのリモート拠点オプションを使用する場合でも、これらのリモート拠点を包含できるように組織のセキュリティ境界を拡張することに注意してください。

主要デバイス

- **ブロードバンド アクセス デバイス** - ブロードバンドネットワーク（DSL、ケーブルなど）へのアクセスを提供
- **VPN 対応のファイアウォール** - リモート拠点と企業ヘッドエンドとの間に、安全なエンドツーエンド暗号化トンネルを提供。リモート拠点のリソースをネットワークレベルで保護し、トラフィックのステートフル フィルタリングを実施
- **レイヤ 2 ハブ** - リモート拠点内の各デバイスに接続を提供（ファイアウォールまたはハードウェア VPN クライアントとの統合が可能）
- **パーソナルファイアウォール ソフトウェア** - 個々の PC をデバイスレベルで保護
- **ファイアウォールおよび VPN 対応のルータ** - リモート拠点と企業ヘッドエンドとの間に、安全なエンドツーエンド暗号化トンネルを提供。リモート拠点のリソースをネットワークレベルで保護し、トラフィックのステートフル フィルタリングを実施。音声サービスや QoS などの高度なサービスを提供
- **VPN ソフトウェアクライアント** - 個々の PC と企業ヘッドエンドとの間に、安全なエンドツーエンド暗号化トンネルを提供
- **VPN ハードウェアクライアント** - リモート拠点と企業ヘッドエンドとの間に、安全なエンドツーエンド暗号化トンネルを提供

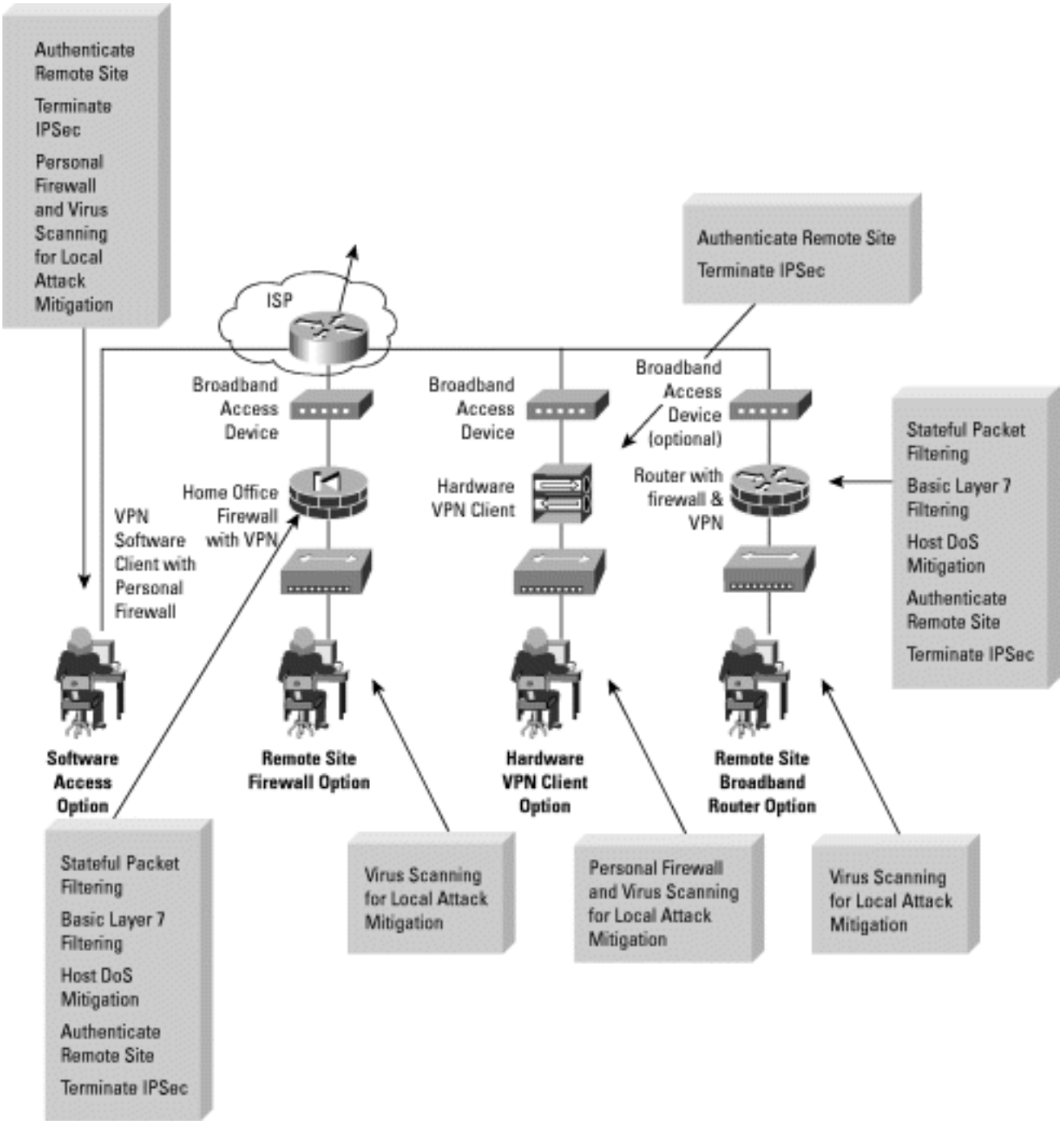
図 13:リモートユーザ構成の詳細



脅威の軽減

- **不正アクセス** - リモート拠点のファイアウォールやルータでのセッションのフィルタリングおよびステートフル検査、またはパーソナルファイアウォール ソフトウェアのアプリケーションアクセス制御による軽減
- **ネットワーク偵察** - リモート拠点デバイスでのプロトコル フィルタリングにより、効果を制限
- **ウィルスおよびトロイの木馬攻撃** - ホストレベルのウィルススキャンによる軽減
- IP **スプーフィング** - ISP エッジおよびリモート拠点デバイスでの RFC 2827 および RFC 1918 フィルタリングによる軽減
- **・中間者による偽装攻撃** - リモートトラフィックの暗号化による軽減

図 14: リモートユーザ設計での攻撃軽減の役割



設計ガイドライン

以降のセクションでは、各リモートユーザ接続オプションの機能について詳しく解説します。

ソフトウェア アクセス オプション

ソフトウェア アクセス オプションは、モバイルワーカーおよび在宅勤務者を対象としています。リモートユーザに必要となるのは、VPN クライアントソフトウェアを搭載した PC と、ダイヤルインまたはイーサネット接続によるインターネットまたは ISP ネットワークへの接続です。VPN ソフトウェアクライアントの主な機能は、クライアントデバイスから VPN ヘッドエンドデバイスまでの経路に、安全な暗号化トンネルを確立することです。ポリシーに基づきアクセス権が付与されるかどうかを、ファイアウォールまたはクライアント自身でフィルタリングする場合、ネットワークに対するアクセスと権限付与は、本社の拠点から制御されます。リモート ユーザはまず認証を受けてから、全 VPN トラフィックに対して使用される IP パラメータ（仮想 IP アドレスなど）、およびネームサーバ（DNS および WINS［Windows Internet Name Service］）の場所を通知されます。中央拠点からは、分割トンネルのオン／オフ

も制御できます。SAFE 設計では分割トンネルを無効にしているので、VPN トンネルが確立されている場合、全リモートユーザは企業接続経由でインターネットにアクセスする必要があります。リモートユーザは、インターネットまたは ISP ネットワークへの接続時に、必ずしも VPN トンネルの確立を望まないため、PC への不正アクセスの軽減にはパーソナルファイアウォールソフトウェアを使用することを推奨します。また、ウィルスやトロイの木馬プログラムの PC への感染を軽減するため、ウィルススキャンソフトウェアの使用も推奨します。

リモート拠点ファイアウォール オプション

リモート拠点ファイアウォール オプションは、在宅勤務者、また、潜在的にはごく小規模のブランチオフィスを対象としています。このオプションでは、リモート拠点で、サービスプロバイダから提供される何らかのブロードバンドアクセスが利用できることを想定しています。DSL モデムまたはケーブルモデムの背後には、ファイアウォールを設置します。

ファイアウォールの主な機能は、ファイアウォール自身と VPN ヘッドエンドデバイスとの間に安全な暗号化トンネルを確立することと、ファイアウォール経由で開始されたセッションに対し、接続状態の制御と詳細なフィルタリングを実施することです。リモート拠点ネットワーク上の個々の PC は、企業リソースにアクセスする際、VPN クライアントソフトウェアを使用する必要はありません。また、ステートフル ファイアウォールによってインターネットへのアクセスが保護されるため、個々の PC には必ずしもパーソナルファイアウォール ソフトウェアをインストールする必要はありません。しかし、ネットワーク管理者がさらに強力なセキュリティを必要とするなら、パーソナルファイアウォールソフトウェアもリモート拠点 PC に実装します。この構成は、在宅勤務者が外出し、出先から何らかの公衆網経由で直接インターネットに接続しようとする場合に便利です。ホストはステートフル ファイアウォールによって保護されるため、全トラフィックをいったん企業本社に戻すのではなく、リモート拠点からインターネットに直接アクセスできます。本社との通信に NAT（ネットワークアドレス変換）を使用しない限り、リモート拠点デバイスの IP アドレスは、本社または他のリモート拠点のアドレス空間と重複しないように割り当てる必要があります。インターネットに直接アクセスする必要があるリモート拠点デバイスは、アドレスを正規の登録アドレスに変換する必要があります。このアドレス変換を行うには、インターネットに向かうすべてのセッションを、ファイアウォール自身の持つグローバル IP アドレスに変換します。

企業ネットワークとインターネットに対するアクセスと権限付与は、リモート拠点ファイアウォールと VPN ヘッドエンドデバイスの両方の設定によって制御します。リモート拠点ファイアウォールの設定とセキュリティ管理には、ファイアウォールの公開側から企業本社に戻る IPSec トンネルを利用します。これにより、リモート拠点ユーザは、ホームオフィスのファイアウォールに何も設定する必要がなくなります。ローカルユーザが不注意にファイアウォールの設定を変更してしまい、このデバイスのセキュリティポリシーが損なわれることがないように、ファイアウォールには認証機能を設定するべきです。このオプションでは、企業ネットワークにアクセスするリモート拠点の個々のユーザは認証を受けません。代わりに、リモート拠点ファイアウォールと VPN ヘッドエンドでデバイス認証を利用します。

企業全体のあらゆる PC と同様、リモート拠点の個々の PC に及ぶウィルスおよびトロイの木馬プログラムの感染を軽減するため、ここでもウィルススキャン ソフトウェアを推奨します。

ハードウェア VPN クライアント オプション

ハードウェア VPN クライアント オプションは、リモート拠点ファイアウォールオプションと同じ構成ですが、ハードウェア VPN クライアントにはステートフル ファイアウォールが常駐していません。この構成では、特に分割トンネルを有効にする場合、個々のホストにパーソナルファイアウォールが必要となります。パーソナルファイアウォールがない場合、VPN デバイス背後の個々のホストのセキュリティは、攻撃者が NAT（ネットワークアドレス変換）の悪用に失敗することを期待するしかなくなります。これは、分割トンネルを利用する場合、インターネットへの接続が単純な 1 対多の NAT 変換を通過するだけで、レイヤ 4 以上のフィルタリングがいっさい適用されないためです。分割トンネルを無効にすると、インターネットへのすべての接続は、企業本社を経由せざるを得なくなります。こうすると、エンドシステムにパーソナルファイアウォールを実装する要件は部分的に緩和されます。

ハードウェア VPN クライアントの使用には、2 つの大きな利点があります。1 つは、VPN ソフトウェアクライアントを使用する場合と同様、企業ネットワークおよびインターネットへのアクセスと権限付与が、本社から一元的に制御できることです。VPN ハードウェアクライアント デバイス自身の設定とセキュリティ管理は、SSL 接続を介して中央拠点から実行されます。これにより、リモート拠点ユーザは、ハードウェア VPN クライアントに対して何も設定する必要がなくなります。2 つ目の利点は、リモート拠点ネットワークの個々の PC が、VPN クライアントソフトウェアを使用せずに企業リソースにアクセスできる点です。ただし、このオプションでは、企業ネットワークにアクセスするリモート拠点の個々のユーザは認証を受けません。代わりに、VPN ハードウェアクライアントと VPN ヘッドエンド コンセントレータは相互に認証し合います。

リモート拠点ルータ オプション

リモート拠点ルータ オプションは、わずかな違いを除き、リモート拠点ファイアウォール オプションとほぼ同じです。このオプションをスタンドアロンのブロードバンドアクセスデバイス背後に配置する場合、唯一の違いは、ルータが QoS やルーティング、その他のカプセル化アプリケーションといった高度なアプリケーションに対応できることです。また、ブロードバンド機能をルータに統合すれば、スタンドアロンのブロードバンドアクセスデバイスは不要になります。このオプションでは、契約先の ISP がブロードバンドルータ自体の管理を許可していることが前提となりますが、このシナリオはあまり一般的ではありません。

脅威の軽減戦略

SAFE は、ネットワークにセキュリティを実装するためのガイドです。ネットワークのセキュリティポリシーとなるものではなく、既存の全ネットワークに完全なセキュリティを提供するための、包括的な設計でもありません。SAFE はむしろ、ネットワーク設計者がセキュリティ要件を満たすための設計および実装方法を検討するための、テンプレートの役割を持ちます。

セキュリティポリシーの策定は、ネットワークを安全なインフラに移行する上で最初に実行すべき作業です。セキュリティポリシーに関する基本的な推奨事項は、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。ポリシーを策定したら、ネットワーク設計者は本文書の冒頭セクションで述べたセキュリティ原則を考慮して、既存のネットワークインフラにこのポリシーを対応させるための具体的な方法を検討する必要があります。

SAFE のアーキテクチャは十分な柔軟性を備えているため、大部分のネットワークに適用できます。設計者は SAFE によって、各ネットワーク機能のセキュリティ要件を、それぞれほぼ独立して取り込むことができます。各モジュールは一般に自己完結型であり、相互接続されたモジュールは基本的なセキュリティレベルにしか存在しないことを想定しています。このため、ネットワーク設計者は、企業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。最も重要なネットワーク機能の安全確保を、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とおりに対処できるのです。

本文書は、SAFE アーキテクチャの詳細を解説した 2 番目のホワイトペーパーです。本文書と『SAFE エンタープライズ』を併読すると、さまざまな規模のネットワークに対するセキュリティ要件およびセキュリティ実装について検証できます。これ以外にも研究、調査、および改良の必要がある多くの分野が残されていることは著者も承知していますが、こうした分野には以下のようなものがあります（ただしこれらに限定されない）。

- セキュリティ管理の綿密な分析と実装
- 自己証明、ディレクトリサービス、AAA　技術、および認証局（CA）の綿密な分析と実装
- ワイヤレスの設計、管理、および実装に関する詳細な考察

付録 A：検証実験（設定例）

この文書で述べる機能性を検証するために、SAFE の参照実装が存在します。この付録では、一般的なデバイス設定に対する総合ガイドラインや、各モジュール内の特定デバイスの設定について詳しく述べます。以下に、この実験で実際に使用したデバイスの設定スナップショットを示しますが、これらの設定をそのまま実ネットワークに適用することはお勧めできません。

全体ガイドライン

ここに示すサンプルコマンドの一部は、この文書の冒頭で述べた SAFE 原則に対応しています。

ルータ

以下のサンプルコマンドでは、実験に使用したほとんどのルータの持つ基本設定オプションの大半を有効にしています。

```
! 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-servers
no service tcp-small-servers
! Turn on logging and read-only snmp
!
service timestamp log datetime localtime
logging 10.3.8.254
logging 10.3.8.253
snmp-server community Txo~QbW3XM ro 98
! Generate RSA keys and enable SSH access. This requires the router support encryption.
! You will be prompted for the size of the RSA key. 1024 bits was chosen for the SAFE
! lab implementation
```

```
!
crypto key generate rsa
ip ssh timeout 120
ip ssh authentication-retries 5
! Set passwords and access restrictions
!
service password-encryption
enable secret %Z<)|z9~zq
no enable password
!
!
access-list 99 permit host 10.3.8.254
access-list 99 deny any log
!
access-list 98 permit host 10.3.8.253
access-list 98 permit host 10.3.8.254
access-list 98 deny any log
!
line vty 0 4
access-class 99 in
login authentication default
password 0 X)[^j+#T98
exec-timeout 2 0
transport input ssh
transport output none
line con 0
login authentication no_tacacs
password 0 X)[^j+#T98
exec-timeout 2 0
transport input none
line aux 0
transport input none
password 0 X)[^j+#T98
no exec
!
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 with authentication and access control
!
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 10.3.4.4 key 1
!
```

```
access-list 96 permit host 10.3.4.4
access-list 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 10.3.8.253 single-connection
tacacs-server key SJj)j~t]6-
```

次のサンプルコマンドは、ネットワーク内のルータに対する OSPF（Open Shortest Path First）認証パラメータを定義します。この設定では、MD5（Message Digest 5）認証が使用されていることに注意してください。

```
interface FastEthernet1/0
ip address 10.3.3.3 255.255.255.0
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 8R%xi!0eUUxF
!
router ospf 1
log-adjacency-changes
area 0 authentication message-digest
network 10.3.3.0 0.0.0.255 area 1
network 10.3.4.0 0.0.0.255 area 1
```

スイッチ

次のサンプルコマンドは、実験に使用したほとんどの Catalyst(R) OS スイッチの基本設定オプションの大半を有効にするものです。Cisco IOS (R) スイッチは、ルータ設定とほぼ同じ設定を使用します。

```
! 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 10.3.4.4 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 10.3.8.253
```

```
set logging server 10.3.8.254
set logging timestamp enable
set snmp community read-only Txo~QbW3XM
set ip permit enable snmp
set ip permit 10.3.8.254 snmp

! Turn on AAA
!
set tacacs server 10.3.8.253 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 10.3.8.253 255.255.255.255 telnet
set ip permit 10.3.8.254 255.255.255.255 telnet
```

ホスト

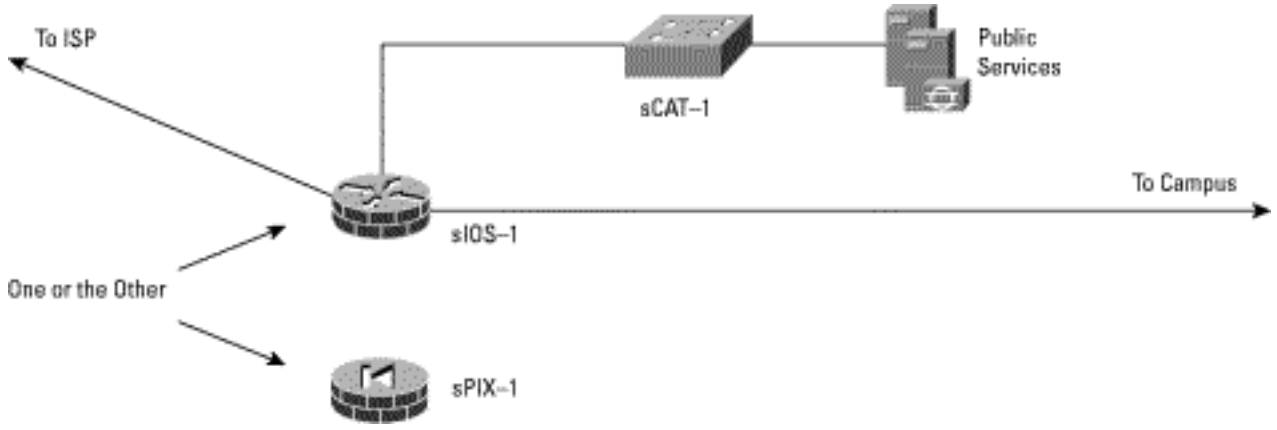
原則のセクションで検証したように、ホストの OS とアプリケーションには HIDS を実行し、最新のパッチと修正版を適用しています。この実験で使用した HIDS アプリケーションは、Entercept Security Technologies 社の Entercept アプリケーションです。この製品の詳細については http://www.entercept.com を参照してください。

小規模ネットワークの設定

以下に、SAFE 小規模ネットワークの設定スナップショットを示します。

企業インターネットモジュール

図 15: 小規模ネットワークにおける企業インターネットモジュールの詳細



使用した製品

- Cisco Catalyst レイヤ 2 スイッチ(sCAT-1)
- 3DES(Triple Data Encryption Standard)暗号化対応の Cisco IOS ルータ(sIOS-1)
- Cisco Secure PIX ファイアウォール(sPIX-1)
- Entercept HIDS

sIOS–1

次の設定スナップショットは、小規模ネットワークのエッジルータに設定し、このネットワークに対する双方向のトラフィックを制御するアクセスリストの詳細です。

注意: 小型のルータ設定には、リモートアクセス VPN 設定が含まれません。この機能は、早急に Cisco IOS ソフトウェアに追加される予定です。

```
! Basic IOS IDS configuration using syslog for reporting
!
ip audit attack action alarm drop reset
ip audit notify log
ip audit name alarm1 info action alarm
ip audit name alarm1 attack action alarm drop
!
! IPSec crypto configuration to remote branches of the small network
!
crypto isakmp policy 1
encr 3des
authentication pre-share
group 2
crypto isakmp key 7Q!r$y$+xE address 172.16.128.2
crypto isakmp key 7Q!r$y$+xE address 172.16.128.5
!
!
crypto ipsec transform-set remote1 esp-3des esp-sha-hmac
!
```

```
crypto map ent1 30 ipsec-isakmp
set peer 172.16.128.2
set transform-set remote1
match address 107
crypto map ent1 40 ipsec-isakmp
set peer 172.16.128.5
set transform-set remote1
match address 108
!
! The access-lists below allow both user traffic as well as management
! traffic to be encrypted
!
access-list 107 permit ip 10.4.0.0 0.0.255.255 10.5.0.0 0.0.255.255
access-list 107 permit ip host 10.4.1.253 host 172.16.128.2
access-list 108 permit ip 10.4.0.0 0.0.255.255 10.6.0.0 0.0.255.255
access-list 108 permit ip host 10.4.1.253 host 172.16.128.5
!
! Interface settings for the inside interface of the router. NAT, IOS IDS, and
! IOS firewall are enabled.
!
interface FastEthernet0/0
description Inside Interface
ip address 10.4.1.1 255.255.255.0
ip access-group 109 in
ip nat inside
ip inspect smbranch_fw in
ip audit alarm1 in
!
! Allow ICMP from within the small network out to the Internet
!
access-list 109 permit icmp any any echo
!
! Allow the internal DNS server to communicate with the public DNS server
!
access-list 109 permit udp host 10.4.1.201 host 10.4.2.50 eq domain
!
! Allow internal users access to the public services server for HTTP,
! SSL and FTP traffic.
!
access-list 109 permit tcp 10.4.0.0 0.0.255.255 host 10.4.2.50 eq www
access-list 109 permit tcp 10.4.0.0 0.0.255.255 host 10.4.2.50 eq 443
access-list 109 permit tcp 10.4.0.0 0.0.255.255 host 10.4.2.50 eq ftp
!
! Allow the internal mail server to communicate with the public mail server
!
access-list 109 permit tcp host 10.4.1.201 host 10.4.2.50 eq smtp
!
! Allow Telnet access from the management host to the sCAT-1 switch
!
access-list 109 permit tcp host 10.4.1.253 host 10.4.2.4 eq telnet
!
! Deny all other access to the public services segment
!
```

```
access-list 109 deny ip any 10.4.2.0 0.0.0.255
!
! Allow the sIOS-1 router and sCAT-2 switch to synchronize time
!
access-list 109 permit udp host 10.4.1.4 host 10.4.1.1 eq ntp
!
! Allow SSH access from the management host to the sIOS-1 router
!
access-list 109 permit tcp host 10.4.1.253 host 10.4.1.1 eq 22
!
! Allow established connections to the management host back to the sIOS-1 router
!
access-list 109 permit tcp host 10.4.1.253 eq tacacs host 10.4.1.1 established
!
! Necessary for TFTP access from the management host to the sIOS-1 router
!
access-list 109 permit udp host 10.4.1.253 gt 1023 host 10.4.1.1 gt 1023
!
! Block all other access to the inside interface on the sIOS-1 router from the
! internal network
!
access-list 109 deny ip 10.4.0.0 0.0.255.255 host 10.4.1.1
!
! Block all other access to the outside interface on the sIOS-1 router from the
! internal network
!
access-list 109 deny ip 10.4.0.0 0.0.255.255 host 172.16.132.2
!
! Allow all other internal devices access to the Internet
!
access-list 109 permit ip 10.4.0.0 0.0.255.255 any
!
! Block and log all other traffic
!
access-list 109 deny ip any any log
!
! Interface settings for the public services interface of the router. NAT, IOS IDS, and IOS firewall are enabled.
!
interface FastEthernet0/1
description DMZ Interface
ip address 10.4.2.1 255.255.255.0
ip access-group 105 in
no ip redirects
ip nat inside
ip inspect smbranch_fw in
ip audit alarm1 in
!
! Allow sCAT-1 switch to synchronize time with sIOS-1 router
!
access-list 105 permit udp host 10.4.2.4 host 10.4.2.1 eq ntp
!
! Allow TACACS+, TFTP, and syslog from the SCAT-1 switch to the
! management host
```

```
!
access-list 105 permit tcp host 10.4.2.4 host 10.4.1.253 eq tacacs
access-list 105 permit udp host 10.4.2.4 host 10.4.1.253 eq tftp
access-list 105 permit udp host 10.4.2.4 host 10.4.1.253 eq syslog
!
! Allow HIDS traffic from the public services server to
! the management host
!
access-list 105 permit tcp host 10.4.2.50 host 10.4.1.253 eq 5000
!
! Allow the public email server to send mail to the internal mail server
!
access-list 105 permit tcp host 10.4.2.50 host 10.4.1.201 eq smtp
!
! Deny all other connections originating from the public services segment
! to the internal network
!
access-list 105 deny ip any 10.4.0.0 0.0.255.255
!
! Permit all mail and DNS traffic originating from the public services
! server
!
access-list 105 permit tcp host 10.4.2.50 any eq smtp
access-list 105 permit udp host 10.4.2.50 any eq domain
!
! Deny all other traffic and log
!
access-list 105 deny ip any any log
!
! Interface settings for the public interface of the router. NAT, IOS IDS,
! IOS firewall, and IPSec are enabled.
!
interface Serial1/0
description Outside Interface
ip address 172.16.132.2 255.255.255.0
ip access-group 103 in
no ip redirects
ip nat outside
ip inspect smbranch_fw in
ip audit alarm1 in
crypto map ent1
!
! Allows traffic from remote sites to the small network. Only needed
! when small network functions as a headend for remote sites.
!
access-list 103 permit ip 10.5.0.0 0.0.255.255 10.4.0.0 0.0.255.255
access-list 103 permit ip 10.6.0.0 0.0.255.255 10.4.0.0 0.0.255.255
!
! RFC 1918 filtering. Note network 172.16.x.x was not included in the
! filter here since it is used to simulate the ISP in the lab.
!
access-list 103 deny ip 10.0.0.0 0.255.255.255 any
access-list 103 deny ip 192.168.0.0 0.0.255.255 any
```

```
!
! Allow any echo replies which originate from the 172.16.132.0
! network (NAT translated internal addresses) back.
!
access-list 103 permit icmp any 172.16.132.0 0.0.0.255 echo-reply
!
! Allow path MTU discovery (PMTUD) traffic.
!
access-list 103 permit icmp any 172.16.132.0 0.0.0.255 unreachable
!
! Allows IPSec traffic from remote sites to terminate on the sIOS-1
! router. Only needed when small network functions as a headend for
! remote sites.
!
access-list 103 permit esp host 172.16.128.2 host 172.16.132.2
access-list 103 permit udp host 172.16.128.2 host 172.16.132.2 eq isakmp
access-list 103 permit esp host 172.16.128.5 host 172.16.132.2
access-list 103 permit udp host 172.16.128.5 host 172.16.132.2 eq isakmp
!
!
! Allows management of remote sites. Only needed when small network
! functions as a headend for remote sites.
!
access-list 103 permit tcp host 172.16.128.2 host 10.4.1.253 eq tacacs
access-list 103 permit udp host 172.16.128.2 host 10.4.1.253 eq syslog
access-list 103 permit udp host 172.16.128.2 host 10.4.1.253 eq tftp
access-list 103 permit tcp host 172.16.128.5 host 10.4.1.253 eq tacacs
access-list 103 permit udp host 172.16.128.5 host 10.4.1.253 eq syslog
access-list 103 permit udp host 172.16.128.5 host 10.4.1.253 eq tftp
!
! Allow access to the public services server (via the NAT
! address of the server) for DNS, FTP, HTTP, SSL, and mail
! traffic
!
access-list 103 permit udp any host 172.16.132.50 eq domain
access-list 103 permit tcp any host 172.16.132.50 eq ftp
access-list 103 permit tcp any host 172.16.132.50 eq www
access-list 103 permit tcp any host 172.16.132.50 eq 443
access-list 103 permit tcp any host 172.16.132.50 eq smtp
!
! Deny all other traffic and log
!
access-list 103 deny ip any any log
!
! The following NAT configuration creates a pool of public addresses which
! are used by internal devices when they access the Internet
!
ip nat pool small_pool 172.16.132.101 172.16.132.150 netmask 255.255.255.0
ip nat inside source route-map nat_internet pool small_pool
!
! Static translation of the public services server to a registered
! address accessible from the Internet
!
```

```
ip nat inside source static 10.4.2.50 172.16.132.50
!
route-map nat_internet permit 10
match ip address 104
!
! Do not use NAT for internal devices communicating with other network
! 10.0.0.0 devices, or for management traffic. Use NAT for all internal
! devices communicating with the Internet.
!
access-list 104 deny ip 10.4.0.0 0.0.255.255 10.0.0.0 0.255.255.255
access-list 104 deny ip host 10.4.1.253 host 172.16.128.2
access-list 104 deny ip host 10.4.1.253 host 172.16.128.5
access-list 104 permit ip 10.4.1.0 0.0.0.255 any
!
```

ブランチとヘッドエンドの設定変更の比較

次の設定スナップショットは、冗長 IPSec-over-GRE VPN 接続によって、小規模ネットワークを大規模ネットワークのブランチとして設定するための変更コマンドの詳細です。

```
!
! Crypto Policy Settings
!
crypto isakmp policy 1
encr 3des
authentication pre-share
group 2
crypto isakmp key 7Q!r$y$+xE address 172.16.226.28
crypto isakmp key 7Q!r$y$+xE address 172.16.226.27
!
!
crypto ipsec transform-set 3dessha esp-3des esp-sha-hmac
mode transport
!
crypto map ent1 10 ipsec-isakmp
set peer 172.16.226.28
set transform-set 3dessha
match address 101
crypto map ent1 20 ipsec-isakmp
set peer 172.16.226.27
set transform-set 3dessha
match address 102
!
access-list 101 permit gre host 172.16.132.2 host 172.16.226.28
access-list 102 permit gre host 172.16.132.2 host 172.16.226.27
!
! GRE Tunnel Settings
!
interface Tunnel0
bandwidth 8
ip address 10.1.249.2 255.255.255.0
tunnel source 172.16.132.2
```

```
tunnel destination 172.16.226.27
crypto map ent1
!
interface Tunnel1
ip address 10.1.248.2 255.255.255.0
tunnel source 172.16.132.2
tunnel destination 172.16.226.28
crypto map ent1
!
! Crypto Map Application to Physical Interface
!
interface Serial1/0
ip address 172.16.132.2 255.255.255.0
ip access-group 103 in
crypto map ent1
!
! Access-list 103 would need to be modified to both the IPSec connections
! from the corporate headquarters, as well as the GRE traffic.
!
access-list 103 permit gre host 172.16.226.28 host 172.16.132.2
access-list 103 permit gre host 172.16.226.27 host 172.16.132.2
access-list 103 permit esp host 172.16.226.27 host 172.16.132.2
access-list 103 permit udp host 172.16.226.27 host 172.16.132.2 eq isakmp
access-list 103 permit esp host 172.16.226.28 host 172.16.132.2
access-list 103 permit udp host 172.16.226.28 host 172.16.132.2 eq isakmp
!
! Note that all configurations pertaining to the remote sites is removed
!
access-list 103 deny ip 10.0.0.0 0.255.255.255 any
access-list 103 deny ip 192.168.0.0 0.0.255.255 any
access-list 103 permit udp any host 172.16.132.50 eq domain
access-list 103 permit tcp any host 172.16.132.50 eq ftp
access-list 103 permit tcp any host 172.16.132.50 eq www
access-list 103 permit tcp any host 172.16.132.50 eq 443
access-list 103 permit tcp any host 172.16.132.50 eq smtp
access-list 103 permit icmp any 172.16.132.0 0.0.0.255 echo-reply
access-list 103 permit icmp any 172.16.132.0 0.0.0.255 unreachable
access-list 103 deny ip any any log
```

他のアクセスリストにも小さな変更を加える必要がありますが、ここには掲載しません。

sPIX-1

次の設定スナップショットは、小規模ネットワークのヘッドエンドデバイスとして PIX ファイアウォールを使用する場合のアクセスリストおよび暗号設定の詳細です。次のように設定した PIX ファイアウォールは、リモート拠点と通信し、ダイヤルイン IPSec VPN 接続を終端する機能を持ちます。

```
!
! Interface settings for the public interface of the firewall
!
ip address outside 172.16.144.3 255.255.255.0
access-group 103 in interface outside
!
```

```
! Allow encrypted traffic from remote sites and remote access users.
!
access-list 103 permit ip 10.5.0.0 255.255.0.0 10.4.0.0 255.255.0.0
access-list 103 permit ip 10.6.0.0 255.255.0.0 10.4.0.0 255.255.0.0
access-list 103 permit ip 10.4.3.0 255.255.255.0 10.4.0.0 255.255.0.0

! RFC 1918 filtering. Note network 172.16.x.x was not included in the
! filter here since it is used to simulate the ISP in the lab.
!
access-list 103 deny ip 10.0.0.0 255.0.0.0 any
access-list 103 deny ip 192.168.0.0 255.255.0.0 any
!
! Allow access to the public services server (via the NAT
! address of the server) for DNS, FTP, HTTP, SSL, and mail
! traffic
!
access-list 103 permit udp any host 172.16.144.50 eq domain
access-list 103 permit tcp any host 172.16.144.50 eq ftp
access-list 103 permit tcp any host 172.16.144.50 eq www
access-list 103 permit tcp any host 172.16.144.50 eq 443
access-list 103 permit tcp any host 172.16.144.50 eq smtp
!
! Allow echo reply generated from the internal network (via NAT translated
! addresses) back into the firewall
!
access-list 103 permit icmp any 172.16.144.0 255.255.255.0 echo-reply
!
! Allow path MTU discovery (PMTUD) traffic through the firewall.
!
access-list 103 permit icmp any 172.16.144.0 255.255.255.0 unreachable
!
! Allow syslog, TFTP, and TACACS+ management traffic in from remote sites.
!
access-list 103 permit udp host 172.16.128.2 host 172.16.144.51 eq syslog
access-list 103 permit udp host 172.16.128.2 host 172.16.144.51 eq tftp
access-list 103 permit tcp host 172.16.128.2 host 172.16.144.51 eq tacacs
access-list 103 permit udp host 172.16.128.5 host 172.16.144.51 eq syslog
access-list 103 permit udp host 172.16.128.5 host 172.16.144.51 eq tftp
access-list 103 permit tcp host 172.16.128.5 host 172.16.144.51 eq tacacs

!
! Interface settings for the private interface of the firewall
!
ip address inside 10.4.1.1 255.255.255.0
access-group 109 in interface inside
!
! Allow echo from internal devices
!
access-list 109 permit icmp any any echo
!
! Allow the internal DNS and mail server to communicate with the
! public DNS and mail server
!
```

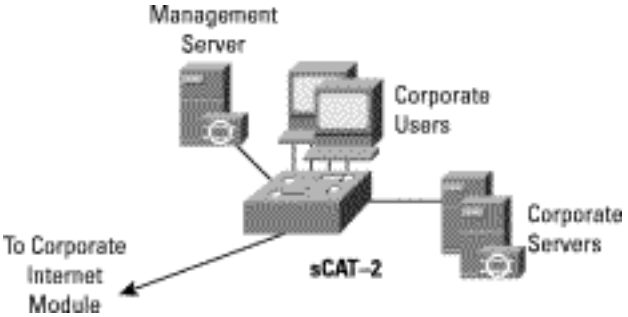
```
access-list 109 permit udp host 10.4.1.201 host 10.4.2.50 eq domain
access-list 109 permit tcp host 10.4.1.201 host 10.4.2.50 eq smtp
!
! Allow internal devices to access the public services server for web, FTP
! and SSL access
!
access-list 109 permit tcp 10.4.0.0 255.255.0.0 host 10.4.2.50 eq www
access-list 109 permit tcp 10.4.0.0 255.255.0.0 host 10.4.2.50 eq ftp
access-list 109 permit tcp 10.4.0.0 255.255.0.0 host 10.4.2.50 eq 443
!
! Allow Telnet access from the management host to the mCAT-1 switch
!
access-list 109 permit tcp host 10.4.1.253 host 10.4.2.4 eq telnet
!
! Block all other access to the public services segment
!
access-list 109 deny ip any 10.4.2.0 255.255.255.0
!
! Permit internal devices access to the Internet
!
access-list 109 permit ip 10.4.0.0 255.255.0.0 any
!
!
! Interface settings for the public services (DMZ) interface of the firewall
!
ip address pss 10.4.2.1 255.255.255.0
access-group 105 in interface pss
!
! Allow echo-replies from internal network back through firewall
!
access-list 105 permit icmp 10.4.2.0 255.255.255.0 10.4.1.0 255.255.255.0 echo-reply
!
! Allow TACACS+, TFTP, and syslog from the sCAT-1 switch to the management server
!
access-list 105 permit tcp host 10.4.2.4 host 10.4.1.253 eq tacacs
access-list 105 permit udp host 10.4.2.4 host 10.4.1.253 eq tftp
access-list 105 permit udp host 10.4.2.4 host 10.4.1.253 eq syslog
!
! Allow HIDS traffic from the public services server to the
! management server
!
access-list 105 permit tcp host 10.4.2.50 host 10.4.1.253 eq 5000
!
! Allow the public mail server to communicate with the internal mail server
!
access-list 105 permit tcp host 10.4.2.50 host 10.4.1.201 eq smtp
!
! Block all other access from this segment to the internal network
!
access-list 105 deny ip any 10.4.0.0 255.255.0.0
!
! Allow access from the public services server to the Internet for
! mail and DNS
```

```
!
access-list 105 permit tcp host 10.4.2.50 any eq smtp
access-list 105 permit udp host 10.4.2.50 any eq domain
!
! IDS Settings
!
ip audit name full info action alarm
ip audit name fullb attack action alarm drop
ip audit interface outside full
ip audit interface outside fullb
ip audit interface inside full
ip audit interface inside fullb
ip audit interface pss full
ip audit interface pss fullb
!
! The following NAT configuration creates a pool of public addresses which
! are used by internal devices when they access the Internet
!
global (outside) 1 172.16.144.201-172.16.144.220
!
nat (inside) 0 access-list nonat
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
nat (pss) 0 access-list nonat
!
! Static translation of the public services server to a registered address
! accessible from the Internet
!
static (pss,outside) 172.16.144.50 10.4.2.50 netmask 255.255.255.255 0 0
!
static (inside,pss) 10.4.1.253 10.4.1.253 netmask 255.255.255.255 0 0
static (inside,pss) 10.4.1.201 10.4.1.201 netmask 255.255.255.255 0 0
static (inside,outside) 172.16.144.51 10.4.1.253 netmask 255.255.255.255 0 0
!
! Access-list nonat determines what addresses use address translation
!
access-list nonat permit ip 10.4.0.0 255.255.0.0 10.5.0.0 255.255.0.0
access-list nonat permit ip 10.4.0.0 255.255.0.0 10.6.0.0 255.255.0.0
access-list nonat permit ip 10.4.1.0 255.255.255.0 10.4.3.0 255.255.255.0
access-list nonat permit ip 10.4.2.0 255.255.255.0 10.4.3.0 255.255.255.0
access-list nonat permit ip 10.4.1.0 255.255.255.0 10.4.2.0 255.255.255.0
!
! The following crypto settings are used when the firewall terminates VPN connections from the remote sites
!
no sysopt route dnat
crypto ipsec transform-set 3dessha esp-3des esp-sha-hmac
crypto ipsec transform-set remote1 esp-3des esp-sha-hmac
crypto dynamic-map vpnuser 20 set transform-set remote1
crypto map ent1 30 ipsec-isakmp
crypto map ent1 30 match address 107
crypto map ent1 30 set peer 172.16.128.2
crypto map ent1 30 set transform-set remote1
crypto map ent1 40 ipsec-isakmp
crypto map ent1 40 match address 108
```

```
crypto map ent1 40 set peer 172.16.128.5
crypto map ent1 40 set transform-set remote1
crypto map ent1 50 ipsec-isakmp dynamic vpnuser
crypto map ent1 client configuration address initiate
crypto map ent1 client authentication vpnauth
crypto map ent1 interface outside
!
access-list 107 permit ip 10.4.0.0 255.255.0.0 10.5.0.0 255.255.0.0
access-list 107 permit ip host 172.16.144.51 host 172.16.128.2
access-list 108 permit ip 10.4.0.0 255.255.0.0 10.6.0.0 255.255.0.0
access-list 108 permit ip host 172.16.144.51 host 172.16.128.5
!
isakmp enable outside
isakmp key 7Q!r$y$+xE address 172.16.128.5 netmask 255.255.255.255
isakmp key 7Q!r$y$+xE address 172.16.128.2 netmask 255.255.255.255
isakmp key 7Q!r$y$+xE address 172.16.226.28 netmask 255.255.255.255
isakmp key 7Q!r$y$+xE address 172.16.226.27 netmask 255.255.255.255
isakmp policy 1 authentication pre-share
isakmp policy 1 encryption 3des
isakmp policy 1 hash sha
isakmp policy 1 group 2
isakmp policy 1 lifetime 86400
!
! The following configuration block configures the PIX to terminate remote access
! VPN users
!
vpngroup VPN1 address-pool vpnpool
vpngroup VPN1 dns-server 10.4.1.201
vpngroup VPN1 default-domain safe-small.com
vpngroup VPN1 idle-time 1800
vpngroup VPN1 password Y0eS)3/i6y
ip local pool vpnpool 10.4.3.1-10.4.3.254
```

キャンパスモジュール

図 16:小規模ネットワークにおけるキャンパスモジュールの詳細



使用した製品

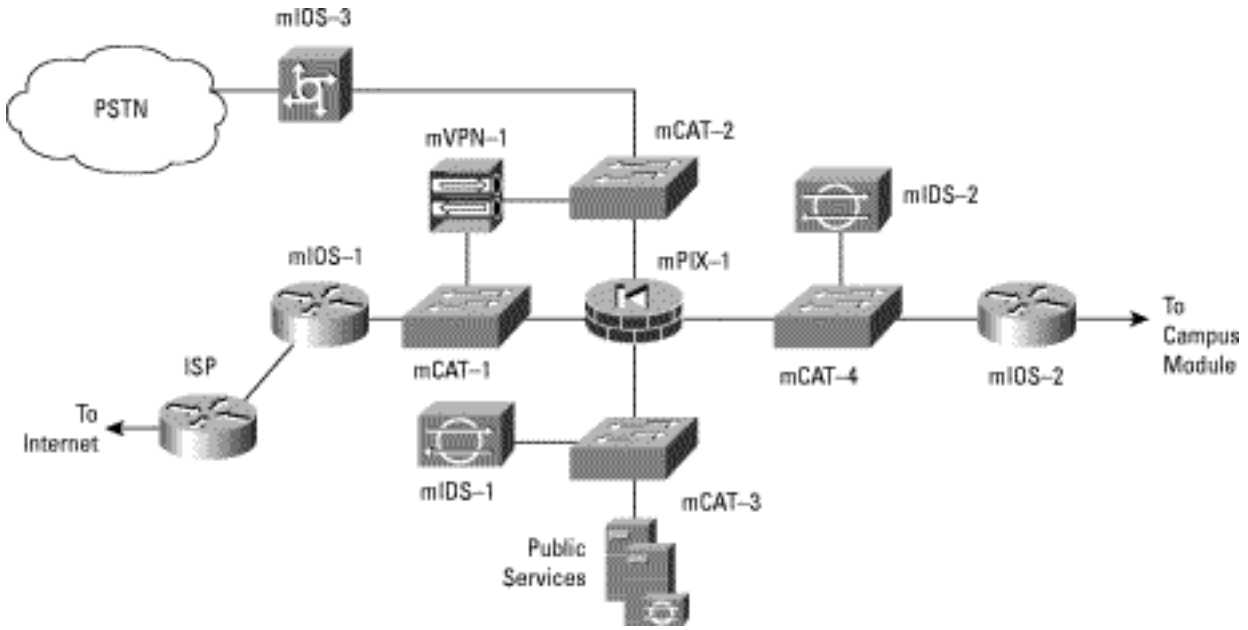
- Cisco Catalyst レイヤ 2 スイッチ（sCAT-2）
- Entercept HIDS
- Cisco Secure Access Control Server
- Cisco Secure Policy Manager Lite
- OpenSystems Private I システムログ分析ツール
- F-Secure SSH（Secure Shell Protocol）クライアント

中規模ネットワークの設定

以下に、SAFE 中規模ネットワークの各設定スナップショットを示します。特に指定のない限り、以下のスナップショットは、ヘッドエンドとして運用する中規模ネットワークの設定を表わします。

企業インターネットモジュール

図 17：中規模ネットワークにおける企業インターネットモジュールの詳細



使用した製品

- Cisco Catalyst レイヤ 2 スイッチ（mCAT-1～mCAT-4）
- 3DES 暗号化対応の Cisco IOS ルータ（mIOS-1 および mIOS-2）
- Cisco IOS Dial-Access Router（mIOS-3）
- Cisco VPN 3000 シリーズコンセントレータ（mVPN-1）
- Cisco Secure PIX ファイアウォール（mPIX-1）
- Cisco Secure IDS Sensors（mIDS-1 および mIDS-2）
- Entercept HIDS
- Baltimore MIMESweeper Email Filtering

mIOS-1

次の設定スナップショットは、中規模ネットワークのエッジルータ（mIOS-1）に実装し、ISP からこのネットワークに送られるトラフィックを制御するアクセスリストの詳細です。

```
interface FastEthernet0/0
ip address 172.16.240.2 255.255.255.0
ip access-group 112 in
no ip redirects

no cdp enable
!
interface Serial1/0
ip address 172.16.131.2 255.255.255.0
ip access-group 150 in
dsu bandwidth 44210
framing c-bit

no cdp enable
!
! RFC 1918 filtering. Note that network 172.16.0.0 was used for the simulated SAFE ISP
! network, and therefore has not been included in the RFC 1918 filtering here.
!
```

```
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
!
!
! Prevent any outside devices from spoofing an address that appears to originate from
! within the medium network.
!
access-list 150 deny ip 172.16.240.0 0.0.0.255 any
!
! Allow relevant IKE and ESP traffic to reach the VPN devices.
!
access-list 150 permit esp any host 172.16.240.3
access-list 150 permit udp any host 172.16.240.3 eq isakmp
access-list 150 permit esp host 172.16.128.2 host 172.16.240.1
access-list 150 permit udp host 172.16.128.2 host 172.16.240.1 eq isakmp
access-list 150 permit esp host 172.16.128.5 host 172.16.240.1
access-list 150 permit udp host 172.16.128.5 host 172.16.240.1 eq isakmp
!
!
! Restrict any other conversations to mIOS-1, mVPN-1, mPIX-1 and mCAT-1.
!
access-list 150 deny ip any host 172.16.240.3
access-list 150 deny ip any host 172.16.240.4
access-list 150 deny ip any host 172.16.240.2
access-list 150 deny ip any host 172.16.240.1
!
!
! Allow all other connections to the 172.16.240 subnet, since internal user devices
! translate to 172.16.240.0 addresses at the firewall as they access the Internet.
!
access-list 150 permit ip any 172.16.240.0 0.0.0.255
!
!
! Block and log all other attempted access.
!
access-list 150 deny ip any any log
!
!
```

次の設定スナップショットは、中規模ネットワークから ISP に送られるトラフィックをエッジルータ上で制御するアクセスリストの詳細です。

```
! Allow TCP sessions that originated from the router to the management hosts
! (TACACS+, etc.). Management hosts 172.16.240.151 and 172.16.240.152 are the
! NAT translated addresses at the firewall.
!
access-list 112 permit tcp host 172.16.240.151 host 172.16.240.2 established
access-list 112 permit tcp host 172.16.240.152 host 172.16.240.2 established
!
!
! Allow SSH connections originated from the management hosts to the router.
!
access-list 112 permit tcp host 172.16.240.151 host 172.16.240.2 eq 22
```

```
access-list 112 permit tcp host 172.16.240.152 host 172.16.240.2 eq 22
!
!
! Necessary for allowing TFTP back from the management host to the router.
!
access-list 112 permit udp host 172.16.240.151 host 172.16.240.2 gt 1024
!
!
! Allow other devices on the 172.16.240 subnet to synchronize clocks to this device.
!
access-list 112 permit udp 172.16.240.0 0.0.0.255 host 172.16.240.2 eq ntp
!
!
! Allow internal devices to ping the Internet.
!
access-list 112 permit icmp 172.16.240.0 0.0.0.255 any
!
!
! Block all other attempts to access this router and log.
!
access-list 112 deny ip any host 172.16.240.2 log
!
!
! Permit all access to the Internet from hosts with 172.16.240.0 addresses.
!
access-list 112 permit ip 172.16.240.0 0.0.0.255 any
!
!
```

mPIX-1

次のファイアウォールの設定スナップショットは、PIX ファイアウォール（mPIX-1）の各インターフェイスのセキュリティレベル、および各インターフェイスのアドレス割り当ての詳細です。

```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 pss security10
nameif ethernet3 vpn security15
!
ip address outside 172.16.240.1 255.255.255.0
ip address inside 10.3.4.1 255.255.255.0
ip address pss 10.3.6.1 255.255.255.0
ip address vpn 10.3.5.1 255.255.255.0
```

次のファイアウォールの設定スナップショットは、PIX ファイアウォールの NAT（ネットワークアドレス変換）設定の詳細です。

```
! In combination with the nonat access list, the below configuration does not allow
! NAT for sessions between internal devices (network 10.x.x.x to network 10.x.x.x), but
! allows NAT for sessions between internal or remote access devices and the Internet.
!
global (outside) 100 172.16.240.101-172.16.240.150 netmask 255.255.255.0
```

```
global (outside) 200 172.16.240.201-172.16.240.250 netmask 255.255.255.0
nat (inside) 0 access-list nonat
nat (inside) 100 10.0.0.0 255.0.0.0 0 0
nat (pss) 0 access-list nonat
nat (vpn) 200 10.3.7.0 255.255.255.0 0 0
static (inside,vpn) 10.3.0.0 10.3.0.0 netmask 255.255.0.0 0 0
static (inside,pss) 10.3.8.253 10.3.8.253 netmask 255.255.255.255 0 0
static (inside,pss) 10.3.8.254 10.3.8.254 netmask 255.255.255.255 0 0
!
!
! Translates the non-registered address of the public services server to a registered
! address, which can be accessed from the Internet.
!
static (pss,outside) 172.16.240.50 10.3.6.50 netmask 255.255.255.255 0 0
!
!
! Translates the non-registered addresses of the management hosts to registered
! addresses so that managed devices outside the firewall can initiate sessions
! to the management servers.
!
static (inside,outside) 172.16.240.151 10.3.8.254 netmask 255.255.255.255 0 0
static (inside,outside) 172.16.240.152 10.3.8.253 netmask 255.255.255.255 0 0
!
!
!
access-list nonat permit ip 10.0.0.0 255.0.0.0 10.0.0.0 255.0.0.0
access-list nonat deny ip 10.0.0.0 255.0.0.0 any
```

次の設定スナップショットは、PIX ファイアウォールに実装するアクセス制御の詳細です。アクセスリスト名は、受信方向のアクセス制御リスト（ACL）が設置された場所を表します。

アクセスリスト「out」は、ファイアウォールの外側（公開）インターフェイスの受信方向に設置されます。

```
! Allow encrypted traffic from remote sites.
!
access-list out permit ip 10.5.0.0 255.255.0.0 10.3.0.0 255.255.0.0
access-list out permit ip 10.6.0.0 255.255.0.0 10.3.0.0 255.255.0.0
!
! RFC 1918 filtering. Note that network 172.16.0.0 was used for the simulated SAFE
! ISP network, and therefore has not been included in the RFC 1918 filtering here.
!
access-list out deny ip 10.0.0.0 255.0.0.0 any
access-list out deny ip 192.168.0.0 255.255.0.0 any
!
! Allow external hosts access to the public services server for HTTP, SSL, FTP
! SMTP, and DNS.
!
access-list out permit tcp any host 172.16.240.50 eq www
access-list out permit tcp any host 172.16.240.50 eq 443
access-list out permit tcp any host 172.16.240.50 eq ftp
access-list out permit tcp any host 172.16.240.50 eq smtp
access-list out permit udp any host 172.16.240.50 eq domain
```

```
!
! Allow echo reply generated from the internal network (via NAT translated
! addresses) back into the firewall
!
access-list out permit icmp any 172.16.240.0 255.255.255.0 echo-reply
!
! Allow path MTU discovery (PMTUD) traffic through the firewall.
!
access-list out permit icmp any 172.16.240.0 255.255.255.0 unreachable
!
! Allow syslog, TFTP, and TACACS+ management traffic in from remote sites.
!
access-list out permit udp host 172.16.128.2 host 172.16.240.151 eq syslog
access-list out permit udp host 172.16.128.2 host 172.16.240.152 eq syslog
access-list out permit udp host 172.16.128.2 host 172.16.240.151 eq tftp
access-list out permit tcp host 172.16.128.2 host 172.16.240.152 eq tacacs
access-list out permit udp host 172.16.128.5 host 172.16.240.151 eq syslog
access-list out permit udp host 172.16.128.5 host 172.16.240.152 eq syslog
access-list out permit udp host 172.16.128.5 host 172.16.240.151 eq tftp
access-list out permit tcp host 172.16.128.5 host 172.16.240.152 eq tacacs
!
! Permit syslog, TFTP, and TACACS+ which originates from the mIOS-1 router
! and the mCAT-1 switch to the management hosts.
!
access-list out permit udp host 172.16.240.2 host 172.16.240.151 eq syslog
access-list out permit udp host 172.16.240.2 host 172.16.240.152 eq syslog
access-list out permit udp host 172.16.240.2 host 172.16.240.151 eq tftp
access-list out permit tcp host 172.16.240.2 host 172.16.240.152 eq tacacs
access-list out permit udp host 172.16.240.4 host 172.16.240.151 eq syslog
access-list out permit udp host 172.16.240.4 host 172.16.240.152 eq syslog
access-list out permit udp host 172.16.240.4 host 172.16.240.151 eq tftp
access-list out permit tcp host 172.16.240.4 host 172.16.240.152 eq tacacs
!
```

アクセスリスト「in」は、ファイアウォールの内側（プライベート）インターフェイスの受信方向に設置されます。

```
! Allow echo from the inside network.
!
access-list in permit icmp any any echo
!
!
! Allow the internal DNS server to query the external DNS server for name
! translation.
!
access-list in permit udp host 10.3.2.50 host 10.3.6.50 eq domain
!
!
! Allow internal corporate users web, SSL, and FTP access to the external public
! services server.
!
access-list in permit tcp 10.0.0.0 255.0.0.0 host 10.3.6.50 eq www
access-list in permit tcp 10.0.0.0 255.0.0.0 host 10.3.6.50 eq 443
```

```
access-list in permit tcp 10.0.0.0 255.0.0.0 host 10.3.6.50 eq ftp
!
!
! Allow mail transfer from the external mail server to the internal mail
! server.
!
access-list in permit tcp host 10.3.2.50 host 10.3.6.50 eq smtp
!
!
! Allow Telnet access from the mgmt hosts to the mCAT-2 switch (does not support ! SSH) on the public services segment.
!
access-list in permit tcp host 10.3.8.253 host 10.3.6.4 eq telnet
access-list in permit tcp host 10.3.8.254 host 10.3.6.4 eq telnet
!
!
! Deny all other access to the public services segment from the internal network.
!
access-list in deny ip any 10.3.6.0 255.255.255.0
!
!
! Permit all internal users access to the Internet.
!
access-list in permit ip 10.0.0.0 255.0.0.0 any
!
```

アクセスリスト「pss」は、ファイアウォールの公開サービスセグメント側インターフェイスの受信方向に設置されます。

```
! Allow syslog, TACAS+, and TFTP originated from the mCAT-2 switch to
! the management hosts.
!
access-list pss permit udp host 10.3.6.4 host 10.3.8.254 eq syslog
access-list pss permit udp host 10.3.6.4 host 10.3.8.253 eq syslog
access-list pss permit tcp host 10.3.6.4 host 10.3.8.253 eq tacacs
access-list pss permit udp host 10.3.6.4 host 10.3.8.254 eq tftp
!
!
! Allow the mCAT-2 switch to synchronize time with the internal router
! mIOS-2.
!
access-list pss permit udp host 10.3.6.4 host 10.3.4.4 eq ntp
!
!
! Allow HIDS traffic from the public services host to the
! network management host.
!
access-list pss permit tcp host 10.3.6.50 host 10.3.8.253 eq 5000
!

! Allow mail originated from the public services host (external mail server)
! to the corporate intranet services host (internal mail server).
!
access-list pss permit tcp host 10.3.6.50 host 10.3.2.50 eq smtp
```

```
!
!
! Deny all other traffic destined for addresses on the internal network.
!
access-list pss deny ip any 10.3.0.0 255.255.0.0
!
.
!
! Allow mail and DNS generated by the public services host to the Internet.
!
access-list pss permit tcp host 10.3.6.50 any eq smtp
access-list pss permit udp host 10.3.6.50 any eq domain
!
```

アクセスリスト「vpn」は、ファイアウォールのリモートアクセス VPN セグメント側インターフェイスの受信方向に設置されます。リモート VPN ユーザには、アクセス制御サーバで定義されたアドレスプールから、10.3.7.0 サブネット内のアドレスが割り当てられます。リモート ダイアルインユーザには、10.3.8.0 サブネット内のアドレスが割り当てられます。

```
! Allow remote users web, SSL, and FTP access only to the public services server.
!
access-list vpn permit tcp 10.3.7.0 255.255.255.0 host 10.3.6.50 eq www
access-list vpn permit tcp 10.3.8.0 255.255.255.0 host 10.3.6.50 eq www
access-list vpn permit tcp 10.3.7.0 255.255.255.0 host 10.3.6.50 eq 443
access-list vpn permit tcp 10.3.8.0 255.255.255.0 host 10.3.6.50 eq 443
access-list vpn permit tcp 10.3.7.0 255.255.255.0 host 10.3.6.50 eq ftp
access-list vpn permit tcp 10.3.8.0 255.255.255.0 host 10.3.6.50 eq ftp
access-list vpn deny ip 10.3.7.0 255.255.255.0 10.3.6.0 255.255.255.0
access-list vpn deny ip 10.3.8.0 255.255.255.0 10.3.6.0 255.255.255.0
!
!
! Allow remote users access to the rest of the internal network and the Internet.
!
access-list vpn permit ip 10.3.7.0 255.255.255.0 any
access-list vpn permit ip 10.3.8.0 255.255.255.0 any
!
!
! Permit syslog, TFTP, and TACAS+ which originates from the VPN concentrator,
! mVPN-1, to the management hosts.
!
access-list vpn permit udp host 10.3.5.5 host 10.3.8.254 eq tftp
access-list vpn permit udp host 10.3.5.5 host 10.3.8.254 eq syslog
access-list vpn permit udp host 10.3.5.5 host 10.3.8.253 eq syslog
access-list vpn permit tcp host 10.3.5.5 host 10.3.8.253 eq tacacs
!
!
! Allow the VPN concentrator to synchronize time with the
! internal router, mIOS-2.
!
access-list vpn permit udp host 10.3.5.5 host 10.3.4.4 eq ntp
!
!
! Permit RADIUS authentication data which originates from the VPN concentrator to
! the management host.
```

```
!
access-list vpn permit udp host 10.3.5.5 host 10.3.8.253 eq 1645
!
!
! Permit syslog, TFTP, and TACAS+ which originate from the dial-in access
! router, mIOS-3, to the management hosts.
!
access-list vpn permit udp host 10.3.5.2 host 10.3.8.254 eq tftp
access-list vpn permit udp host 10.3.5.2 host 10.3.8.254 eq syslog
access-list vpn permit udp host 10.3.5.2 host 10.3.8.253 eq syslog
access-list vpn permit tcp host 10.3.5.2 host 10.3.8.253 eq tacacs
!
!
! Allow the dial-in access router, mIOS-3, to synchronize time with the
! internal router, mIOS-2.
!
access-list vpn permit udp host 10.3.5.2 host 10.3.4.4 eq ntp
!
!
! Permit syslog, TFTP, and TACAS+ which originates from the mcAT-3 switch
! to the management hosts.
!
access-list vpn permit udp host 10.3.5.4 host 10.3.8.254 eq tftp
access-list vpn permit udp host 10.3.5.4 host 10.3.8.254 eq syslog
access-list vpn permit udp host 10.3.5.4 host 10.3.8.253 eq syslog
access-list vpn permit tcp host 10.3.5.4 host 10.3.8.253 eq tacacs
!
!
! Allow the mCAT-3 switch to synchronize time with the
! internal router mIOS-2.
!
access-list vpn permit udp host 10.3.5.4 host 10.3.4.4 eq ntp
!
!
```

VPN に関する考察

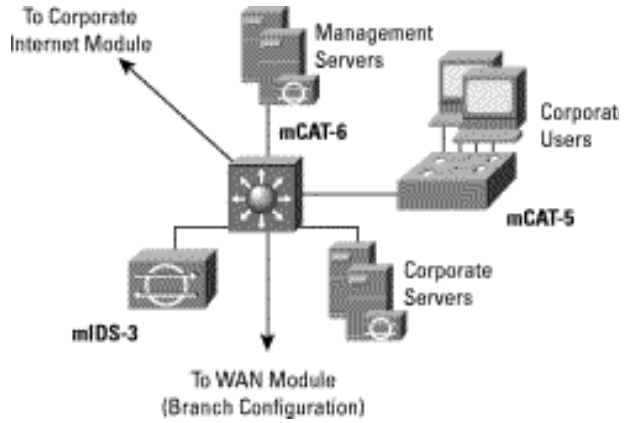
次の設定は、リモート拠点への拠点間 IPSec VPN を有効にするために追加します。

```
! Ensures both user and management traffic is encrypted to the first remote device.
!
access-list remote1 permit ip 10.3.0.0 255.255.0.0 10.5.0.0 255.255.0.0
access-list remote1 permit ip host 172.16.240.151 host 172.16.128.2
access-list remote1 permit ip host 172.16.240.152 host 172.16.128.2
!
!
! Ensures both user and management traffic is encrypted to the second remote device.
!
access-list remote2 permit ip 10.3.0.0 255.255.0.0 10.6.0.0 255.255.0.0
access-list remote2 permit ip host 172.16.240.151 host 172.16.128.5
access-list remote2 permit ip host 172.16.240.152 host 172.16.128.5
!
```

```
!
! Defines crypto map and applies it to the outside interface.
!
crypto ipsec transform-set 3dessha esp-3des esp-sha-hmac
crypto map remote1 10 ipsec-isakmp
crypto map remote1 10 match address remote1
crypto map remote1 10 set peer 172.16.128.2
crypto map remote1 10 set transform-set 3dessha
crypto map remote1 20 ipsec-isakmp
crypto map remote1 20 match address remote2
crypto map remote1 20 set peer 172.16.128.5
crypto map remote1 20 set transform-set 3dessha
crypto map remote1 interface outside
!
!
! Defines the use of IKE using pre-shared keys.
!
isakmp enable outside
isakmp key 7Q!r$y$+xE address 172.16.128.2 netmask 255.255.255.255
isakmp key 7Q!r$y$+xE address 172.16.128.5 netmask 255.255.255.255
isakmp identity address
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption 3des
isakmp policy 10 hash sha
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400
!
```

キャンパスモジュール

図 18：中規模ネットワークにおけるキャンパスモジュールの詳細



使用した製品

- Cisco Catalyst レイヤ 3 スイッチ（mCAT-6）
- Cisco Catalyst レイヤ2スイッチ（mCAT-5）
- Cisco Secure IDS センサ（mIDS-3）
- Entercept HIDS
- Cisco Secure Policy Manager
- Cisco Secure Access Control Server
- CiscoWorks 2000
- OpenSystems Private I システムログ分析ツール
- F-Secure SSH クライアント
- RSA SecureID OTP システム

次の設定スナップショットは、Catalyst レイヤ 3 スイッチに実装するアクセスリストの詳細です。このアクセスリストは、管理ホストの仮想 LAN（VLAN）へのアクセスを制御し、公開サーバ VLAN とビルディングスイッチ VLAN に対して RFC 2827 フィルタリングを実行します。VLAN 10は、企業ユーザのサブネットを定義します。VLAN 11 は、企業イントラネットサーバのサブネットを定義します。VLAN 12 および 13 は、それぞれ企業インターネットと WAN モジュールに接続します。最後に、VLAN 99 は管理ホストのサブネットを定義します。

```
mCAT-6
! Corporate user VLAN.
!
interface Vlan10
ip address 10.3.1.1 255.255.255.0
ip access-group 101 in
no ip redirects
no cdp enable
!
!
! Corporate intranet server VLAN.
!
interface Vlan11
ip address 10.3.2.1 255.255.255.0
ip access-group 102 in
no ip redirects
no cdp enable
!
!
interface Vlan12
ip address 10.3.3.1 255.255.255.0
no ip redirects
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 7 134E031F4158140119
no cdp enable
!
interface Vlan13
ip address 10.3.9.1 255.255.255.0
no ip redirects
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 7 024D105641521F0A7E
no cdp enable
!
! Management host VLAN.
!
interface Vlan99
ip address 10.3.8.1 255.255.255.0
ip access-group 103 out
no ip redirects
no cdp enable
!
!
! RFC 2827 filtering on corporate user VLAN.
!
access-list 101 permit ip 10.3.1.0 0.0.0.255 any
access-list 101 deny ip any any
!
!
! RFC 2827 filtering on corporate intranet server VLAN.
!
access-list 102 permit ip 10.3.2.0 0.0.0.255 any
access-list 102 deny ip any any log
```

```
!
!
! Example filtering for access to the management subnet (not complete).
!
access-list 103 permit udp host 10.3.2.50 eq domain host 10.3.8.253
access-list 103 permit udp host 10.3.2.50 eq domain host 10.3.8.254
access-list 103 permit tcp host 10.3.2.50 eq www host 10.3.8.253 established
access-list 103 permit tcp host 10.3.2.50 eq www host 10.3.8.254 established
access-list 103 permit tcp host 10.3.2.50 eq ftp host 10.3.8.253 established
access-list 103 permit tcp host 10.3.2.50 eq ftp host 10.3.8.254 established
access-list 103 permit tcp host 10.3.2.50 eq ftp-data host 10.3.8.253
access-list 103 permit tcp host 10.3.2.50 eq ftp-data host 10.3.8.254
access-list 103 permit tcp host 10.3.2.50 host 10.3.8.253 eq 5000
access-list 103 permit udp host 10.3.1.4 host 10.3.8.253 eq syslog
access-list 103 permit udp host 10.3.1.4 host 10.3.8.254 eq syslog
access-list 103 permit tcp host 10.3.1.4 host 10.3.8.253 eq tacacs
access-list 103 permit udp host 10.3.1.4 host 10.3.8.254 eq tftp
access-list 103 permit udp host 10.3.1.4 host 10.3.8.254 gt 1023
access-list 103 permit udp host 10.3.1.4 eq snmp host 10.3.8.254
access-list 103 permit tcp host 10.3.1.4 eq telnet host 10.3.8.253 established
access-list 103 permit tcp host 10.3.1.4 eq telnet host 10.3.8.254 established
access-list 103 deny ip any any
!
```

ブランチとヘッドエンドの比較

次の設定は、中規模ネットワークをヘッドエンドとして構成する場合にコアスイッチのアクセスリストに追加して、リモートに管理されるデバイスから管理ホストに向けて送信される設定およびセキュリティ管理トラフィックを許可します。

```
access-list 103 permit udp host 172.16.128.5 host 10.3.8.253 eq syslog
access-list 103 permit udp host 172.16.128.5 host 10.3.8.254 eq syslog
access-list 103 permit tcp host 172.16.128.5 host 10.3.8.253 eq tacacs
access-list 103 permit udp host 172.16.128.5 host 10.3.8.254 eq tftp
access-list 103 permit udp host 172.16.128.5 host 10.3.8.254 gt 1023
access-list 103 permit tcp host 172.16.128.5 eq 22 host 10.3.8.253 established
access-list 103 permit tcp host 172.16.128.5 eq 22 host 10.3.8.254 established
access-list 103 permit tcp host 172.16.128.5 eq 443 host 10.3.8.253 established
access-list 103 permit tcp host 172.16.128.5 eq 443 host 10.3.8.254 established
access-list 103 permit udp host 172.16.128.2 host 10.3.8.253 eq syslog
access-list 103 permit udp host 172.16.128.2 host 10.3.8.254 eq syslog
access-list 103 permit tcp host 172.16.128.2 host 10.3.8.253 eq tacacs
access-list 103 permit udp host 172.16.128.2 host 10.3.8.254 eq tftp
access-list 103 permit udp host 172.16.128.2 host 10.3.8.254 gt 1023
access-list 103 permit tcp host 172.16.128.2 eq 22 host 10.3.8.253 established
access-list 103 permit tcp host 172.16.128.2 eq 22 host 10.3.8.254 established
```

mCAT-5

次の設定スナップショットは、このモジュール内のレイヤ 2 スイッチに対する VLAN 設定の一部を示します。未使用ポートを無効にしていることに注目してください。コアスイッチへのアップリンク以外の全ポートに、プライベート VLAN を使用しています。

```
! User workstation ports.
!
interface FastEthernet0/1
port protected
switchport access vlan 99
no cdp enable
!
interface FastEthernet0/2
port protected
switchport access vlan 99
no cdp enable
!
!
! Unused ports.
!
interface FastEthernet0/3
port protected
shutdown
no cdp enable
!
interface FastEthernet0/4
port protected
shutdown
no cdp enable
!
!
! Uplink to core switch mCAT-1
!
interface GigabitEthernet0/1
switchport access vlan 99
no cdp enable
!
!
!
! Management interface to the switch.
!
interface VLAN99
ip address 10.3.1.4 255.255.255.0
no ip directed-broadcast
no ip route-cache
!
```

WAN モジュール

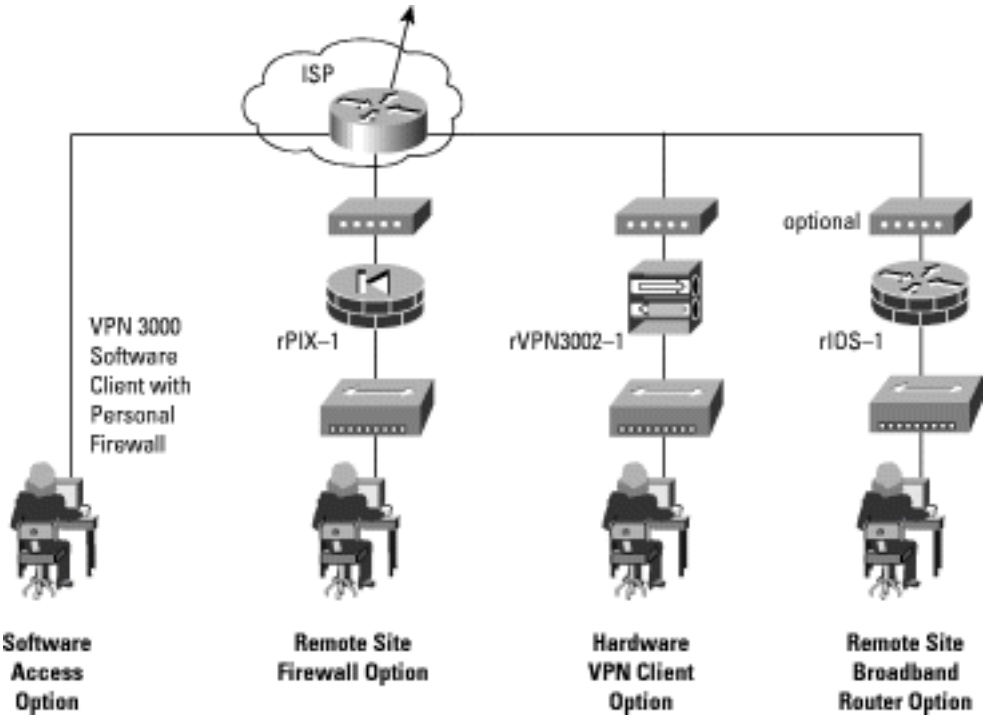
図 19：WAN モジュールの詳細

使用した製品

- Cisco IOS ルータ（mIOS-4）

リモートユーザ設計

図 20：リモートユーザ設計の詳細



使用した製品

- 3DES 暗号化対応の Cisco IOS ルータ（rIOS-1）
- Cisco VPN 3002 ハードウェア クライアント（rVPN3002-1）
- Cisco Secure PIX ファイアウォール（rPIX-1）
- Cisco VPN 3000 ソフトウェア クライアント
- Cisco MicroHub（またはレイヤ 3 デバイスに統合）
- Zone Alarm Pro Personal Firewall

以下の設定スナップショットは、SAFE リモートユーザ設計の一部を示します。

rIOS-1（リモート拠点ルータ オプション）

次に、企業本社に戻る IPSec トンネルの設定を示します。

```
crypto isakmp policy 1
encr 3des
authentication pre-share
group 2
crypto isakmp key 7Q!r$y$+xE address 172.16.240.1
!
```

```
!
crypto ipsec transform-set 3dessha esp-3des esp-sha-hmac
!
crypto map remote1 10 ipsec-isakmp
set peer 172.16.240.1
set transform-set 3dessha
match address 101
!
!
! The first lines of the following access-list specifies all traffic from
! network 10.5.0.0 to networks 10.3.0.0 will be encrypted.
!
! The last two lines of the access-list allow encryption of all configuration and
! security management traffic from the remote site router to the headquarters
! management hosts.
!
access-list 101 permit ip 10.5.0.0 0.0.255.255 10.3.0.0 0.0.255.255
access-list 101 permit ip host 172.16.128.2 host 172.16.240.151
access-list 101 permit ip host 172.16.128.2 host 172.16.240.152
!
!
```

次に、ルータのプライベート側（FastEthernet0/0）と公開側（FastEthernet0/1）に設定するアクセス制御、およびこれらのインターフェイスへの Cisco IOS ファイアウォールの適用を示します。

```
interface FastEthernet0/0
ip address 10.5.1.2 255.255.255.0
ip access-group 105 in
ip nat inside
ip inspect remote_fw in
!
interface FastEthernet0/1
ip address 172.16.128.2 255.255.255.0
ip access-group 102 in
ip nat outside
crypto map remote1
!
! IKE and ESP traffic must be allowed from the headquarters IPSec peer. All
! traffic from network 10.5.0.0 to networks 10.3.0.0 must also
! be allowed. Finally, traffic from the management hosts is allowed.
!
access-list 102 permit ip 10.3.0.0 0.0.255.255 10.5.0.0 0.0.255.255
access-list 102 deny ip 10.0.0.0 0.255.255.255 any
access-list 102 deny ip 192.168.0.0 0.0.255.255 any
access-list 102 permit icmp any host 172.16.128.2 echo-reply
access-list 102 permit icmp any host 172.16.128.2 unreachable
access-list 102 permit esp host 172.16.240.1 host 172.16.128.2
access-list 102 permit udp host 172.16.240.1 host 172.16.128.2 eq isakmp
access-list 102 permit tcp host 172.16.240.151 host 172.16.128.2 eq 22
access-list 102 permit tcp host 172.16.240.152 host 172.16.128.2 eq 22
access-list 102 permit tcp host 172.16.240.152 eq tacacs host 172.16.128.2
access-list 102 permit udp host 172.16.240.151 host 172.16.128.2 gt 1023
access-list 102 deny ip any any log
```

```
!
!
! RFC 2827 filtering only allows 10.5.0.0 addresses to access both the corporate
! headquarters and the Internet.
!
access-list 105 permit ip 10.5.0.0 0.0.255.255 any
access-list 105 deny ip any any log
!
```

次に、ルータに適用する多対 1 の NAT 設定を示します。リモート拠点からインターネットに接続する全デバイスは、ルータの公開アドレスを使用します。

```
ip nat pool remote_pool 172.16.128.2 172.16.128.2 netmask 255.255.255.0
ip nat inside source route-map nat_internet pool remote_pool
!
route-map nat_internet permit 10
match ip address 104
!
access-list 104 deny ip 10.5.0.0 0.0.255.255 10.0.0.0 0.255.255.255
access-list 104 permit ip 10.5.0.0 0.0.255.255 any
!
```

rPIX-1（リモート拠点ファイアウォール オプション）

次に、企業本社に戻る IPSec トンネルの設定を示します。

```
crypto ipsec transform-set 3dessha esp-3des esp-sha-hmac
crypto map remote1 10 ipsec-isakmp
crypto map remote1 10 match address remote1
crypto map remote1 10 set peer 172.16.240.1
crypto map remote1 10 set transform-set 3dessha
crypto map remote1 interface outside
isakmp enable outside
isakmp key 7Q!r$y$+xE address 172.16.240.1 netmask 255.255.255.255
isakmp identity address
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption 3des
isakmp policy 10 hash sha
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400
!
! The first line of the following access-list specifies all traffic from
! network 10.6.0.0 to networks 10.3.0.0 will be encrypted.
!
! The last two lines of the access-list allow encryption of all configuration and
! security management traffic from the remote site firewall to the headquarters
! management hosts.
!
access-list remote1 permit ip 10.6.0.0 255.255.0.0 10.3.0.0 255.255.0.0
access-list remote1 permit ip host 172.16.128.5 host 172.16.240.151
access-list remote1 permit ip host 172.16.128.5 host 172.16.240.152
!
```

次に、ファイアウォールのプライベート側(inside)と公開側(outside)に対するアドレス割り当てとアクセス制御を示します。

```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
!
ip address outside 172.16.128.5 255.255.255.0
ip address inside 10.6.1.1 255.255.255.0
!
access-group out in interface outside
access-group in in interface inside
!
! RFC 2827 filtering only allows 10.6.0.0 addresses to access both the corporate
! headquarters and the Internet.
!
access-list in permit ip 10.6.0.0 255.255.0.0 any
!
! Allows encrypted traffic from corporate headquarters.
!
access-list out permit ip 10.3.0.0 255.255.0.0 10.6.0.0 255.255.0.0
!
! RFC 1918 filtering. Note network 172.16.x.x was not included in the
! filter here since it is used to simulate the ISP in the lab.
!
access-list out deny ip 10.0.0.0 255.0.0.0 any
access-list out deny ip 192.168.0.0 255.255.0.0 any
!
! Allow echo replies and path MTU discovery (PMTU) traffic.
!
access-list out permit icmp any host 172.16.128.5 echo-reply
access-list out permit icmp any host 172.16.128.5 unreachable
!
! Allow ESP and IKE traffic from the corporate headquarters peer.
!
access-list out permit esp host 172.16.240.1 host 172.16.128.5
access-list out permit udp host 172.16.240.1 host 172.16.128.5 eq isakmp
```

次に、ファイアウォールに適用する多対 1 の NAT 設定を示します。リモート拠点からインターネットに接続する全デバイスは、ファイアウォールの公開アドレスを使用します。

```
global (outside) 100 interface
nat (inside) 0 access-list nonat
nat (inside) 100 10.6.1.0 255.255.255.0 0 0
!
! The access-list prevents any traffic destined for the corporate site from using
! address translation.
!
access-list nonat permit ip 10.6.0.0 255.255.0.0 10.0.0.0 255.0.0.0
access-list nonat deny ip 10.6.0.0 255.255.0.0 any
!
```

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

インターネットは、私達の生活や仕事の進め方を常に変化させています。こうした変化は、現在利用されている用途（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、拡張通信オプションなど）、未利用の用途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伴い、個人データ、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。これらに対し、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 つは、インターネットの遍在性です。現在、無数のデバイスがインターネットに接続され、その経路上にはさらに多数のデバイスが存在します。これに従い、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、インターネットの遍在性は、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だけで、数千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。

もう 1 つは、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であれば、一般に配布できるような使いやすいアプリケーションを開発できます。パブリックドメインで入手可能なハッカーツールの中には、IP アドレスかホスト名さえ分かれば、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場合、TCP/IP プロトコルに固有のいくつかの限界を理解することが重要となります。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、政府機関や大学同士をリンクするものでした。当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、初期のインターネットプロトコル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）が提案された現在になってようやく、IP を安全に配置するためのツールが利用できるようになりました。特定の IP セキュリティ規定が初めから設計されていないため、IP 固有のリスクを軽減するためのネットワークセキュリティの慣行、サービス、および製品によって IP の実装を補うことが重要となります。以下に、IP ネットワークで一般的に見受けられる攻撃の種類と、これらの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回線上で受信した全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、特定のコリジョンドメイン内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。スニファは現在、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（Telnet、FTP、SMTP、POP3 など）はデータを平文で送信するため、パケットスニファがユーザ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提供してしまうことがあります。

ユーザ名とパスワードの取得に関する重大な問題の 1 つに、多くの場合、ユーザがログイン名とパスワードを複数のアプリケーションやシステム間で再使用することがあります。実際に多くのユーザは、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対し、パスワードを 1 つしか使用していません。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利用して、企業内または外部の他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バックドアとしていつでも使用できる新規アカウントを作成します。

パケットスニファの脅威を軽減するには、以下のいくつかの方法があります。

- **認証** - 強力な認証の使用は、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。強力な認証は、容易に攻略できないユーザ認証手段として広く定義できます。強力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 要素認証の一種です。2 要素認証では、あるものを使用すると同時に、あるものを知っている必要があります。たとえば、ATM（現金自動預け払い機）にはこの 2 要素認証方式が使用されています。ATM で取引する顧客は、ATM カードを所有すると同時に、個人識別番号（PIN）を知っている必要があります。OTP では、デバイスまたはソ

フトウェアアプリケーションの認証に、PIN とトークンカードが必要となります。トークンカードは、一見してランダムな新規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たとしても、そのパスワードはすでに失効しているため、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** - ユーザ環境からパケットスニファに反撃するためのもう 1 つの方法は、スイッチ型インフラの配置です。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なくなります。スイッチ型インフラは、パケットスニファ自体の脅威は当然排除できませんが、その効果を大幅に減らすことができます。
- **スニファ防止ツール** - 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、脅威を完全に排除できるわけではありませんが、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「スニファ防止」機能は、ホストからの応答時間の変化を検知して、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、Security Software Technologies 社の AntiSniff があります。この製品についての詳細は、次の URL を参照してください。
  http://www.securitysoftwaretech.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、無意味なものとすることです。通信チャネルを暗号技術的に安全化すれば、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。シスコが配備するネットワークレベルの暗号技術は、IP セキュリティ（IPSec）に基づきます。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。ネットワーク管理用の暗号プロトコルには、他に SSH（Secure Shell）や 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、信頼あるコンピュータによる対話を装っ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、ネットワーク内の信頼ある 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特定リソースへのアクセス権限を持つ外部 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、しばしば他の攻撃の起点となります。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 攻撃を開始する場合があります。

IP スプーフィング攻撃は通常、クライアント／サーバ型のアプリケーション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、悪意あるデータまたはコマンドを挿入する行為に限定されています。双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 アドレスを指すように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。ハッカーのもう 1 つの手段として、アプリケーションからの応答をいっさい考慮しないこともあります。ハッカーがシステムから機密ファイルを入手しようとする場合、アプリケーションからの応答は重要でないからです。

しかし、何らかの方法により、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変更できた場合、ハッカーはスプーフィングしたアドレス宛のネットワークパケットをすべて受信し、信頼されたユーザと全く同様に応答できるようになります。

以下の方法によって 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設定することです。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存在すべき送信元アドレスを使っているにもかかわらず、外部ネットワークからくるすべてのトラフィックを拒否するようにアクセス制御を設定します。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、信頼できるアドレスが内部アドレスだけである場合です。信頼できるアドレスが外部アドレスにも含まれる場合、この方法は効果がありません。
- **RFC 2827 フィルタリング** - ネットワークから外部に送られるトラフィックに対し、送信元アドレスが組織固有の IP 範囲内にないトラフィックを防ぐことで、ネットワークユーザが他のネットワークをスプーフィングできないようにすることもできます。この種のフィルタリングは ISP 側でも実装でき、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に対して期待される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制限できます。ただし、すべての ISP がこの種のフィルタリングを実装しない限り、その効果は非常に小さくなります。また、フィルタリングするデバイスからの距離が遠くなるほど、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

を実施するには、メジャーネットワーク番号全体(10.0.0.0/8)がアクセスルータを通過できるように許可する必要があります。SAFE アーキテクチャのように、分散レイヤでフィルタリングを実行すれば、より限定的なフィルタリング(10.1.5.0/24)を実施できます。

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場合と同様、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 アドレスに基づく認証を使用する場合だけです。したがって、別の認証方式を追加すれば、IP スプーフィング攻撃は無効になります。追加する認証方式としては暗号認証が最適ですが、不可能な場合は、OTP を使用する強力な 2 要素認証も効果的です。

サービス妨害

最もよく知られる攻撃形態であるサービス妨害（DoS）攻撃も、完全な排除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るには、より認知度の高いいくつかの攻撃で使用されている手段を調査することが役に立ちます。こうした攻撃には、次のようなものがあります。

- TCP SYN Flood
- Ping of Death
- TFN（Tribe Flood Network）および TFN2K（Tribe Flood Network 2000）
- Trinoo
- Stacheldraht
- Trinity

その他、セキュリティトピックを扱った優れたリソースの 1 つに CERT（Computer Emergency Response Team）があります。CERT は DoS 攻撃への対応に関する優れた論文を公開しており、この文書は次の URL で参照できます。
http://www.cert.org/tech_tips/denial_of_service.html

DoS 攻撃は、基本的に攻撃対象の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するものではない点が、他のほとんどの攻撃と異なります。DoS 攻撃の狙いは、サービスの正常利用を不可能にすることです。一般にこれは、ネットワーク上、あるいはオペレーティングシステムやアプリケーション内の何らかのリソース制限を使い果たすことで実現されます。

特定のネットワーク サーバ アプリケーション（Web サーバ、FTP サーバなど）を対象とする攻撃では、このサーバがサポートする有効な全接続を獲得し、オープンな状態を維持することに的を絞ることで、そのサーバまたはサービスの正規ユーザを実質的にロックアウトできます。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、ソフトウェアのバグやセキュリティホールではなく、攻撃対象システムのアーキテクチャ全体における弱点につけ込むものです。一方、ネットワークの性能を損なうために、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不正な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、上流の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。帯域幅を枯渇させようとするトラフィックが上流で阻止されなければ、ネットワークへの入口でそれを拒否しても、ほとんど効果はありません。この時点で、帯域幅はすでに消費されているからです。この種の攻撃が多数の異なるシステムから同時に仕掛けられた場合は、この攻撃を分散型サービス妨害攻撃（DDoS）と呼ぶことがあります。

DoS 攻撃の脅威は、以下の 3 つの方法によって軽減できます。

- **スプーフ防止機能** - ルータとファイアウォールにスプーフ防止機能を適切に設定することで、リスクを軽減できます。この設定には、最低限 RFC 2827 フィルタリングが必要です。ハッカーは、自分の正体を隠すことができなければ攻撃しにくくなります。
- **DoS 防止機能** - ルータとファイアウォールに DoS 防止機能を適切に設定することで、攻撃の効果を制限できます。こうした機能の多くは、システムが許可するハーフオープン接続の量を常に制限します。
- **トラフィックレート制限** - 組織では、ISP と協調してトラフィックレート制限を実施できます。この種のフィルタリングでは、ネットワークセグメントを通過する重要度の低い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、診断目的でしか使用されない ICMP トラフィックに対し、ネットワーク内に許可する量を制限することです。ICMP ベースの DDoS 攻撃は一般的です。

パスワード攻撃

ハッカーはパスワード攻撃を実行する際、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数種類の方法を使用できます。パケットスニファと IP スプーフィングを使用すれば、ユーザアカウントとパスワードを入手できますが、パスワード攻撃とは通常、ユーザアカウントまたはパスワードを割り出すために繰り返される試行を指します。この反復的な試行は、ブルートフォース（総当たり）攻撃と呼ばれます。

ブルートフォース攻撃は多くの場合、ネットワーク上で実行され、サーバなどの共有リソースへのログインを試みるプログラムを使用して実行されます。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と同じ権利を持つことになります。被害を与えたユーザアカウントが必要な権限を持っていれば、このユーザアカウントのステータスやパスワードの変更を気にすることなく、将来のアクセスに備えてバックドアを作成できます。

ユーザが、強力ではあっても接続するすべてのシステムで同一なパスワードを使用していれば、新たに別の問題が生じます。こうしたシステムには個人システム、企業システム、インターネット上のシステムなどが含まれます。このパスワードのセキュリティは、このパスワードを保持する複数のホストの中でも、管理が最も貧弱なホストのレベルでしかないため、そのホストが被害を受けると、ハッカーは全範囲のホストに対し、同じパスワードを試すことができます。

パスワード攻撃を排除する最も簡単な方法は、そもそも平文のパスワードに頼らないことです。OTP または暗号認証を使用すれば、パスワード攻撃の脅威を事実上排除できます。しかし残念なことに、アプリケーション、ホスト、デバイスのすべてが、これらの認証方法に対応するわけではありません。標準的なパスワードを使用する場合は、推測しにくいパスワードを選ぶことが重要です。パスワードは 8 文字以上とし、大文字小文字のアルファベット、数字、および特殊文字(#、%、$ など)を組み合わせて使用すべきです。最も良いパスワードはランダムに生成したものですが、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。このような攻撃を軽減するには、指定した回数だけ試行の失敗が続いた時点で、このアカウントを無効にしてしまう方法もあります。

ユーザと管理者によるパスワード保守に関しては、さまざまな進歩があります。現在では、パスワードリストを暗号化して、ハンドヘルドコンピュータに保存するソフトウェアアプリケーションも市販されています。これにより、ユーザは、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。管理者の観点から見ると、管理下のユーザのパスワードをブルートフォース攻撃する方法はいくつかあります。その　1　つに、ハッカー集団が使用する　LC3(旧称 L0phtCrack)と呼ばれるツールがあります。LC3　　は、Windows NT のパスワードをブルートフォース攻撃し、ユーザがごく推測しやすいパスワードを選んだ時点を検出できます。詳細については、次の URL を参照してください。

http://www.atatake.com/research/lc3/index.html

中間者による偽装攻撃（Man-in-the-Middle Attacks）

ハッカーが中間者による偽装攻撃を行うには、ネットワークを通るネットワークパケットにアクセスできることが条件です。このような構成の例として、ISP の勤務者が挙げられます。ISP 人員であれば、勤務先のネットワークとそれ以外の全ネットワークとの間で送信されるすべてのネットワークパケットにアクセスできます。このような攻撃の多くは、ネットワークパケットスニファや、ルーティングプロトコルおよび伝送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およびそのユーザに関する情報収集、サービス拒否、送信データの破壊、ネットワークセッションへの新規情報の挿入といったことが考えられます。

中間者による偽装攻撃を効果的に軽減する唯一の方法は、暗号化技術の使用です。暗号化されたプライベートセッションの中間で何者かがデータをハイジャックしても、このハッカーが閲覧できるのは暗号文でしかなく、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、中間者による偽装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、サーバで一般に使用されるソフトウェア（sendmail、HTTP、FTP など）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、このアプリケーションを実行する権限を持つアカウント（通常は特権システムレベル）として、コンピュータにアクセスできます。こうした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、この攻撃について同時に知識を得ることになります。

アプリケーションレイヤ攻撃で一番問題となるのは、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、よく攻撃に TCP ポート 80 を使用します。Web サーバはページをユーザに提供しているため、ファイアウォールではそのポートに対するアクセスを許可する必要があります。ファイアウォールから見れば、いずれも標準のポート 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排除することは不可能です。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善の方法は、適切なシステム管理を実践することです。以下に、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のログファイルを読むか、またはログ分析アプリケーションによって分析します。
- Bugtraq（http://www.securityfocus.com）や Computer Emergency Response Team(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保ちます。

適切なシステム管理の実践に加え、侵入検知システム（IDS）を使用します。IDS には、補完し合う 2 つの技術があります。

- **ネットワークベース　IDS(NIDS)：** 特定のコリジョンドメインを通過するすべてのパケットを監視することで機能します。NIDS は、既知または疑わしい攻撃に一致するパケット(単独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設定するか、セッションを終了できます。

- **ホストベース** IDS(HIDS)：保護対象のホストにエージェントを挿入することで機能します。HIDS は、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、攻撃シグニチャの使用によって機能します。攻撃シグニチャは、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とみなされるために満たす必要のある特定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 システムの最大の弱点は、システムが生成する偽陽性アラームの量です。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防止することが重要です。

ネットワーク偵察

ネットワーク偵察とは、公的に利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ます。特定のネットワークへの侵入を試みるハッカーは、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（Domain Name System）クエリ、ping スイープ、ポートスキャンといった形で実行されます。DNS クエリを使用すれば、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あばくことができます。DNS クエリによってあばいたアドレスを 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したホスト上で実行中の全サービスの完全リストを生成できます。最後に、ハッカーはこのホスト上で実行されているアプリケーションの特性を調べます。これにより、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をエッジルータで無効にすれば、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、ping スイープが完全でなくても、ポートスキャンは簡単に実行できます。存在するかどうか分からない IP アドレスもスキャンしなければならないため、長く時間がかかるだけです。ネットワークレベルおよびホストレベルの IDS は、通常、偵察的な情報収集攻撃が始まると管理者に通知できます。これにより、管理者はこれから起こる攻撃に十分に備えることや、あるいは偵察プローブを始動したシステムを収容する ISP に通知することができます。

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。多くの場合、これらのネットワークセグメントは DNS、SMTP、および HTTP サーバを収容します。これらはすべて同じセグメントにあり、同じネットワークにつながったシステムどうしが相互に信頼し合っている可能性があるため、1 つのシステムが被害を受けると、他のシステムも被害を受けることがあります。もう 1 つの例は、ファイアウォールの内側にあるシステムが、ファイアウォール外側のシステムと信頼関係を持つ場合です。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を軽減するには、ネットワーク内の信頼レベルを厳しく制約します。ファイアウォール内側のシステムは、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 アドレス以外の属性で認証するべきです。

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、通常であれば破棄されるはずのトラフィックにファイアウォールを通過させます。3 つのインターフェイスを持ち、それぞれにホストが接続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公開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、内側のホストには到達できません。公開サービスセグメント上にあるホストは、ファイアウォール内外の両方のホストにアクセスできます。ハッカーが公開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、外側のホストからのトラフィックを内側のホストへ直接転送するソフトウェアをインストールできます。いずれの通信もファイアウォールに実装された規則に違反しませんが、公開サービスホストで行われるポート転送プロセスによって、外側のホストは内側のホストと接続できるようになります。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）を使用することによって軽減できます。現在攻撃を受けているシステムでは、ホストベースの IDS を使用して、ハッカーがこのようなユーティリティをホスト上にインストールすることを検知および防御できます。

不正アクセス

不正アクセス攻撃とは、特定の攻撃の種類ではなく、現在ネットワーク上で実行されるほとんどの攻撃を指します。Telnet ログインをブルートフォース攻撃するには、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 ポートに接続すると、「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、ネットワークの内外で発生します。

不正アクセス攻撃を軽減する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可能性を減らす、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 ポートを、ハッカーのアクセスから防御しま

す。ハッカーがそのポートに到達できなければ、攻撃は極めて困難になります。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。

ファイアウォールの最も一般的な種類の 1 つが、ステートフル ファイアウォールです。このファイアウォールは双方向のトラフィックを検査し、アプリケーションの必要に応じて動的にポートを開きます。たとえば、アクティブな FTP が、データを伝送するために特定のポート開放を要求するとします。すると、ステートフル ファイアウォールはパケットからこの情報を読み取り、サーバとクライアント間の通信にこのポートの利用を許可します。この仕組みは、アプリケーションの認識を伴わない、標準的なパケットフィルタリング デバイスとは大きく異なります。こうしたデバイスは、アクセス制御の判断に、レイヤ 3 および 4 のデータを参照するだけです。以上の FTP の例にこれらのデバイスを適用するなら、管理者は FTP を正常に実行するため、すべての TCP 上位ポート（1023 以上）を外部から手動で開放する必要があります。

ウィルスおよびトロイの木馬アプリケーション

エンドユーザのワークステーションにおける最大の脆弱性は、ウィルスおよびトロイの木馬攻撃です。ウィルスとは、他のプログラムに添付され、ユーザ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、悪意あるソフトウェアを指します。ウィルスの例として、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、検出可能な他の全バージョンの command.com に感染す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プログラムであるかのように記述されているという点だけが異なります。トロイの木馬の例として、ユーザのワークステーション上で簡単なゲームを実行する、あるソフトウェアアプリケーションがあります。このプログラムは、ユーザがゲームに夢中になっている間、そのユーザのアドレス帳にあるユーザ全員に、自身のコピーをメールで送信します。そして、他のユーザ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、ウィルス対策ソフトウェアを効果的に使用することで、ユーザレベル、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。ウィルス対策ソフトウェアは、ほとんどのウィルスと多数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蔓延することを防止できます。この種の攻撃に関する最新の開発情報を常に把握しておくことも、より効果的な対策となります。企業は、新種のウィルスまたはトロイの木馬アプリケーションが公表されるつど、ウィルス対策ソフトウェアおよび各アプリケーションのバージョンを最新状態に保つ必要があります。

「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に対して許可される使用ポリシーのような単純なものもあれば、数百ページにもわたって接続の全要素とその関連ポリシーを詳しく規定したものもあります。範囲が多少限定されていますが、RFC 2196 では、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、企業の技術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。」

本文書では、セキュリティポリシーの策定については詳しく説明しません。RFC 2196 にはこの題材に関する適切な情報が一部含まれるほか、Web 上の多くの場所でポリシーおよびガイドラインの例が公開されています。セキュリティポリシーについて関心がある場合は、以下の 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は、進化の過程であると理解することが重要です。その単独使用で組織を「セキュア」にできる製品はありません。真のネットワークセキュリティを実現するには、製品とサービスを組み合わせ、さらに、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姿勢が必要です。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整備せずに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。

管理プロトコルと機能

- SSH および SSL - 管理対象デバイスに対し、暗号化および認証したリモートアクセスを提供
- Telnet - 管理対象デバイスに対し、平文によるリモートアクセスを提供
- Syslog - 管理サーバに対し、デバイスロギングとアラーム情報を提供
- TFTP（Trivial File Transfer Protocol）- 管理者が管理対象デバイスの設定ファイルを管理サーバに送信するためのプロトコル
- SNMP（Simple Network Management Protocol）- 管理サーバにデバイス情報を送信するためのプロトコル
- NTP（Network Time Protocol）- デバイス間のクロック同期を提供

以下に、各デバイスで有効にする各管理機能について解説します。

設定管理（SSH、SSL、Telnet）- デバイスへのリモートアクセスには、可能であれば IPSec、SSH、SSL、あるいは管理情報の送信に対応する他の何らかの暗号化および認証伝送手段を使用するべきです。しかし、デバイス側がいずれのプロトコルにも対応していない場合は Telnet を使用せざるを得ませんが、このプロトコルはあまり推奨できません。ネットワーク管理者は、Telnet セッションではデータが平文で送信されること、したがってデバイスと管理サーバ間のデータパス上で、誰かがパケットスニファを使用してデータを捕捉する可能性があることを認識する必要があります。データには、デバイス自身の設定情報やパスワードといった機密情報が含まれることもあります。デバイスへのリモートアクセスに SSH、SSL、または Telnet のどれを使用する場合であっても、管理サーバだけにデバイスへの接続を許可するように、アクセス制御リスト（ACL）を設定しておくべきです。他の IP アドレスからの接続の試みは、すべて拒否および記録する必要があります。管理ホストのアドレスをスプーフィングした外部からの攻撃の機会を減らすため、ネットワーク入口のルータで RFC 2827 フィルタリングを実施することも必要です。SSH は TCP ポート 22 を、Telnet は TCP ポート 23 を、SSH は TCP ポート 443 をそれぞれ使用します。

ロギング - Syslog も、管理対象デバイスと管理ホストとの間で平文により送信されます。Syslog には、パケットの内容が伝送中に改ざんされていないことを保証するための、パケットレベルの整合性検査機能がありません。攻撃者は、攻撃中にネットワーク管理者を混乱させる目的で、システムログを改ざんするかもしれません。伝送中の改ざんの機会を減らすため、Syslog トラフィックは可能な限り IPSec トンネル内で暗号化すべきです。費用やデバイス自身の機能の問題により、IPSec トンネル内で Syslog データを暗号化できない場合、管理者は、Syslog データが攻撃者によって改ざんされる可能性があることに注意してください。ファイアウォール外部のデバイスからの Syslog アクセスを許可する場合は、ネットワーク出口のルータで RFC 2827 フィルタリングを実施すべきです。これにより、管理対象デバイスのアドレスをスプーフィングして、管理ホストに虚偽の Syslog データを送信する、ネットワーク外部からの攻撃の可能性を軽減できます。また、ファイアウォールの ACL は、管理対象デバイス自身からの Syslog データだけが管理ホストに到達できるように設定する必要があります。これにより、攻撃者が攻撃中にネットワーク管理者を混乱させる目的で、管理サーバに大量の虚偽の Syslog データを送りつけることを防止できます。Syslog は、UDP ポート 514 を使用します。

TFTP - 多くのネットワークデバイスは、設定ファイルまたはシステムファイルのネットワーク上での送信に TFTP を使用します。TFTP は UDP ポート 69 を使用するほか、デバイスと TFTP サーバ間のデータストリームには上位の UDP ポート（1023 以上）を使用し、データを平文で送信します。ネットワーク管理者は、TFTP セッション内のデータが、デバイスと管理サーバ間のデータパス上でパケットスニファによって捕捉される可能性があることを認識する必要があります。データには、デバイス自身の設定情報といった機密情報が含まれることもあります。データ捕捉の機会を減らすため、TFTP トラフィックは可能な限り IPSec トンネル内で暗号化する必要があります。

SNMP - SNMP は、ネットワークデバイスから情報を収集するため（一般に「読み取り専用アクセス」と呼ばれる）、またはデバイスのパラメータをリモートに設定するため（一般に「読み書きアクセス」と呼ばれる）のネットワーク管理プロトコルです。SNMP エージェントは、UDP ポート 161 からの応答を受信します。SNMP は、非常に単純なセキュリティの形態として、コミュニティ文字列と呼ばれるパスワードを各メッセージ内で使用します。残念ながら、現在ネットワークデバイスに実装されるほとんどの SNMP は、コミュニティ文字列をメッセージと共に平文で送信します。したがって、SNMP メッセージは、デバイスと管理サーバ間のデータパス上でパケットスニファによって捕捉される可能性があり、コミュニティ文字列も攻撃対象となる場合があります。コミュニティ文字列を盗聴した攻撃者は、SNMP 経由の読み書きアクセスが許可されている場合、デバイスを再設定できるようになります。このため、SNMP の設定には、読み取り専用のコミュニティ文字列だけを使用することを推奨します。SNMP 経由で管理したいデバイスに対し、適切な管理ホストからのアクセスだけを許可するようにアクセス制御を設定すれば、さらに防御を強化できます。

NTP - NTP（Network Time Protocol）は、ネットワーク上のさまざまなデバイスのクロックを同期させるために使用します。ネットワーク内のクロック同期は、デジタル認証において、およびシステムログデータ内のイベントを正確に解釈する上で重要です。ネットワークのクロックを安全に同期するには、ネットワーク管理者が、衛星または無線経由で UTC（協定世界時）に同期させた独自のマスタクロックを、プライベートネットワークに実装します。しかし、ネットワーク管理者が費用などの理由から独自のマスタクロックの実装を望まない場合は、同期のためのクロックソースはインターネット経由で利用できます。このとき攻撃者は、ディジタル認証を無効に見せかけるためにネットワークデバイスのクロックを変更しようとして、インターネット経由で虚偽の NTP データを送信することにより、ネットワークに DoS 攻撃を試みる可能性があります。さらに攻撃者は、ネットワークデバイスのクロックを乱すことで、攻撃中にネットワーク管理者を混乱させようと企むこともあります。これにより、ネットワーク管理者は、複数のデバイス上で発生したシステムログイベントの順序を判断することが難しくなります。バージョン 3 以上の NTP は、ピア間の暗号化認証に対応します。こうした攻撃を軽減するには、ACL で、他のネットワークデバイスとの同期をどのネットワークデバイスに許可するかを規定すると共に、この認証機能を使用することを推奨します。ネットワーク管理者は、インターネットからクロックを参照することの費用的な利点と、これを実行すること自体、およびこのプロセスにファイアウォールの通過を許可することに伴う潜在的なリスクとを、比較して検討する必要があります。インターネット上の多くの NTP サーバは、ピア間の認証をいっさい要求しません。したがってネットワーク管理者は、クロック自身が信頼でき、有効かつ安全であると信じる必要があります。NTP は UTP ポート 123 を使用します。

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に提供するサーバ。提供するサービスには、ワークフロー、一般的なオフィス業務、セキュリティアプリケーションなどがあります。

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 フィルタリング デバイス。定義済みのアクセス制御フィルタに一致するトラフィック、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トラフィックだけが、ファイアウォールを通過できます。

HIDS（ホストベース侵入検知システム） - 個々のホスト上の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。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や、ログファイル、ファイルシステム情報、およびネットワーク接続の検査などがあります。

NIDS（ネットワークベース侵入検知システム） - 通常は運用を停止させない方法で使用されるデバイス。LAN セグメントを流れるトラフィックを捕捉し、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比較します。シグニチャには、原子的（単一のパケットおよび方向）なものから、ステートテーブルとレイヤ 7 アプリケーション追跡が必要となる複合的（マルチパケット）なものがあります。

Cisco IOS ファイアウォール - Cisco IOS（Internetwork Operating System）ソフトウェア上でネイティブ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

Cisco IOS ルータ - 幅広い種類を揃えた柔軟なネットワークデバイス。あらゆる性能要件に対し、多くのルーティングおよびセキュリティサービスを提供します。ほとんどのデバイスはモジュラ型であり、幅広い種類の LAN および WAN 物理インターフェイスを備えています。

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各ネットワークセグメントに提供。通常このデバイスは、10/100 個のスイッチドポート、ギガビット イーサネット アップリンク、VLAN トランキング、レイヤ 2 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と共に、ルーティング、QoS、セキュリティの各機能を追加提供。このスイッチは多くの場合、特殊機能プロセッサを搭載します。

管理サーバ - 企業ネットワークのオペレータにネットワーク管理サービスを提供するサーバ。このサービスには、一般的な設定管理、ネットワーク セキュリティ デバイスの監視、セキュリティ機能の操作などがあります。

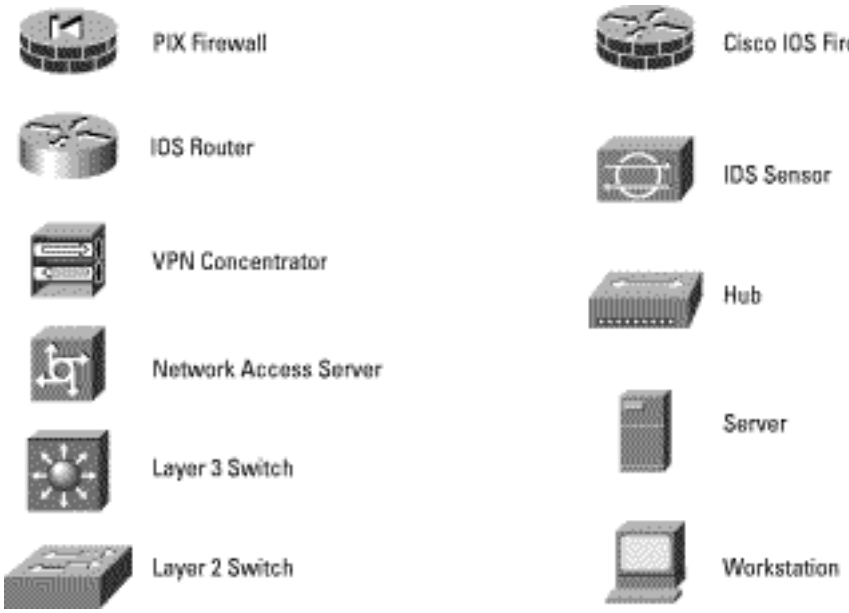
SMTP コンテンツ フィルタリング サーバ - 通常、外部の SMTP サーバで実行されるアプリケーション。着信メールや発信メールの内容（添付ファイルを含む）を監視して、そのメールがそのまま転送、変更して転送、または破棄されるように許可されているかを判断します。

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。このサーバ宛に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べきかどうかをネットワークデバイスに通知します。企業はこれにより、不正とみなすインターネットサイトのカテゴリを規定するセキュリティポリシーを実施できます。

VPN 終端デバイス - 拠点間またはリモートアクセスの 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を実現するには、付加的な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端末 - エンドユーザが直接使用する、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21：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 282「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.securitysoftwaretech.com/antisniff

「LC3」
http://www.atstake.com/research/lc3/index.html

「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

Entercept Host-Based IDS：
http://www.entercept.com

RSA SecureID OTP System：
http://www.rsasecurity.com/products/securid/

Baltimore MIMESweeper Email Filtering System：
http://www.mimesweeper.com

Websense URL Filtering：
http://www.websense.com/products/integrations/ciscopix.cfm

F-Secure SSH Client：
http://www.fsecure.com/products/ssh/

OpenSystems PrivateI Syslog Analysis Tool：
http://www.opensystems.com/products/index.asp

Zone Alarm Pro Personal Firewall：
http://www.zonelabs.com/products/index.html

General Cisco AVVID Security and VPN Solution Partners Information：
http://www.cisco.com/go/securitypartners

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れました。このグループの中心となった Rahimulah Rahimi 氏、Jason Halpern 氏、Mark Doering 氏、Tom Hunter 氏、Masamichi Kaneko 氏、Alok Mittal 氏、および Mike Steinkoenig 氏を含む、皆様の多大なる努力に感謝します。

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

02.06