SAFE 設計ガイド

セキュリティドメイン：脅威に対する防御

ユース ケース：シスコのランサムウェアに対する防御

最新の情報を追加 - 2017 年 8 月更新

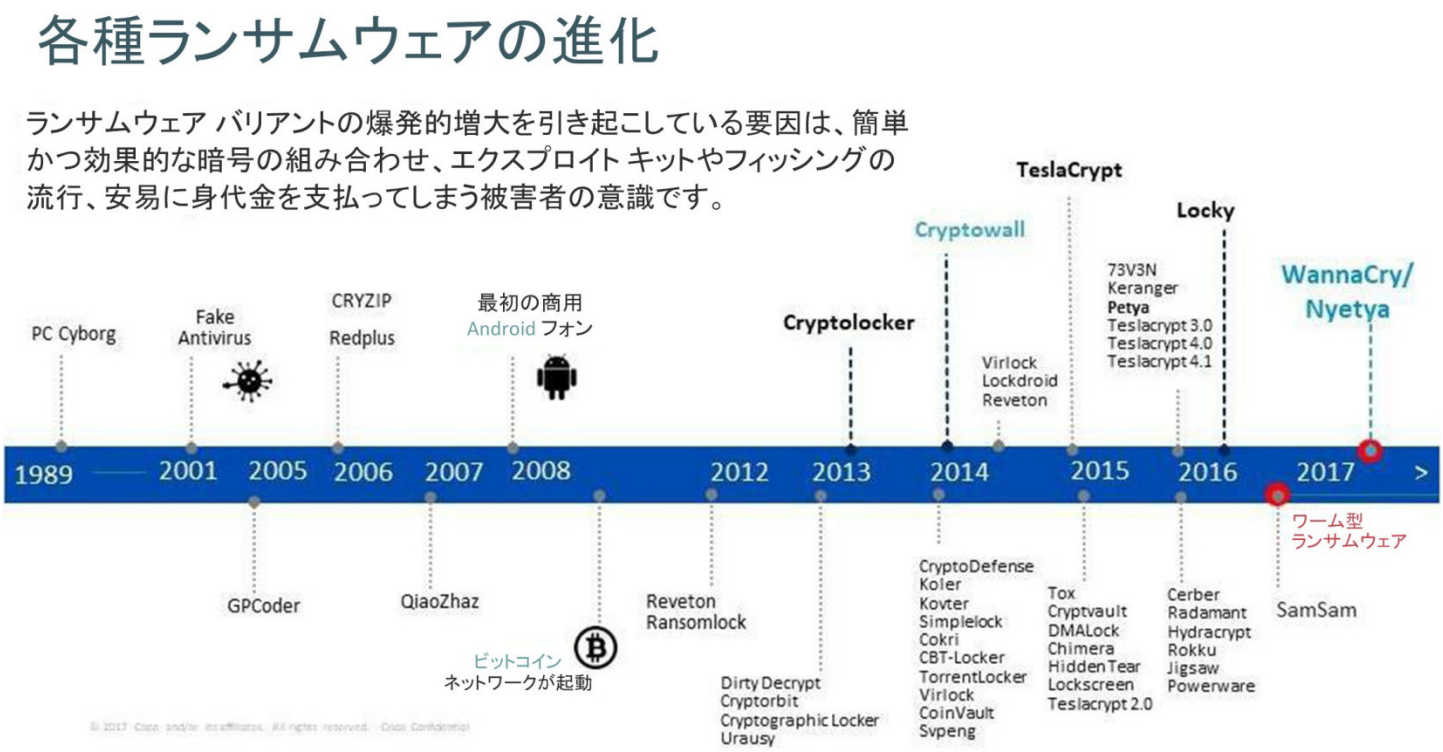
目次

はじめに

ランサムウェアは、史上最も収益性が高いタイプのマルウェアです。かつてマルウェアは、システムへのアクセスを拒否することもデータを破壊することもありませんでした。攻撃者の主な目的は、情報を盗み出し、システムと被害者のリソースへのアクセスを長期間維持することでした。しかしランサムウェアの登場により、攻撃の中心は「隠匿型の検知されない情報詐取」から「恐喝」へと変化しました。

ファイルを回復するためにお金を支払うすべての企業と個人は、攻撃者に直接支払いを行います。ビットコインやリップルなどの比較的新しい匿名通貨の登場によって、攻撃者は比較的低いリスクで容易に収益を上げる手段を確保できたため、ランサムウェアの魅力が高まるとともに、次世代のランサムウェアの開発に資金が拠出されるようになりました。その結果、ランサムウェアは驚くべき速さで進化しています。最近のランサムウェア攻撃はワームのように伝搬され、連携して組織全体に攻撃を拡散させます。身代金をまとめて要求するものや、身代金の支払いではなくビジネスの中断や破壊を目的とするものもあります。

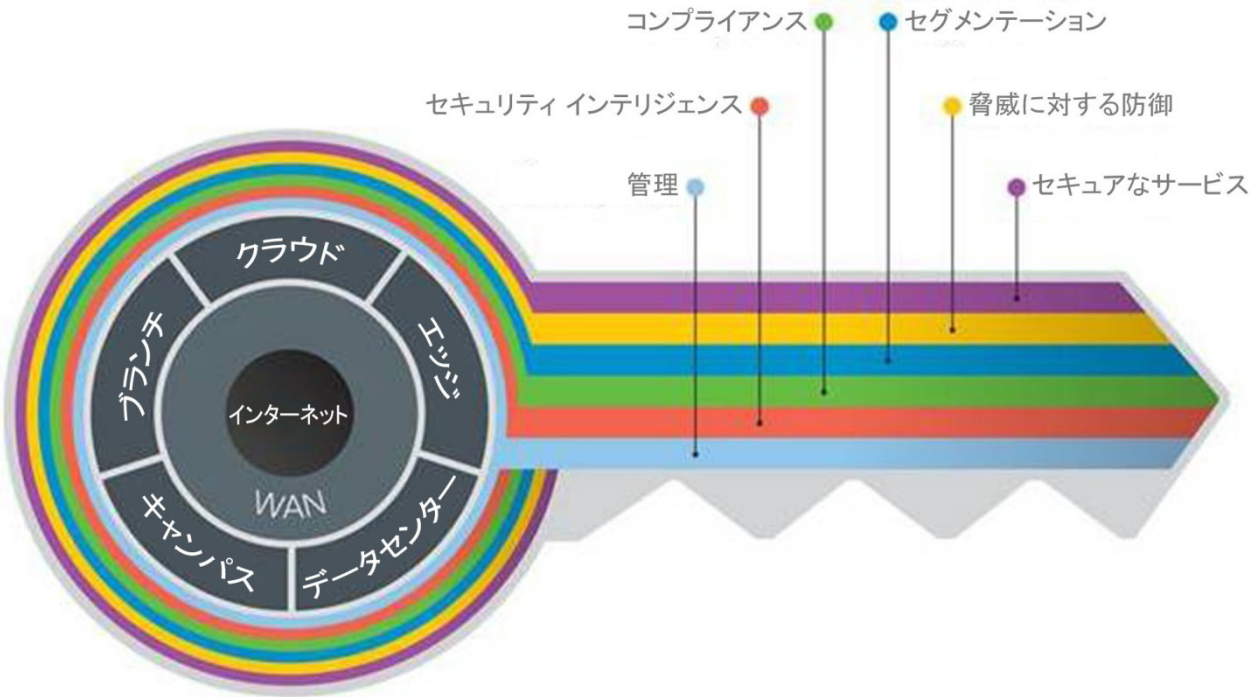
図 1 - 各種ランサムウェアの進化



シスコは、階層型防御アーキテクチャ アプローチを使用してランサムウェアの脅威からビジネスを保護できるように支援します。このアプローチは、ネットワーク内外のユーザを保護します。

このガイドは、SAFE の「脅威に対する防御」ドメインに含まれるランサムウェアのユース ケースに対応しています。このガイドには、キャンパス PIN に推奨されるランサムウェア防御アーキテクチャが含まれています。SAFE は、組織が保護しなければならない領域に焦点を当てたモデルを利用して、企業全体に広がる複雑さをシンプルにします。このモデルは、最新の脅威と、こうした脅威から各領域を保護するために必要な機能に焦点を当て、各領域に総合的に対応します。シスコは、この重大なビジネスの課題を展開し、テストと検証を実施しました。これらのソリューションは、設定手順を含むガイダンスを提供しますので、お客様に効率的かつ安全に導入いただくことができます。

図 2 - SAFE の脅威に対する防御



SAFE では、複雑で全体的なセキュリティを Places in the Network（PIN）とセキュア ドメインに切り分けます。

SAFE は、ビジネス フローと各フローに対する脅威から、脅威に対応するセキュリティ機能、アーキテクチャ、設計を網羅する、包括的で理解しやすいガイダンスを提供します。

Cisco SAFE によってセキュリティをシンプルにする方法の詳細については、www.cisco.com/jp/go/safe を参照してください。

概要

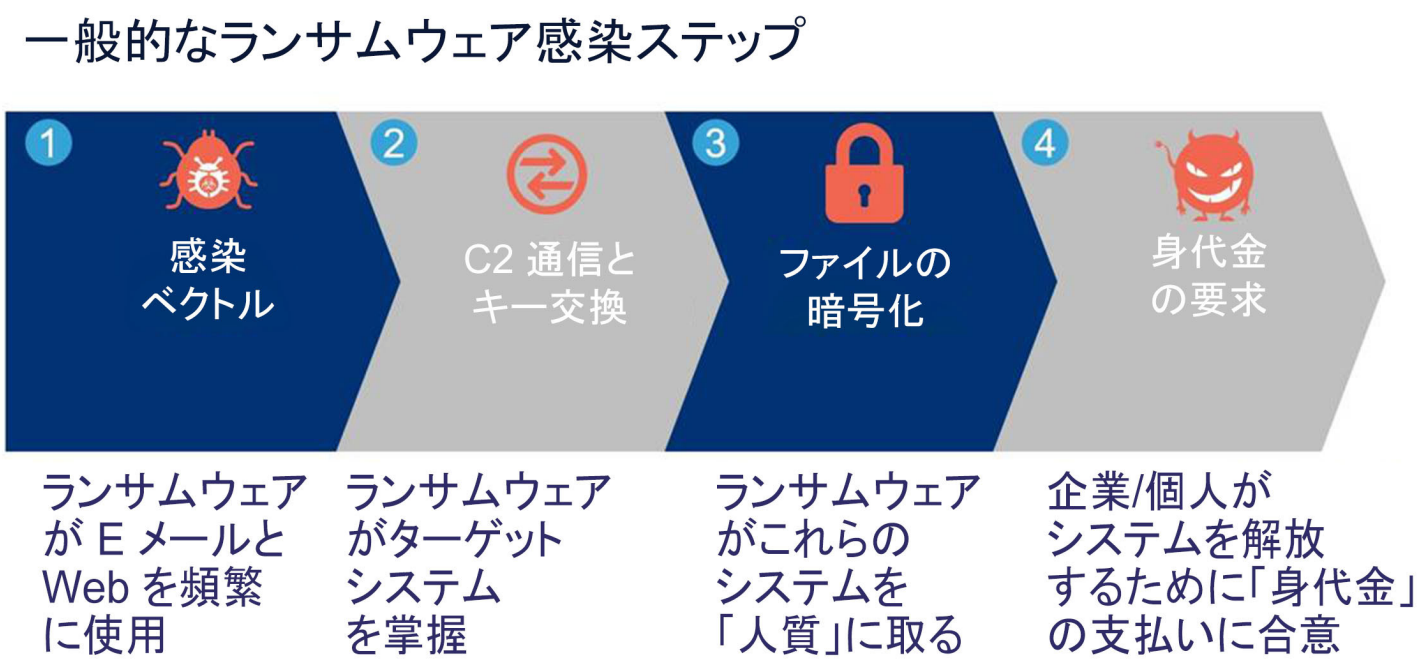
企業や個人は、重要なリソースをロックするランサムウェアというマルウェアによって、「人質」をとられることがあります。ランサムウェアは、フィッシング メール、既知の脆弱性、エクスプロイト キットなどの従来のマルウェア攻撃ベクトルを使用してデスクトップに送り込まれます。一度入り込んだランサムウェアは、システムおよび保存されたデータを乗っ取ってその内容を暗号化し、アクセスを拒否して、身代金（ランサム）が支払われるまでそれを人質に取ります。またランサムウェアは、この間にネットワーク全体に広まり、ビジネスに大きな混乱を引き起こします。ランサムウェアは堅牢な公開キー/秘密キー暗号化方式を使用しているため、ファイルをリカバリするには、身代金を支払うか、バックアップからファイルを復元するしか方法はありません。身代金を支払うと、多くの場合アクセスを復元するための復号キーが攻撃者から提供されますが、必ずしもそうではないことが今では知られています。

こうした重要リソースにアクセスできない場合、ビジネスに破壊的な影響が及ぶことがあります。

- 病院の場合、患者のリアルタイム ケア（入院、手術、投薬など）の提供機能を失うことがあります。
- 製造業者は、製品のダウンタイムが発生したり、出荷/納期予定を満たせない可能性があります。
- 第一対応者が、119 番や緊急連絡先への連絡を阻止されることがあります。
- 金融機関のシステムがオフラインになり、取引または銀行業務ができなくなる可能性があります。
- 小売業者は支払いを処理できず、顧客は商品を購入できなくなることがあります。

ランサムウェア感染

図 3 - 一般的なランサムウェア感染ステップ



1. 通常ランサムウェアは、大規模なフィッシング キャンペーン、マルバタイジング、標的型エクスプロイト キットを通じて配信されます。
2. 配信されたランサムウェアは、システムの制御を奪い、ファイルの暗号化に使用できる公開キー/秘密キーの作成と転送のために、自身のコマンド/コントロール インフラストラクチャとの通信を試みることができます。
3. ランサムウェアは必要なキーを手に入れると、暗号化する特定のファイルのタイプとディレクトリを識別します。多くのシステム ディレクトリとプログラム ディレクトリを回避することにより、実行終了後に身代金を確実に届けられるようにします。
4. 暗号化が完了すると、身代金の支払い方法に関する指示を含む通知がユーザに残されます。

組織への一般的な感染ベクトル

組織は多くの方法でランサムウェアの侵害を受ける可能性がありますが、最も一般的なのは電子メール フィッシング攻撃と Web でホストされているマルバタイジングです。

電子メール：電子メールは、配布リストとマス メーリングを使用すると 1 対多の感染ベクトルになります。通常 1 人のユーザは、個人用と会社用に複数の電子メール アカウントを管理しています。こうしたアカウントはすべて、セキュリティ上の脅威になります。たとえば、IT 組織が多大な時間と労力をかけて Cisco E メール セキュリティ アプライアンスまたはクラウドなどのメール セキュリティ サービスを選択しても、通常ユーザは Hotmail や Gmail などのパブリック メール サービスを使用して個人的なメールをチェックします。これらのプライベート電子メール アカウントには、電子メール セキュリティ サービスをバイパスする Web ポータルを介して容易にアクセスできます。したがって、プライベート アカウントを通じてユーザが電子メール添付ファイルやフィッシング リンクにアクセスし、マルウェアをダウンロードし、実行することが大きな懸念事項になっています。

Web：マルバタイジング広告は、意図的にシステムに感染してエクスプロイト キットやランサムウェアを直接インストールする、犯罪者に制御されているマルウェアです。マルバタイジング広告はあらゆるサイトの広告に含ま

れている可能性があり、その多くはユーザに日常的にアクセスされています。この種の広告をクリックしたユーザは特定のサイトに誘導され、そこでユーザのコンピュータが感染します。マルバタイジング ネットワークは数千ものネットワーク ドメイン名で構成され、絶えず変化する共有インフラストラクチャを形成しています。これらのドメイン名はランダムまた半構造のものですが、すべてのドメイン名は寿命が比較的短く、頻繁にリプレースされています。これらのドメインでは、犯罪者がシステムの感染、制御、中断を目的に使用するエクスプロイト キット、ツール、コマンド/コントロール サービスがホストされます。これらの通信はほぼすべて暗号化されます。

ユーザがマルバタイジングと接触する方法はいくつかあります。単に広告を出しているサイトにアクセスする場合もあれば、検索結果ページや電子メールのリンクをクリックする場合もあります。[1]賢明な Web サーファーの多くは、保護を目的にシステムに広告ブロッカーを導入していますが、このツールはサイトの広告収入に影響を与えるため、コンテンツを抑制し、広告ブロックの無効化を要求する戦いが起きています。大手サイトは広告ブロッカーの使用に応じてサイトへのアクセスを制限できますが、提供する広告が悪意のあるものではないことを保証することはできません。こうしたサイトとサービスは、侵害とリダイレクトの主な標的になっています。

ランサムウェアは、他のマルウェア（Nimda、Sasser、Code Red、SQL Slammer、Sality、Conficker など）が備える強力な侵入機能を取り入れるために積極的に進化しているため、企業ネットワーク全体に広がり感染させ、巨額の支払いを求めて企業がアクセス可能なすべてのデータを暗号化するケースや、ネットワーク全体にマルウェアを拡散させて大規模な混乱を引き起こすケースが発生しています。

ランサムウェアの通信

ランサムウェアの通信に含まれるコマンド/コントロール（C2）コールバックは、表 1 に示したように、暗号化キーと支払いメッセージの取得のために行われます。

表 1 - ランサムウェアの通信方法

	暗号化キー				支払いメッセージ
名前*	**DNS**	**IP**	**C2 なし**	**TOR**	**支払い**
Locky	✓	✓			DNS
SamSam			✓		DNS（TOR）
TeslaCrypt	✓				DNS
CryptoWall	✓				DNS
TorrentLocker	✓				DNS
PadCrypt	✓				DNS（TOR）
CTB-Locker	✓			✓	DNS
FAKEBEN	✓				DNS（TOR）
PayCrypt	✓				DNS
KeyRanger	✓			✓	DNS

*2016 年 3 月現在の主要バリアント

[1] http://blog.talosintel.com/2016/05/spin-to-win-malware.html

システムへの侵入に成功すると、エクスプロイト キットは環境（OS、パッチが適用されていないアプリケーションなど）を分析した後、効果的なランサムウェア バリアントを取得してドロップします。次にランサムウェア インフラストラクチャに対してコールバックを行い、システムを暗号化するために必要なキーを取得します。広く普及しているエクスプロイト キットとランサムウェア バリアントの多くは、このコールバックを開始するためにドメイン名から IP アドレスを割り出します。

一部のランサムウェア バリアントは動作が異なります。たとえば、SamSam は、C2 コールバックを必要としない組み込みの暗号化キーを使用し、他のバリアントでは Tor ベースでのオニオン ルーティングや IP のみでのコールバックを使用して DNS を回避しています。これらに対し、ランサムウェア防御ソリューションは多様な方法でセキュリティを確保できます。

ランサムウェア キル チェーン

上記で説明した感染プロセスの最初の 2 つのステップは、一般的には図 4 に示すように、7 つの攻撃段階に分類されます。すべての攻撃がすべての段階を使用するわけではありませんが、この手法が最も一般的です。

図 4 - 7 つの攻撃段階

「キル チェーン」という言葉は、正しい能力を行使できる場合にこのいずれかの段階で攻撃をブロックできることを意味します。各段階の簡単な説明を以下に示します。セキュリティ業界では一般に、（名前は多少異なるとしても）次のように理解されています。[2]

偵察：攻撃者は、信頼できるように見える場所とメッセージを作成して悪意のある広告やフィッシング メールをステージングする目的で、情報を収集します。

ステージング：サイバー犯罪者は偵察時に収集された情報を使用して、ユーザを騙して電子メールを開かせたり、リンクをクリックさせたりしようとします。

開始：ステージング サイトは、信頼できるように見えるサイトから、エクスプロイト キットやその他の悪意あるコンテンツを開始（起動）するサイトにリダイレクトします。

エクスプロイト：侵害されたサイトにユーザが来ると、ユーザ システムがスキャンされ、脆弱性が見つかった場合にはそれがエクスプロイト（不正利用）されてユーザ システムの制御が奪われます。

インストール：エクスプロイトにより制御が奪われると、最後に送り込まれるファイルやツールがインストールされ、それが標的システムを感染させて暗号化します。これがランサムウェア ペイロードです。また、この段階では、他のマルウェアを将来送り込むための追加の実行可能ファイルが含まれることもあります。

[2] http://www.cisco.com/c/ja_jp/products/security/security-reports.html

コールバック： 感染したシステムは、コマンド/コントロール サーバ（C2）への「コール ホーム」を行い、暗号化の実行や追加の命令を受信するためのキーを取得します。

永続化： ハード ディスクのファイル、マップされたネットワーク ドライブ、および USB デバイスが暗号化され、通知やスプラッシュ画面がポップアップされ、元のファイルを回復するために身代金の支払いを要求する指示が表示されます。この通知は画面に居座り、時々ファイルを削除し、解除キーを取得できる期限までのカウント ダウンをタイマーで表示するため、ユーザにとっては大きなプレッシャーになります。また、攻撃者のエクスプロイト キットが永続化すると、そこを拠点としてより重要な他のシステムに向かうこともあります。

ランサムウェア防御

ランサムウェア防御ソリューションでは、シスコ セキュリティのベスト プラクティス、製品、サービスを利用して、ランサムウェア攻撃の防止、検出、対処を行う階層型防御アーキテクチャを構築します。シスコのランサムウェア防御ソリューションは、特効薬でも保護を保証するものありませんが、次のことに役立ちます。

- 可能な限りランサムウェアの企業への侵入を防止する
- ランサムウェアがコマンド/コントロールを取得する前に、システム レベルでランサムウェアを阻止する
- ネットワーク内に存在し、感染を広げている最中のランサムウェアを検出する
- 他のシステムやネットワーク領域へのランサムウェアの拡大を食い止める
- インシデント対応を実行し、攻撃された脆弱性と領域を修復する

このソリューションによって、人質を取られることや重要なシステムの制御を失うことを恐れずにビジネス活動を継続させることができます。

ランサムウェア キル チェーンから防御するには、適切な防御階層を構築するための特定の機能が必要です。表 2 に、この防御に最適な SAFE メソドロジ機能（青の円）を示します。

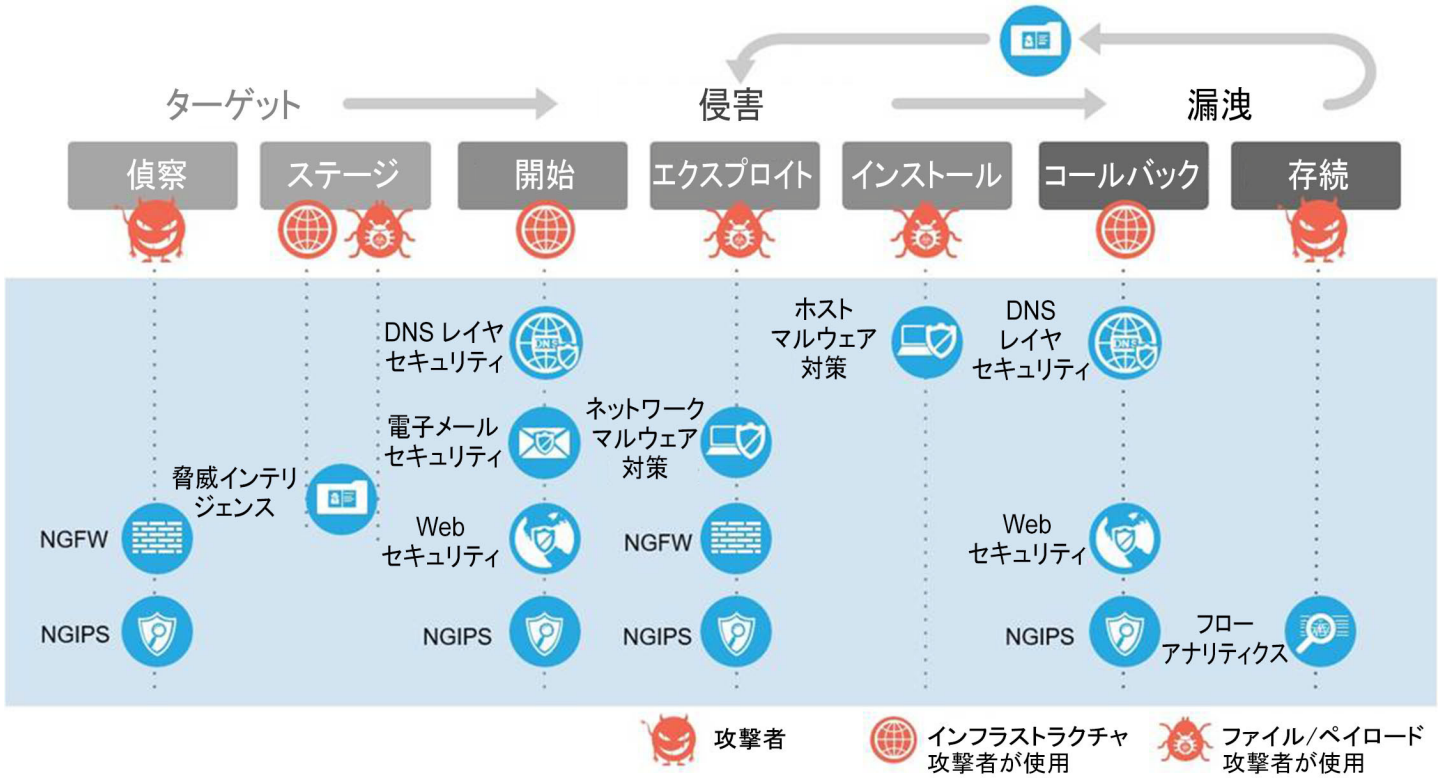
表 2 - ランサムウェア攻撃から防御する SAFE の機能

アイコン	機能	説明
	脅威インテリジェンス	既存のランサムウェアと通信ベクトルについての知識、および新しい脅威について学習された知識
	E メール セキュリティ	ランサムウェアの添付ファイルとリンクをブロックする
	DNS セキュリティ	既知の悪意のあるドメインをブロックし、コマンド/コントロール コールバックを切断する
	クライアント セキュリティ	ランサムウェアやウイルスがないか検査し、隔離して、削除する
	Web セキュリティ	感染したサイトとファイルへの Web 通信をブロックする

	ID ベースのファイア ウォールのセグメンテーション	アクセスを認証し、ロールとポリシーに基づいてトラフィックを分離する
	侵入防御	攻撃、エクスプロイト、情報収集を遮断する
	ネットワークの監視	フローベースのアナリティクスを使用してインフラストラクチャの通信を監視し、異常なトラフィック フローを識別してアラートを出す

7 つの攻撃段階に対抗して防御するために、図 5 に示すようにこれらの機能を導入します。

図 5 - セキュリティ機能を利用したキル チェーンの破壊



これらの機能は、連携して複数の防御階層を形成し、ランサムウェアの脅威と拡大から組織を保護します。

ベスト プラクティス

期待できる成果

ワールド クラスの階層型防御アーキテクチャを導入するだけでは不十分です。組織では、ビジネスを運営する上での重要な優先事項と、システムがロック ダウンされたときにこれらの優先事項が影響を受けるかどうかを把握する必要があります。

- 最も重要なアクションは、有効なバックアップを確実に取り、バックアップ システムの効果を検証することです。週次バックアップを取っている場合は、日次バックアップに移行し、日次バックアップを取っている場合は、毎時またはリアルタイム バックアップを取ることを検討します。一部のバックアップでは、攻撃が発生する前の状態へのロール バックがサポートされています。この機能は、有益に活用できる環境も役に立たない環境もあります。

- 優れたディザスタ リカバリ計画を立てるとともに、ビジネスの拡大や変化に応じてこの計画を定期的に検証および更新します。
- 「最初の連絡先」を把握します。従業員がランサムウェア攻撃に遭った場合、最初に連絡するのは誰ですか？多くのケースでは IT 部門ですが、常にそうとは限りません。講じるべきアクションを「最初の対応者」が把握し、迅速に対応できるような体制を整えてください。
- 重大なシステムの中断やイベントへの対応に必要なすべての人、プロセス、ツールを特定します。これらの計画をテストする訓練を定期的に実施します。
- アプリケーション、システム イメージ、情報、通常のネットワーク パフォーマンスの包括的なベースラインを作成します。これにより、ネットワークの変化を可視的に把握し、異常な事態を検出できるようになります。
- オペレーティング システムとデスクトップのイメージを標準化し、感染したインフラストラクチャのリカバリの際にイメージを容易に再作成できるようにします。

最悪の事態が発生した際のリカバリ

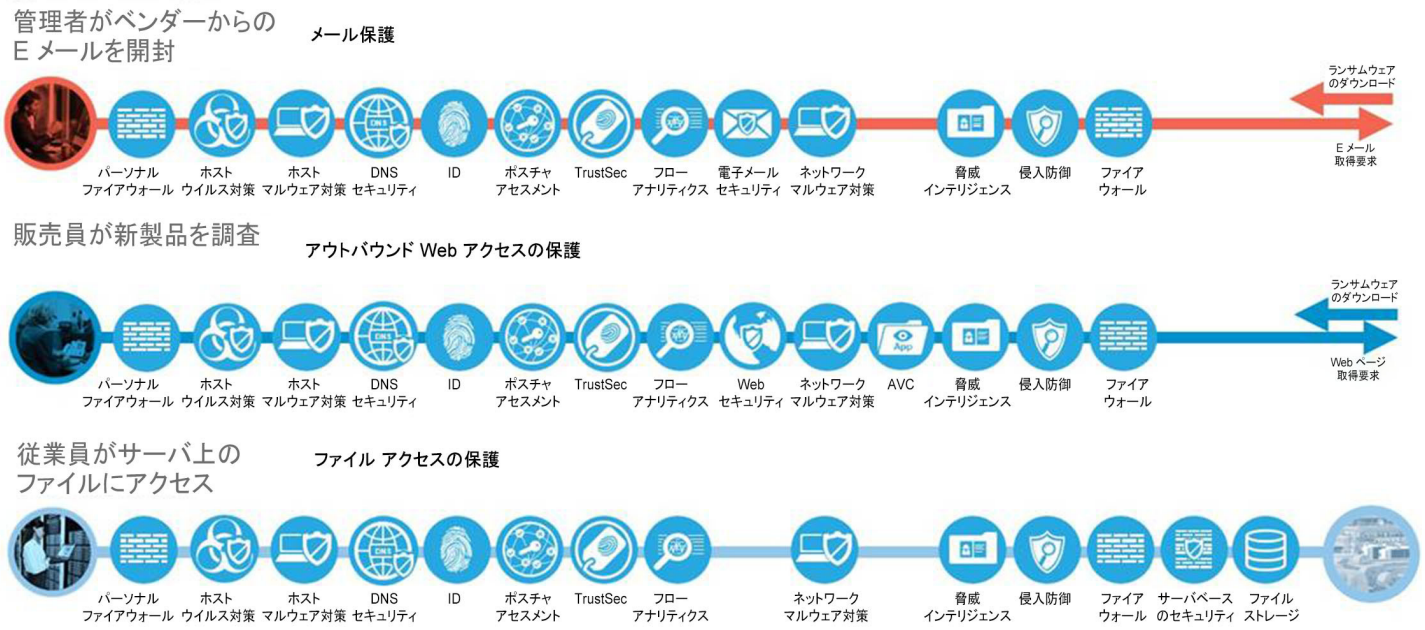
バックアップのリカバリは、最後の防御策となり、攻撃者への身代金の支払いを防ぎます。データの損失やサービスの中断を最小限に抑えてこの攻撃から復旧できるかどうかは、攻撃の一環でシステム バックアップやディザスタ リカバリ サイトが侵害されたかどうかに左右されます。バックアップが侵害されたかどうかは、バックアップ システム、ネットワーク、リカバリ サイトがメイン ネットワークから十分にセグメント化されているかによって決まります。組織でオンサイト バックアップをまったく使用しておらず、代わりにクラウド バックアップ ソリューション（Amazon Glacier など）を選択している場合、これらのクラウド バックアップのクレデンシャル情報を容易にアクセス可能な場所に置いていたり、パスワードを再利用していたりすると、攻撃者はすべてのバックアップ インスタンスを容易に削除できるので、他のバックアップ ソリューションを導入していない場合はデータは 100% 失われます。安全なオフサイトの企業バックアップ ソリューションも、パスワードを再利用したり、パスワード管理が不十分だと容易に攻撃されてしまいます。

バックアップ ソリューションを活用している場合は、非常に幅広いバックアップ手法を利用できます。SANS Reading Room には、非常に役立つテープ ローテーション スキームに関する包括的な文書が掲載されています。一般的なテープ ローテーション ポリシーの一環として、テープの一部はオフサイトのストレージ施設に輸送されます。その目的はディザスタ リカバリです。組織のデータをホストしているサイトで重大な障害が発生しても、ストレージ施設にテープがあるためバックアップから復旧を行うことができます。ローカル バックアップが削除されたり、攻撃者の手によってアクセス不能になってしまった場合には、オフサイトのバックアップが身代金を支払わずにサービスをリストアする唯一の望みになります。バックアップをオフサイトに輸送する頻度によって、（ある場合）どの位のデータがアクセス不能になるか、または失われるかが決まります。

ソリューション アーキテクチャ

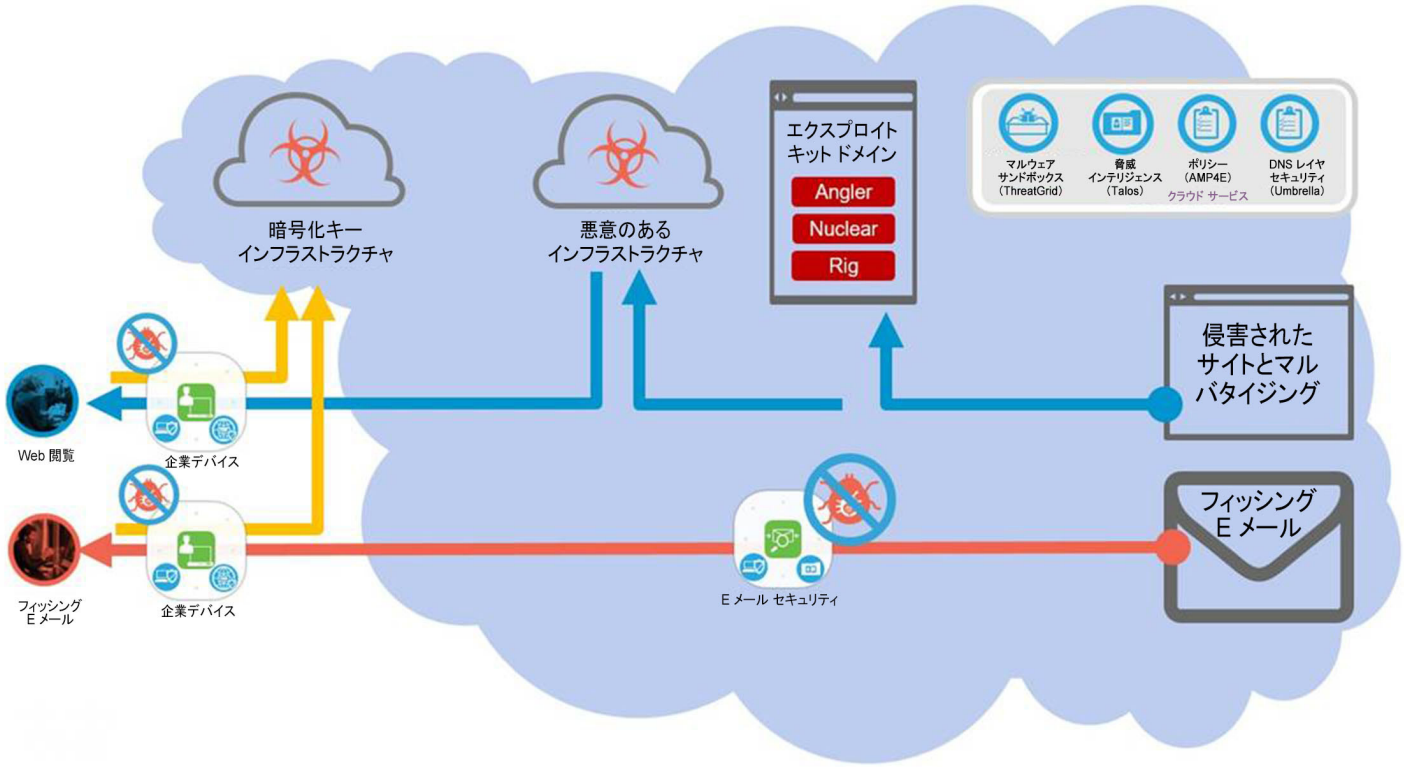
階層型防御アーキテクチャ開発の最初の一歩は、ランサムウェア キル チェーンを破壊できるすべての機能を利用し、SAFE モデルで特定された実際のビジネス機能/フローに対応付けることです。ランサムウェア固有のものとして、Web ブラウジングと電子メールの使用があります。これらは最もリスクが高い感染手法です。3 つ目の例が社内ストレージ内のファイルです。図 6 に、この 3 つのビジネス フローと、上記で説明したこれらのフローに対応する機能を示します。組織全体では、これらの機能が複数の PINS に重複していることがあります。この図では、重複する機能をすべて削除しています。また、機能は必ずしも特定の順番で配置されているわけではありません。この図は、エンドツーエンドでフローを保護する最善の手法の例を表しています。

図 6 - SAFE ビジネス フローと機能



これらの機能を包括的に導入する場合、相当なコストと時間が必要になる可能性があるため、このソリューションは 2 つのフェーズに分割されました。図 7 に示したように、フェーズ 1 には、比較的少ない労力で導入でき、大幅なリスクの低減を達成できるいくつかの機能が含まれています。残りの機能はフェーズ 2 で追加されます。フェーズ 2 は、イグザンプル キャンパス ネットワーク PIN アーキテクチャに示しています。

図 7 - クラウドとエンドポイントの機能



フェーズ 1 - 迅速な防止

ランサムウェア攻撃と感染の脅威は身近に迫っているため、組織は次の被害者になる前にランサムウェアをブロックするアクションを講じる必要があります。まず電子メール、DNS、マルウェア対策のセキュリティ機能を導入して既存のセキュリティ対策を補完しなければなりません。以下に、ランサムウェア攻撃が成功するリスクを即座に低減する、迅速に導入できるクラウド対応サービスを示します。

迅速に防御を成功させる 3 つのステップ:

1. 最大の感染ベクトルをブロックします—1 人のユーザに到達する前に、電子メール添付ファイルと URL をフィルタリングします（Cisco E メール セキュリティ）。
2. コマンド/コントロール（C2）通信と、悪意のあるサイトへのリダイレクトを阻止します—オンネットおよびオフネット保護用の DNS セキュリティ階層（Umbrella）を追加します。
3. 基盤インフラストラクチャ（ホスト、ネットワーク、E メール、Web）全体で、悪意のあるファイルからの保護（AMP）機能を有効化します。

これらの機能を導入することは非常に重要です。グループ（管理者、エグゼクティブ、重要サーバ）別に優先的に機能を導入した後、できるだけ広範に機能を導入します。

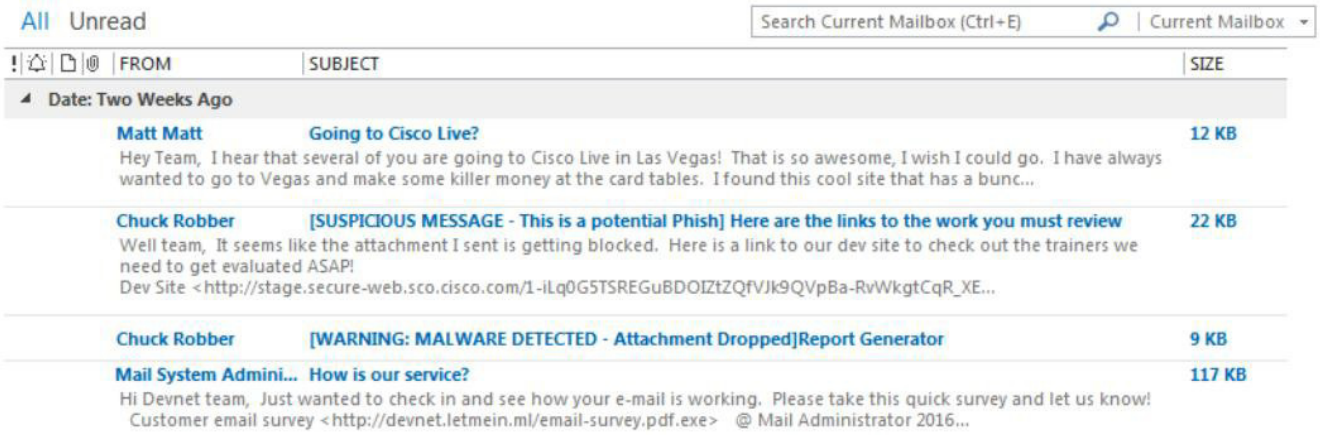
これらのサービスはすべて、Talos Threat Intelligence、Threat Grid ファイル分析、Umbrella Security Graph のクラウドベース サービスを共有しています。

電子メール セキュリティ

電子メール セキュリティは、ランサムウェアを開いたりクリックしたりする実際のユーザに到達する前に、組織内に入るすべてのメッセージを事前にフィルタリングする（図 7 の赤矢印）ことにより、膨大な量のランサムウェア攻撃をブロックします。メッセージは、複数のポリシー適用検証ステップを通じて評価されます。このステップは有効化しておく必要があります。行われる検証には、コンテンツおよびウイルス チェック、マルウェア チェック、スプーフィングが含まれます。マルウェア チェックは、Advanced Malware Protection（AMP）統合サービスを使用して実行されます。既知の悪意のある添付ファイルは（ファイル ハッシュやその他の認識機能に基づいて）除去可能ですが、メッセージ全体をドロップまたは隔離するのがベスト プラクティスです。不明な添付ファイルを含むメッセージは、隔離され、その間に添付ファイルが Threat Grid ファイル サンドボックス サービスでファイル分析されます。返される分析レポートの重大度に応じて、転送の決定が選択されます。クラウド E メール セキュリティ（CES）とメール システムを適切に統合すれば、レトロスペクションを実行し、他のユーザが取得する前に、感染した電子メールをクリーンアップできます。図 8 に、添付ファイルが除去されたメッセージを示します。

注:ごくまれに、悪意のあるファイルが最初に「安全」として分類されることがあります。これは、分析後に動作を変更する機能が悪意のあるファイルに備わっているためです。

図 8 -「件名」の前に通知が追加された電子メール



この電子メール システムは、URL の評価も実施し、メッセージにスパムやフィッシングが含まれているかどうかを見極め、URL のレピュテーションに基づいて適切なアクションを実行します。ランサムウェアに対する保護を強化するには、メッセージの変更フィルタとウイルス アウトブレイク フィルタもグローバルに有効化し、電子メール ポリシーに追加しなければなりません。アウトブレイク フィルタは、新しい脅威や複合型の攻撃に対処します。このフィルタでは、ファイルの種類、ファイル名、ファイル サイズ、メッセージ内の URL など 6 種類のパラメータを任意に組み合わせてルールを発行することができます。

Cisco Talos の脅威インテリジェンスは、アウトブレイクの詳細を把握すると、ルールを変更し、それに応じて隔離領域からメッセージを送信できます。アウトブレイク フィルタは、疑わしいメッセージ内の URL を書き換えることもできます。この受信者ブラウジング アクティビティは、Web インタラクション トラッキング（WIT）を有効化することで追跡できます。この新しい URL をクリックすると、受信者は Cisco Web セキュリティ プロキシを介してリダイレクトされます。当該の Web サイトのコンテンツはアクティブにスキャンされ、このサイトにランサムウェアをドロップする可能性があるマルウェアやエクスプロイト キットが含まれている場合は、アウトブレイク フィルタによってユーザにブロック画面が表示されます。このコンテンツが不明の場合は、図 9 に示したように決定オプションが提示されます。

図 9 - Web インタラクション トラッキングによって提示される決定オプション

DNS セキュリティ

DNS セキュリティは、インターネット上のサーバに到達するために名前を IP アドレスに変換するドメイン名解決ステップでセキュリティを強化します。この DNS レイヤでのセキュリティにより、Web サイトだけでなく、すべてのタイプの通信を実施している組織ネットワーク内外両方のデバイスを保護することができます。URL によってユーザが信頼できるように見えるサイトに誘導される最初の「起動」時には、Umbrella がこの DNS 要求をブロックし、ユーザがリンクをクリックした場合も、侵害されたサイトからリダイレクトされた場合でも、ユーザのブラウザが悪意のあるサイトに接続する前に安全な宛先とリプレースします（図 10 を参照）。

図 10 - DNS ブロック ページ

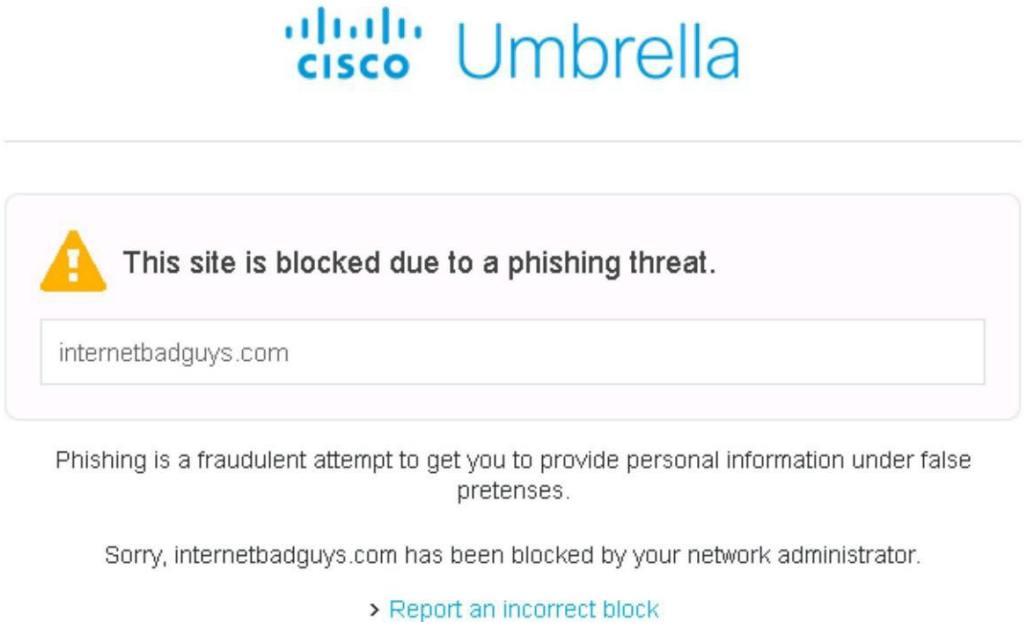
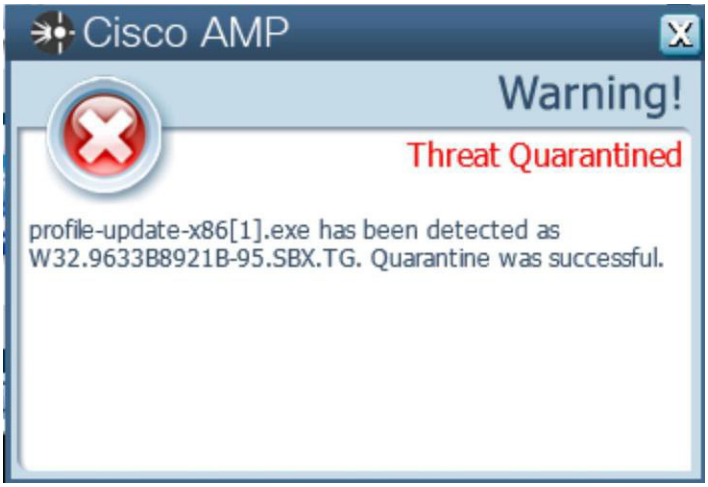


図 7 を再び参照すると、キル チェーンの各段階に複数の異なるドメイン ネットワークが存在し（青矢印）、それぞれのネットワークについてさまざまなレベルの脅威インテリジェンスが収集されます。最初のフィッシング サイトには、作成されて数時間または数分の新しいドメインを使用されることがありますが、その後使用される悪意のあるインフラストラクチャには、数日から数週にわたる既知の悪質な履歴情報が存在する可能性があります。キル チェーンの各段階は、DNS セキュリティに対して、侵害が発生する前にこの通信をブロックし、感染からユーザを保護する機会を提供します。さらに Umbrella は、感染が発生した場合に（黄矢印）、使用されるポートやプロトコルを問わずに C2 コールバックも阻止します。したがって、ランサムウェアによるファイルのドロップや、暗号化キーを取得するための C2 コールバックを防止することができます。

マルウェア対策によるセキュリティ

ホストベースのマルウェア対策は、最後の防御線であると同時に、多くの場合エンドツーエンドで暗号化された通信（パスワードで保護されたアーカイブ、https/sftp、チャット ファイル転送など）に対する唯一の防御でもあります。シスコの Advanced Malware Protection（AMP）は、ユーザのシステムに到達するすべてのファイルを分析します。悪意のあるファイルと断定されたファイルは、図 11 に示すように即座に隔離されます。

図 11 - AMP の隔離通知

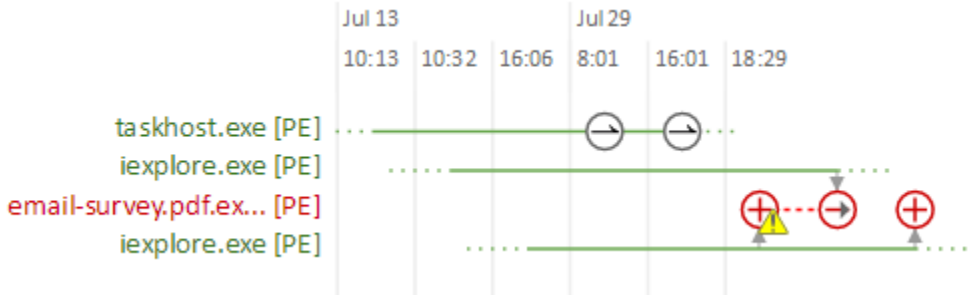


ファイルの拡散度が低い（ファイルが初めて検出された、または履歴情報がない）場合、ファイルは分析のために Threat Grid に自動的にアップロードされます（追加の設定とライセンスが必要）。Threat Grid は、最初の検査を回避したマルウェアを検出するレトロスペクティブ セキュリティを提供します。

AMP は、ファイル シグネチャ、ファイル レピュテーション、侵入兆候、サンドボックスの組み合わせを使用して、初期のエクスプロイト キットがユーザのシステムで実行されることを阻止し、またドロップされたランサムウェア ファイルの実行を停止して削除することができます。

さらに AMP は、システム上のすべてのファイル アクティビティを、ファイルの性質に関わらず継続的に分析して記録します。その後、動作の疑わしいファイルが見つかると、AMP はレトロスペクティブにファイルを検出し、アラートを送信します。AMP は、ネットワークに侵入した方法、転送先、現在の動作などを含め、長期的なマルウェアの動作について詳細な履歴を記録します。次に、セット ポリシーに基づいて、自動的または手動で脅威を封じ込め、修復することができます。図 12 に、AMP がシステム内のファイルのアクションを追跡する方法を示します。

図 12 - AMP のデバイス トラジェクトリ

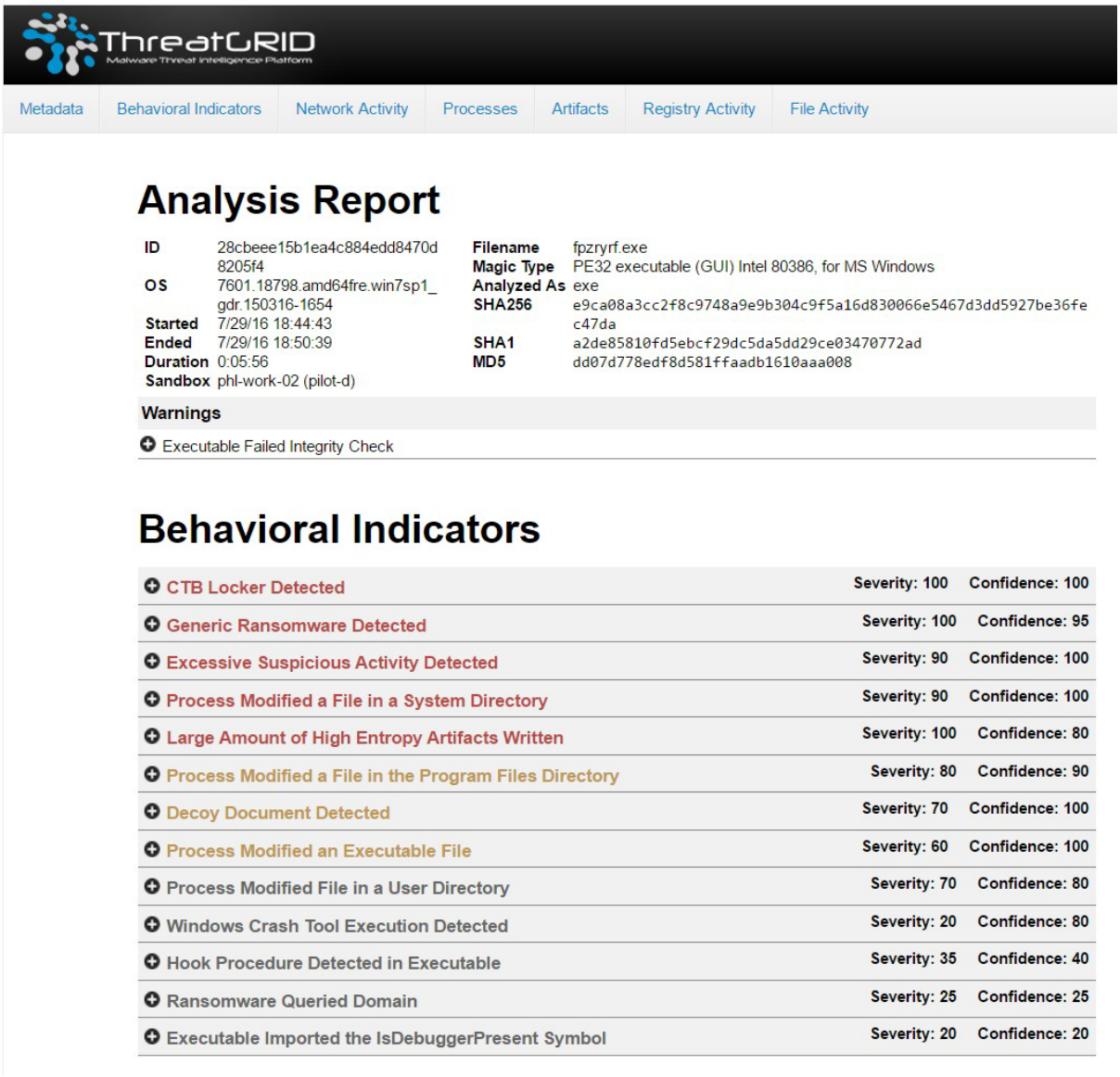


脅威インテリジェンス

Cisco Talos Group（Cisco Threat Intelligence Group）は、毎日数百万のマルウェア サンプルと数テラバイトのデータを分析し、そのインテリジェンスを AMP に送信することにより、24 時間 365 日保護を提供しています。また、高度なサンドボックス機能が、500 以上の動作指標に対して未知のファイルの静的/動的分析を自動的に実行し、ステルス性の脅威を発見します。

Talos と Threat Grid 脅威分析エンジン両方を組み合わせることで、疑わしい電子メール添付ファイルやファイルをサンドボックスで分析し、20 ～ 30 分という短時間でマルウェアまたはランサムウェアとして分類することができます。ただし、拡散度が低いファイルの場合には、分析で誤検出が発生する可能性を最低限に抑えるために、分析と特定に若干長い時間がかかることがあります。図 13 に、ソリューションの検証テストで使用されたマルウェア サンプルの分析レポートを示します。

図 13 - ファイル分析レポート



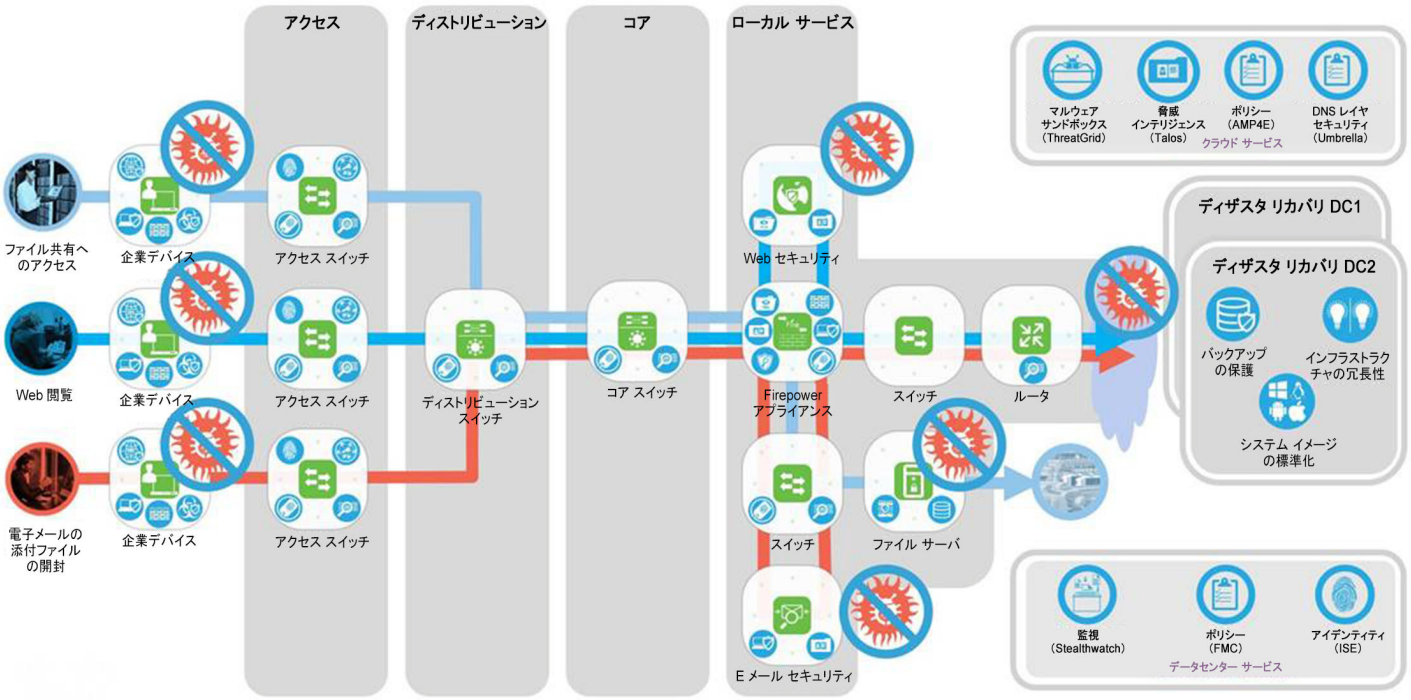
最初の検査を回避したマルウェアのレトロスペクティブ セキュリティ インテリジェンスは、Talos Threat Intelligence を介して、電子メール サービスとホスト マルウェア対策サービスの両方と共有されます。こうした悪意のあるファイルの現在のインスタンスと将来発生するインスタンスはすべて、ブロックまたは削除されます。

フェーズ 2 - ランサムウェアの検出と封じ込め

フェーズ 2 のアーキテクチャは、フェーズ 1 で導入された機能を基盤に構築され、ネットワーク監視および適用機能が全体に導入された、完全にセグメント化されたロールベースのインフラストラクチャです。図 14 に、SAFE のセキュア キャンパス PIN と、電子メール、Web、ファイル共有のビジネス ユース ケース フローの階層を使用したサンプルのキャ

ンパス アーキテクチャを示します。これらのフローの保護に必要な各機能は、適切なシステム プラットフォーム（緑色の四角）に適用されているか、クラウド サービスとして表示されています。

図 14 - フェーズ 2 のサンプル キャンパス アーキテクチャ



高度な Web セキュリティ

シスコの Web セキュリティは、Web フィルタリングおよび Web レピュテーション スコアを通じて、75 以上のコンテンツ カテゴリに分類されるフィルタを適用することで、5 千万以上の既知の Web サイトへのアクセスを制御します。この制御は、Web ページ、個々の Web パーツ、マイクロアプリケーションへのアクセスに対応するため、従業員は作業に必要なサイトにアクセスすることができます。また、ソーシャル ネットワーキング サイトやその他のサービスなど、既知の信頼できるドメインでホストされているランサムウェアに対してきめ細かい制御と検査を適用します。

- 場所に関係なくすべてのユーザを保護するクラウド ベースまたはオンプレミス型の Web セキュリティ ゲートウェイ
- 100 人から 10,000 人以上のユーザに対応できるスケーラビリティ
- Web セキュリティ、アプリケーション制御、管理、レポートを完全に統合
- Talos Threat Intelligence の活用による、ゼロデイ脅威からの包括的な保護

アウトブレイク インテリジェンスは、Web ページのコンポーネントを安全性の高い仮想エミュレーション環境で実行することで、個々のコンポーネントの動作を確認し、マルウェアまたはランサムウェアがあればそれをブロックします。

ファイル レピュテーション機能は、組織のネットワークを通過する際に各ファイルのフィンガープリントが取得します。これらのフィンガープリントが AMP のクラウド ベースのインテリジェンス ネットワークに送信され、レピュテーションが判定されます。攻撃が発生したら、ファイル レトロスペクション機能を使用して、ファイルの性質が侵入後にどのように変化したかを追跡できます。マルウェアと判明した場合は、そのファイルがどこから侵入して現在どこに配置されているかを特定し、今後の侵入を阻止するための対策を講じます。さらに、シスコの Cognitive Threat Analytics（CTA）統合機

能により、振る舞い分析、異常検出、マシン学習を通じてマルウェア感染の兆候が積極的に特定されるため、脅威特定までの時間を短縮できます。

ネットワークの監視

Cisco Stealthwatch は、攻撃前、攻撃中、および攻撃後に、組織全体に可視性とセキュリティ インテリジェンスを提供します。絶えずネットワークを監視し、ランサムウェアのアウトブレイクが発生した場合には、リアルタイムでの脅威検出およびインシデント対応フォレンジック機能を提供します。

Stealthwatch は、ネットワークをセンサーとして活用して、インフラストラクチャとワークステーションから NetFlow データを取得して分析し、組織と組織内ユーザの通常の通信のベースラインを作成します。このベースラインがあれば、高度な攻撃者がネットワークに侵入し、分析やランサムウェアの配備を試みたときにはるかに簡単に特定することができます。また、マルウェア、分散型サービス妨害（DDoS）攻撃、標的型攻撃（APT）、内部脅威などを特定できます。ノースサウス（インターネットとサーバ間のトラフィック）およびイーストウェスト（データセンター内のサーバ間トラフィック）の状況を監視し、非常に広範な攻撃を検出します。

Stealthwatch は、Cisco Identity Services Engine（ISE）および Cisco TrustSec テクノロジーと連携して機能します。この統合を通じて、ユーザとシステムを特定し、手動隔離時のシステムの動作に基づいて重要なネットワーク資産を適切にセグメント化することができます。

ID ベースのセグメンテーション

ランサムウェアの拡散に対する組織の防御を最大限に高めるには、職務の遂行に必要なリソースとシステム ファイル共有へのアクセスのみをユーザに許可する必要があります。ランサムウェアに感染したシステムは、現在のシステム ユーザのクレデンシャルを使用して暗号化または感染可能な、ネットワーク内の他のファイル共有ドライブや脆弱なシステムを探そうとします。したがって、ネットワーク全体に広まる前にランサムウェアを特定し、感染したデバイスをセグメント化することがきわめて重要です。

Cisco TrustSec と Cisco ISE は、ネットワークをセグメント化し、ロールベースのアクセス制御を施行します。Cisco TrustSec テクノロジーを使用することで、ネットワークのセグメントやリソースに対するアクセスを、特定のセキュリティ ポリシーに従ってコンテキストおよびユーザ、デバイス、場所ごとに制御できます。

Security Group Tag（SGT）の適用では、メンテナンス請負業者のクレデンシャルを持つユーザ システムは、ネットワーク トポロジに関わらず、またはネットワークへのアクセスに有線/ワイヤレスのどちらを使用しているかどうかに関わらず、財務データへのアクセスをブロックされます。

Stealthwatch との統合により、ネットワーク上の異常な動作に基づいて感染システムが特定された場合には、Cisco ISE は学習したこの動作に基づいて認証の変更を開始し、異なる SGT ポリシーを適用してこのシステムを隔離し、ネットワークの別の部分を即座に保護することができます。

インフラストラクチャのセグメンテーションと侵入防止

NGFW によるセグメンテーション

Cisco Firepower 次世代ファイアウォール（NGFW）は、統合された管理機能を備えたフル統合型、脅威重視型の次世代ファイアウォールです。ネットワークからエンドポイントまで対応するファイアウォール、アプリケーション制御、脅威防

御、高度なマルウェア防御機能の包括的な統合ポリシー管理を提供します。これらの各機能は、ランサムウェアの脅威に対する防御の追加または代替階層を提供します。組織がランサムウェア攻撃の標的にされると、これらの各機能が連携してネットワークの偵察を阻止します。さまざまなネットワーク リソース間の通信のブロック機能により、ビジネス通信に必要な許可されたユーザ、システム、プロトコルにインフラストラクチャをセグメント化し、データへの侵入、データの悪用、データの盗用、暗号化キーの取得、ネットワーク内での永続化に使用されたリソースをブロックします。

Firepower NGFW は、アクセスを制御して攻撃を阻止し、マルウェアに対して防御する包括的なポリシー管理を実現します。攻撃側が侵入に成功してしまった場合も、攻撃を追跡して封じ込め、さらに攻撃から回復するためのツールを提供します。

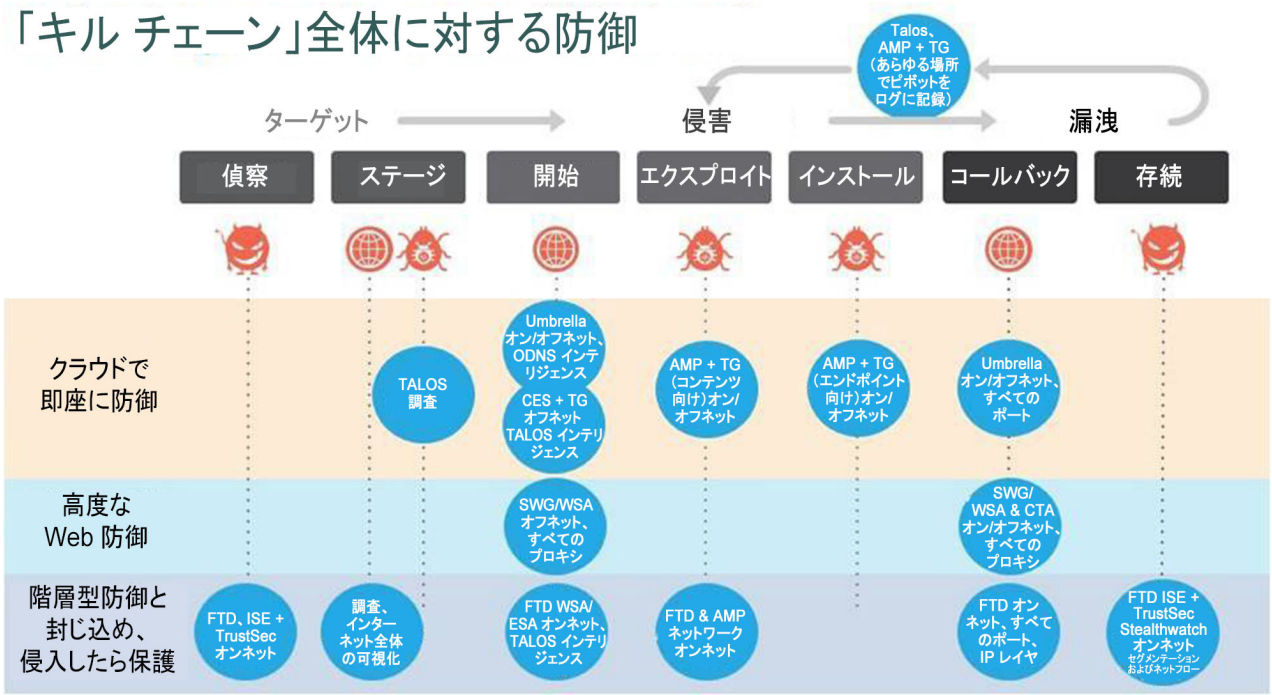
Firepower Management Center による管理

Firepower Management Center は、ネットワーク セキュリティ ソリューションの管理における中枢として機能します。すべてのファイアウォールを対象とした完全かつ包括的なユニファイド マネジメント、アプリケーション制御、侵入防御、URL フィルタリング、そして Firepower プラットフォーム上の高度なマルウェア防御を実現します。ファイアウォールの管理からアプリケーションの制御までを簡単に実施して、ランサムウェアのアウトブレイクを調査し、修復できます。Cisco Firepower Management Center と Stealthwatch の振る舞い分析機能により、セキュリティ インテリジェンスを共有し、ISE を通じた脅威の封じ込めを自動化することができます。

アーキテクチャの概要

上記のフェーズで紹介した各製品は、図 15 に示したキル チェーン全体にわたる攻撃に対する防御に必要な機能の要件を満たしています。

図 15 - キル チェーンに対応する製品の機能



フェーズ 1—迅速な防止機能の実装

表 3 の製品は、ランサムウェア防御ソリューションのフェーズ 1 の検証テストに実装されました。以下の各製品のセクションでは、ランサムウェアに対する防御を最大限に高めるために、通常のインストール後にどのようにカスタマイズしたかを説明します。

表 3 - 検証されたソリューションに含まれる製品

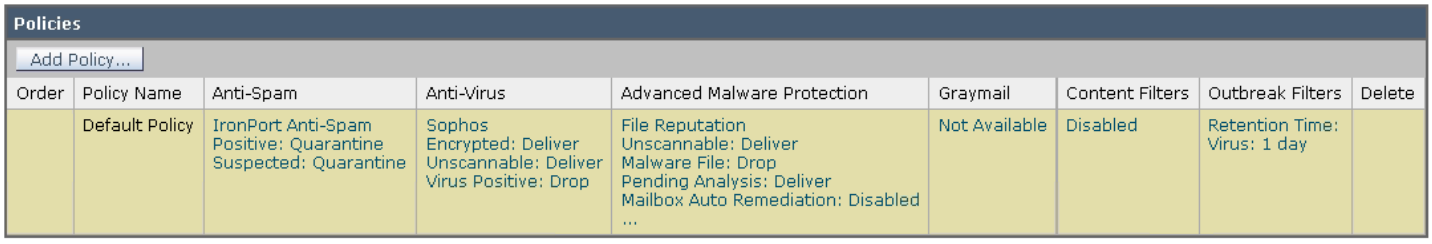
製品	説明	プラットフォーム	バージョン
クラウド E メール セキュリティ	AMP による電子メール セキュリティ	クラウド	v10.0.0-071
Umbrella Roaming およびネットワークベース DNS 保護	組織外のローミング ユーザ向けの DNS セキュリティ。すべての内部デバイスおよびシステム用のネットワーク DNS。	クラウド/ローミング クライアント	v2.0.189
Advanced Malware Protection（AMP）	エンドポイント向けホストベース マルウェア対策保護	クラウド/クライアント エンドポイント	v4.4.2.10200

Cisco クラウド E メール セキュリティ

以下に、クラウド E メール セキュリティ サービスが起動し、通常に動作し、メール プロセス フローと完全に統合された後に、ランサムウェアやその他の標的型攻撃（APT）に対する防御を最大限に高めるために E メール セキュリティを設定する方法の概要を示します。新たに CES をインストールする場合、デフォルト ポリシーは図 16 のようになります。

ステップ 1　　[メールポリシー（Mail Policies）] > [受信メールポリシー（Incoming Mail Policies）] の順に選択します。

図 16 - 新規導入時のデフォルト ポリシー



[受信メールポリシー（Incoming Mail Policies）] 内で、[デフォルトポリシー（Default Policy）] 要素の [Advanced Malware Protection]、[コンテンツフィルタ（Content Filters）]、[アウトブレイクフィルタ（Outbreak Filters）] を編集します。

Advanced Malware Protection

次に、Advanced Malware Protection を使用して、受信メール ポリシーのファイル レピュテーション スキャニングとファイル分析を設定します。Advanced Malware Protection は、電子メールの添付ファイルに含まれるゼロデイ攻撃や標的型のファイル ベース脅威からの防御のために、次の機能を提供します。

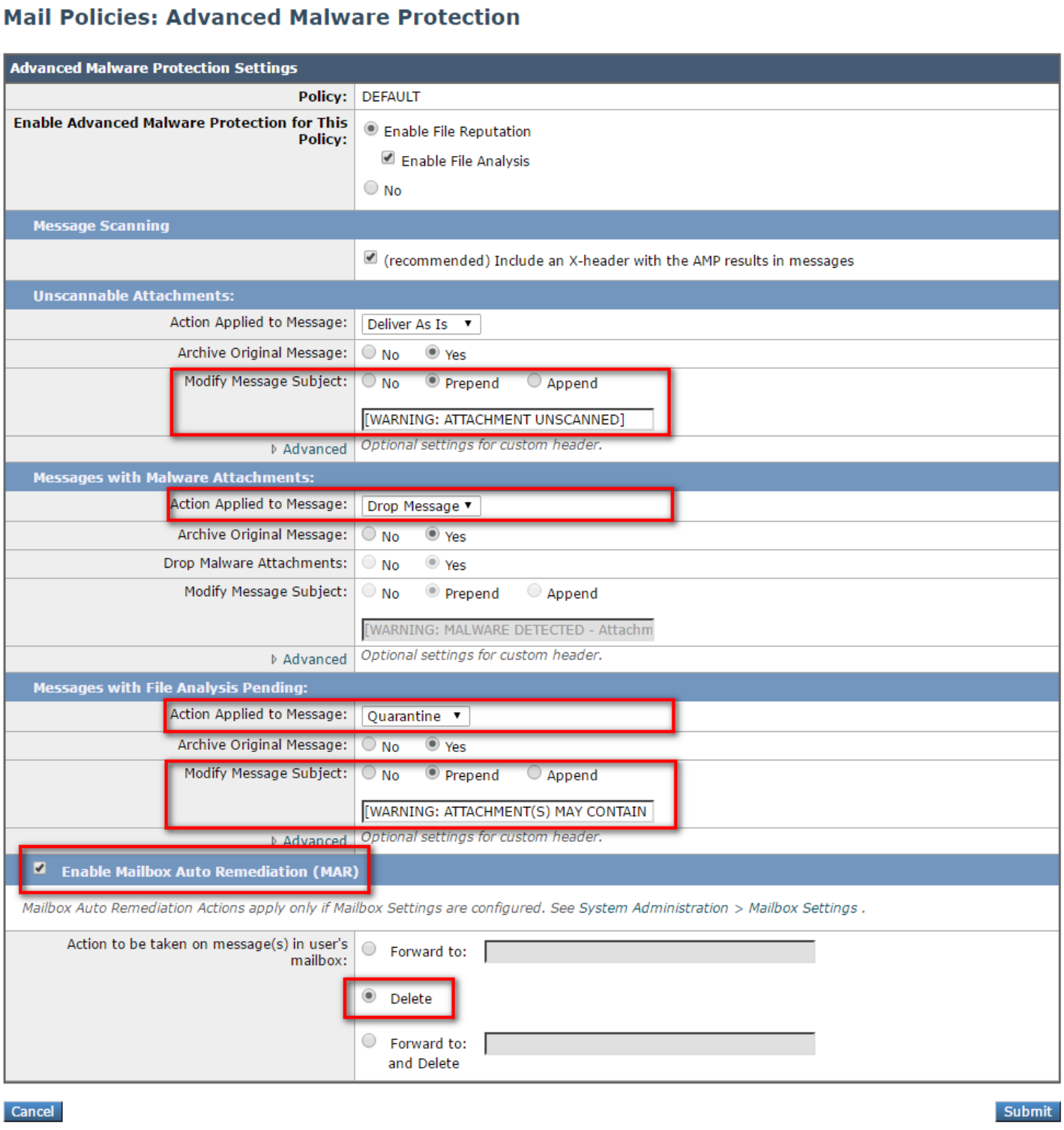
- 既知のファイルのレピュテーションを取得する
- レピュテーション サービスにまだ認識されていない特定のファイルの動作を分析する

- 新しい情報が利用可能になり次第、新しい脅威を継続的に評価し、組織のネットワークに侵入した後に脅威であることが判明したファイルについて通知する

これらの機能は、受信メッセージに対してのみ使用できます。発信メッセージに添付されたファイルは評価されません。

ステップ 2　　[デフォルトポリシー（Default Policy）] の [Advanced Malware Protection] 列のリンクをクリックして修正します。

図 17 - [デフォルトポリシー（Default Policy）] の [Advanced Malware Protection]



メッセージの添付ファイルのステータスに基づいて、警告情報を電子メール メッセージの件名の前に追加するのがベスト プラクティスです。

ステップ 3　[スキャン不能な添付ファイル（Unscannable Attachments）] および [ファイル分析保留中（File Analysis Pending）] 両方に対して、[メッセージ件名を修正（Modify Message Subject）] を設定します。

[マルウェアが添付されているメッセージ（Messages with malware attachments）] は、添付ファイルを除去するか、警告とともに配信するか、全体をドロップすることができます。最も一般的なのは、メッセージ全体のドロップです。

ステップ 4　[メッセージに適用するアクション（Action Applied to Message）] > [メッセージのドロップ（Drop Message）] を設定します。

[ファイル分析保留中のメッセージ（Message with File Analysis Pending）] は、配信することも隔離することもできます。このような電子メール メッセージは、分析エンジンから結果を取得するまで隔離するのがベスト プラクティスです。添付ファイルが悪意のあるものの場合は、[添付ファイル（Attachments）] 設定に従います。結果が不明として返された場合、このメッセージは配信されますが、メッセージの件名の前に警告が追加されます。

ステップ 5　[メッセージに適用するアクション（Action Applied to Message）] > [隔離（Quarantine）] を設定します。

[メールボックスの自動修復（Mailbox Auto Remediation（MAR））] を有効化すると、後で脅威ベクトルが悪意のあるものに変更されたときに、ユーザのメールボックスに配信済みのメッセージを削除できます。

ステップ 6　[有効化（Enable）] をチェックして MAR を有効にし、アクションを [削除（Delete）] に設定します。

ステップ 7　これらの変更が終了したら、[送信（Submit）] をクリックします。

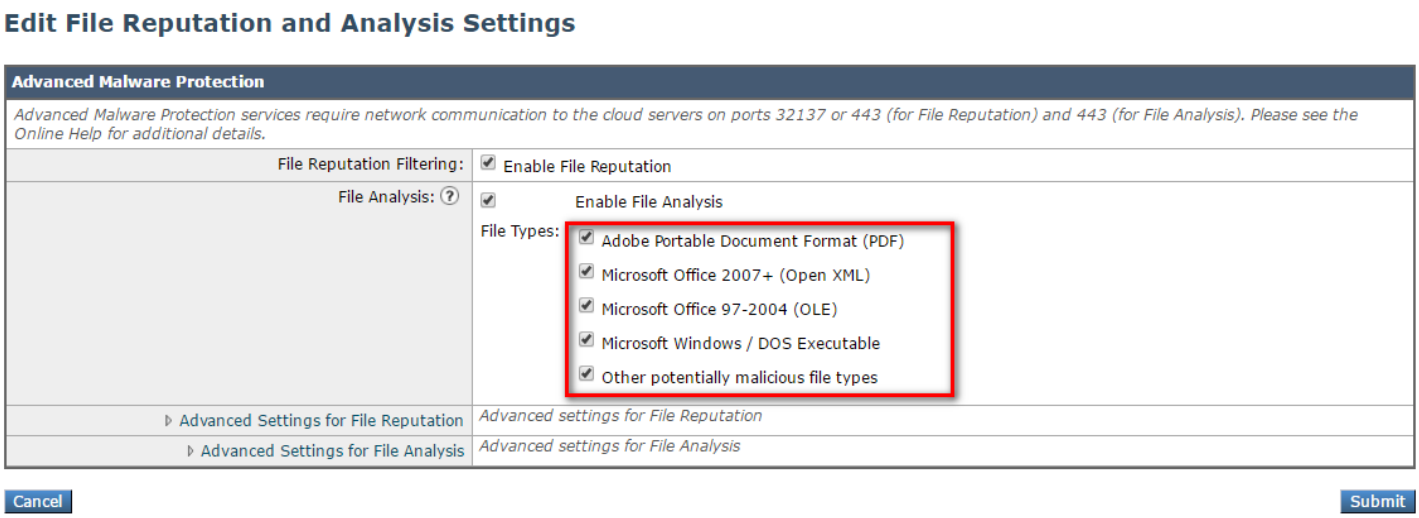
ファイル レピュテーションおよび分析サービスは、AMP エンジンを使用して、上記のポリシーで有効化されたようにメッセージを検査します。新しい実装の場合、ファイル分析はデフォルトで有効化されており、Windows および DOS 実行可能ファイルが検査されますが、分析する追加のファイル タイプも選択する必要があります。

ステップ 8　[セキュリティサービス（Security Services）] > [ファイルレピュテーションと分析（File Reputation and Analysis）] を選択します。

ステップ 9　[グローバル設定を編集（Edit Global Settings）] を選択します。

ステップ 10　図 18 のように追加のファイル タイプを有効にします。[送信（Submit）] をクリックします。

図 18 - ファイル分析設定



コンテンツ フィルタリング

一部のランサムウェアとエクスプロイト キットは、スクリプトとしてメッセージに添付されます。こうしたスクリプトはまだファイル分析で検査されませんが、ユーザが開くとシステム上でローカルで実行され、Web ブラウザのセキュリティを迂回することができます。ベスト プラクティスとして、コンテンツ フィルタを使用してこれらのタイプのスクリプト添付ファイル（.js、.wsf、.vbs）を削除することを推奨します。

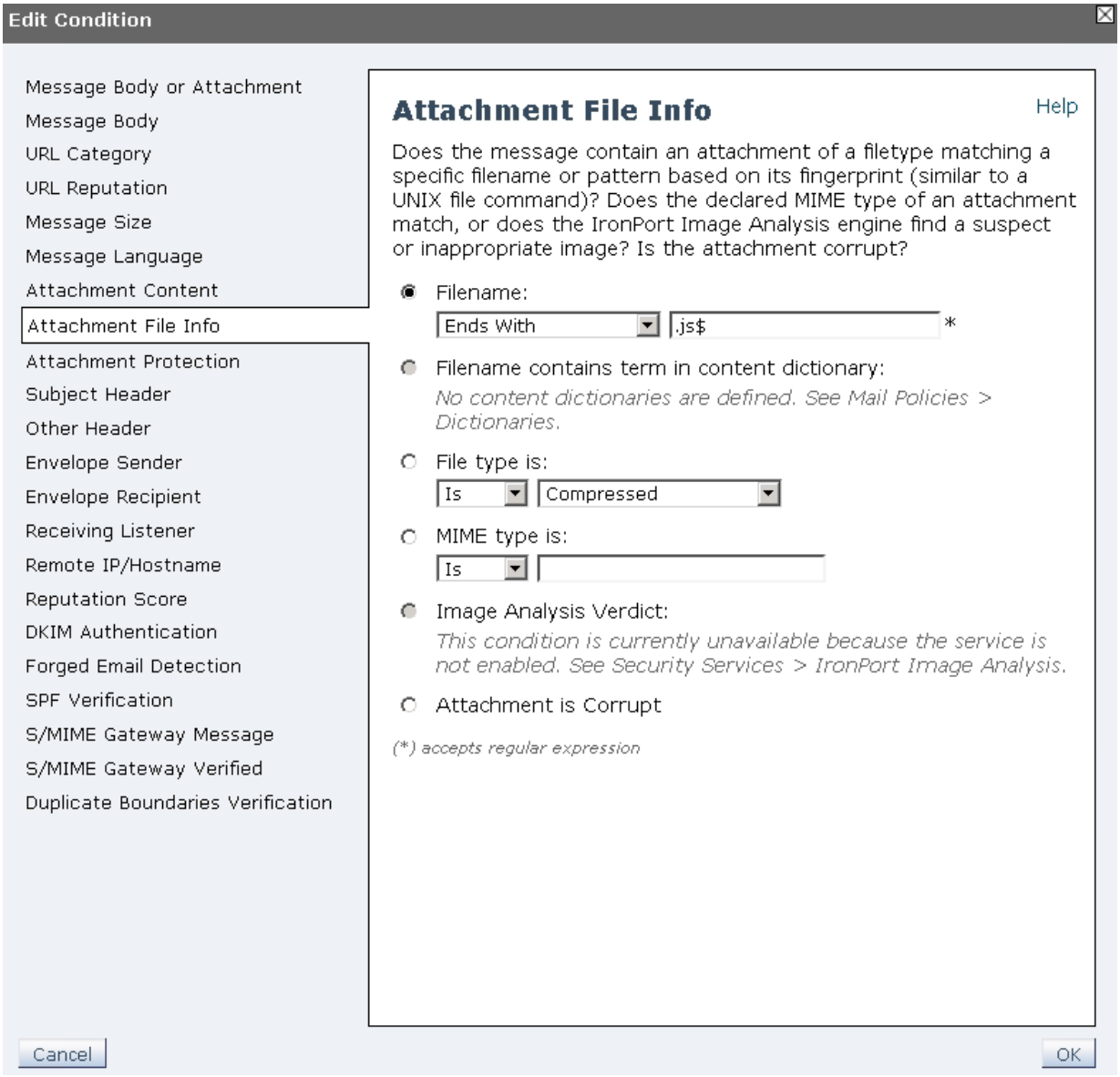
これらのスクリプトが添付されているメッセージをドロップする新しい受信コンテンツ フィルタを作成します。

ステップ 11　[メールポリシー（Mail Policies）] > [受信コンテンツフィルタ（Incoming Content Filters）] > [フィルタの追加（Add Filter）] を選択します。

ステップ 12　フィルタに名前を付け、説明を追加します。
[名前（Name）]：BlockScriptAttachments
[説明（Description）]：スクリプト添付ファイル（.js、.wsf、.vbs）をブロックしてランサムウェアからユーザを保護する

ステップ 13　[条件の追加（Add Condition）] > [添付ファイル情報（Attachment File Info）] > [.jsで終了するファイル名（Filename Ends With .js）] をクリックします。

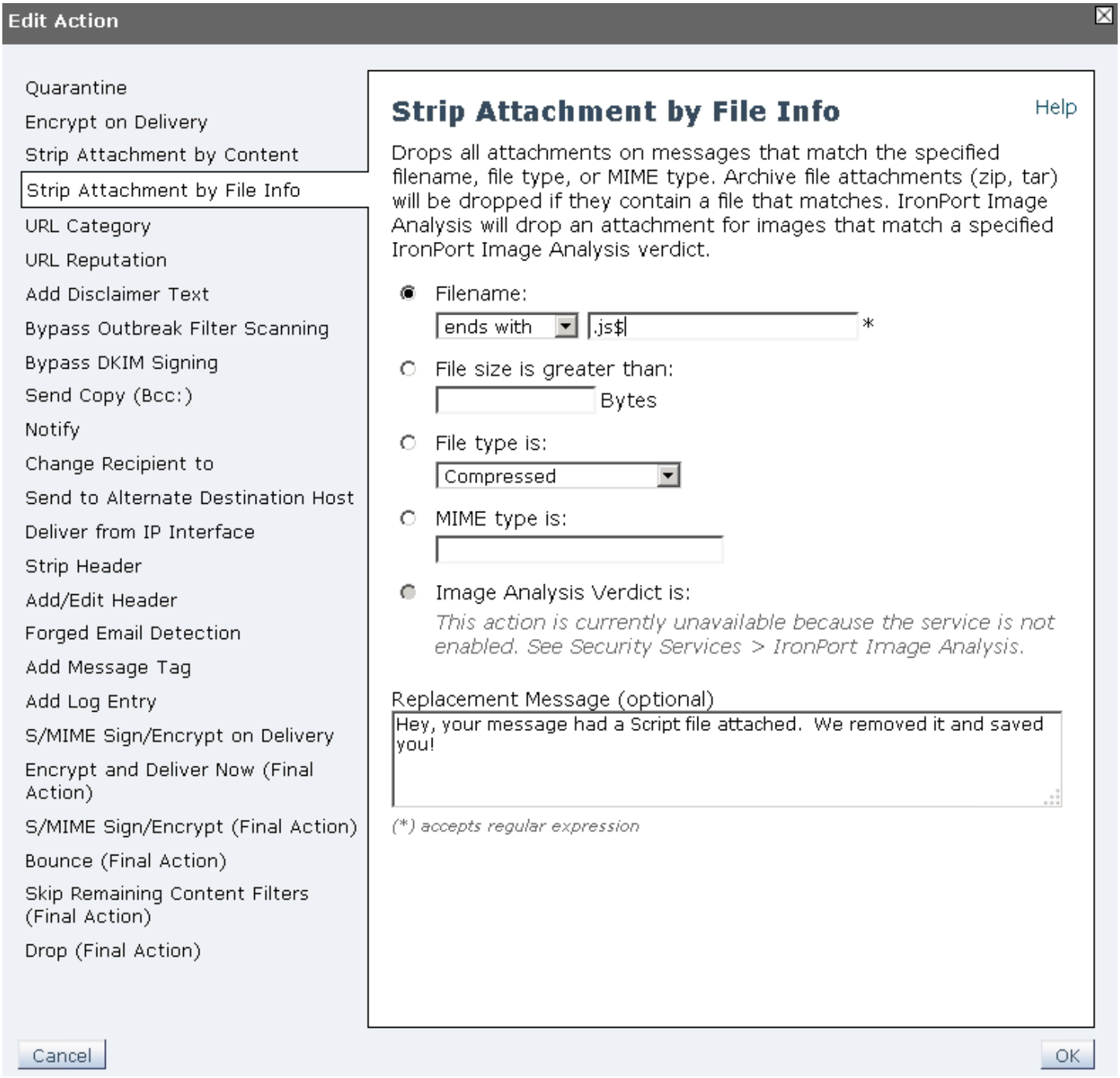
図 19 - 新しいコンテンツ フィルタ条件



ステップ 14　　[OK] をクリックします。

ステップ 15　　[アクションの追加（Add Action）] > [ファイル情報によって添付ファイルを除去（Strip Attachment by File Info）] > [.js$で終了するファイル名（Filename ends with .js$）] をクリックします。

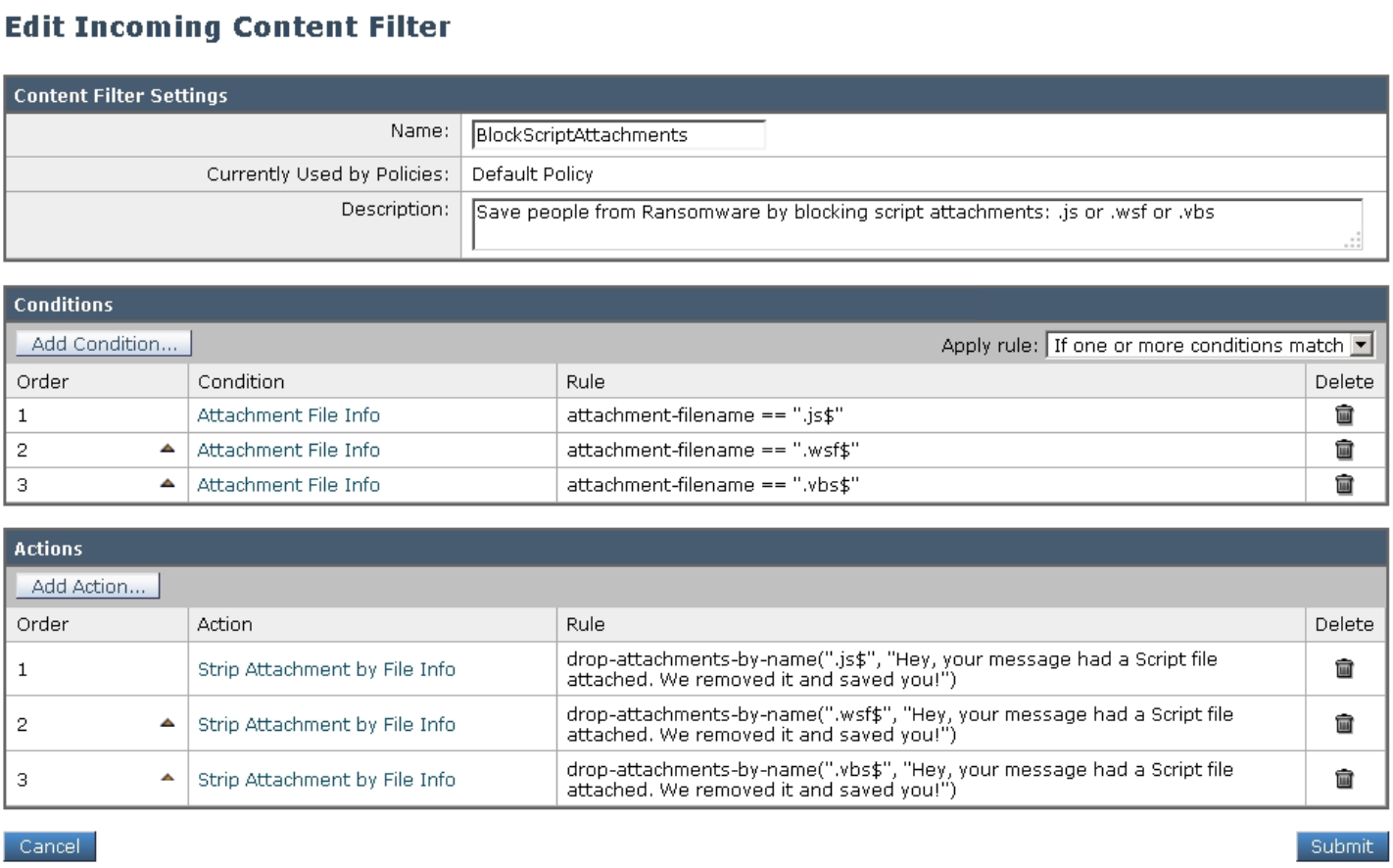
図 20 - 新しいコンテンツ フィルタ アクション



ステップ 16　　[OK] をクリックします。

.wsf および .vbs ファイル タイプに対してもステップ 13 ～ 16 を繰り返します。最終的なフィルタには、図 21 に示すように 6 つすべてのフィルタが含まれます。

図 21 - スクリプト ファイルを削除するコンテンツ フィルタ



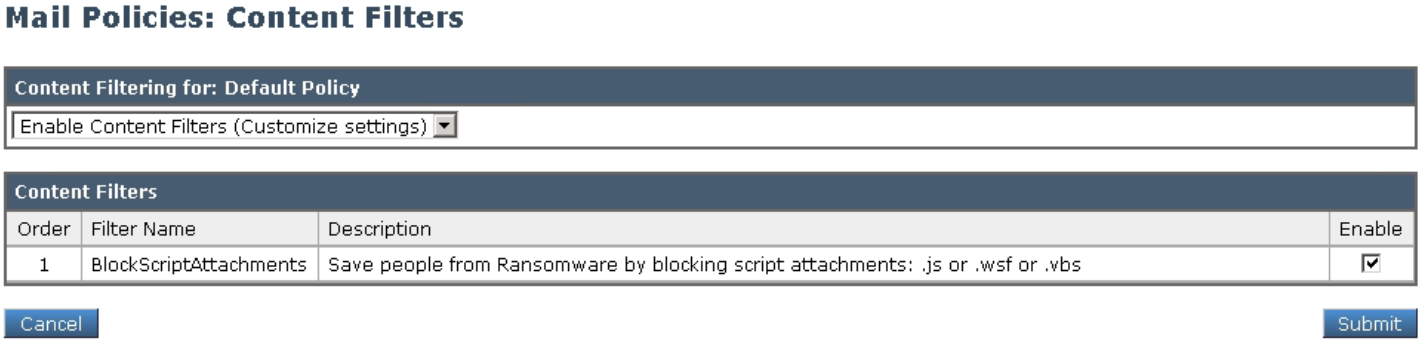
ステップ 17　　終了したら、[送信（Submit）] をクリックします。

デフォルト ポリシーでの新しいコンテンツ フィルタの有効化

ステップ 18　　[デフォルトポリシー（Default Policy）] の [コンテンツフィルタ（Content Filter）] 列の [メールポリシー（Mail Policies）] > [受信メールポリシー（Incoming Mail Policies）] > [無効（Disabled）] をクリックして修正します。

ステップ 19　　ドロップダウンで [コンテンツフィルタを有効にする（Enable Content Filters）] を選択し、新たに作成したフィルタの [有効化（Enable）] 列をチェックします。

図 22 - コンテンツ フィルタリングとフィルタの有効化



ステップ 20　　終了したら、[送信（Submit）] をクリックします。

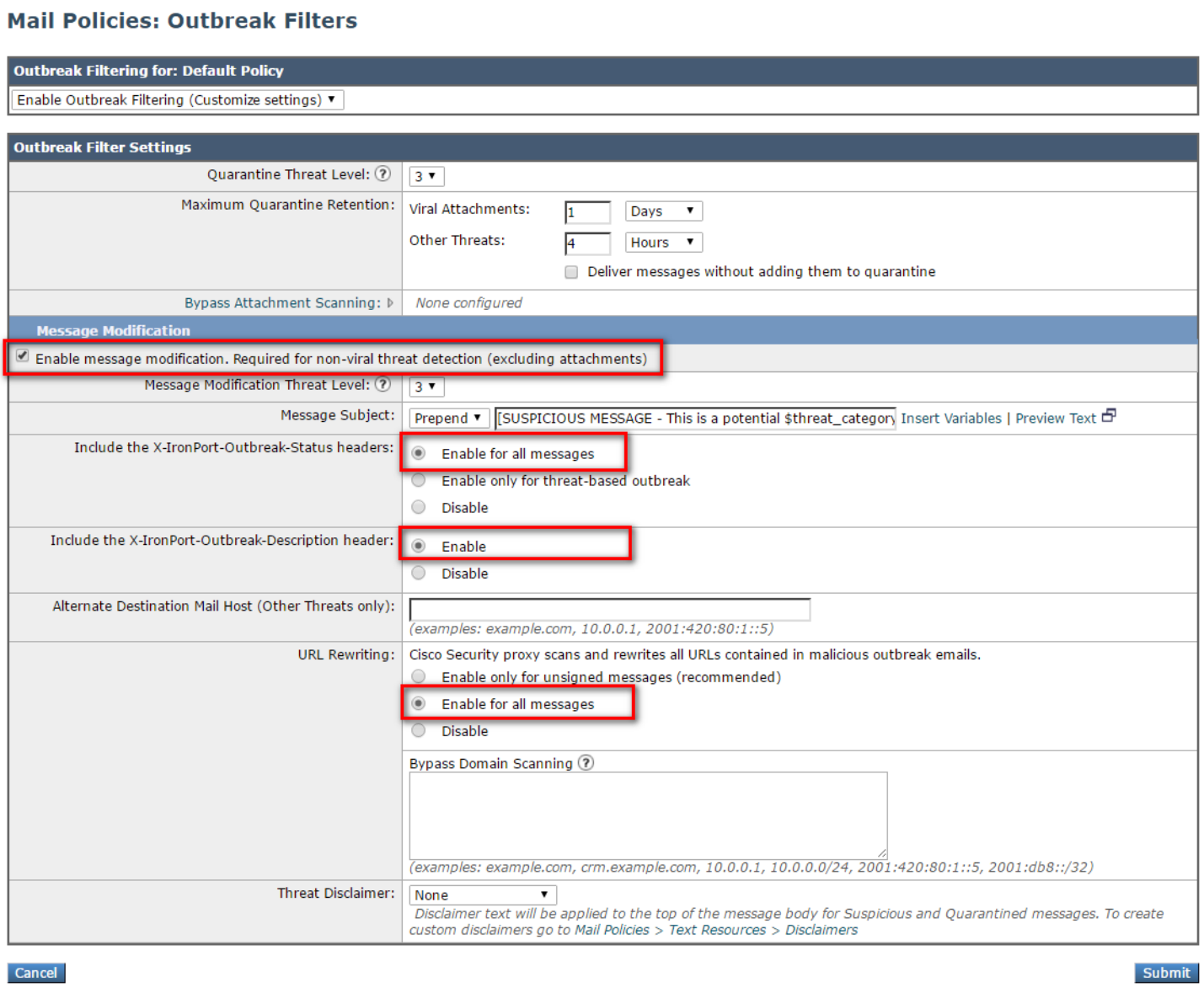
アウトブレイク フィルタ

アウトブレイク フィルタは大規模なウイルスの拡散や小規模な非ウイルス性の攻撃（フィッシング詐欺およびマルウェア配布など）が発生した際にネットワークを保護します。シスコは、拡散するアウトブレイクに関するデータを収集し、リアルタイムで脅威インテリジェンスを更新することにより、組織のユーザへのこれらのメッセージの到達を防止します。

新規インストールの場合、アウトブレイク フィルタはデフォルトで有効化されていますが、メッセージ上の URL の書き換えを可能にする、メッセージの変更も有効化するのがベスト プラクティスです。この機能により、特定のメッセージを開こうとするユーザに警戒するように通知されます。

ステップ 21　[デフォルトポリシー（Default Policy）] の [アウトブレイクフィルタ（Outbreak Filter）] 列の [メールポリシー（Mail Policies）] > [受信メールポリシー（Incoming Mail Policies）] > [保持期間（Retention Time）] をクリックして修正します。

図 23 - アウトブレイク フィルタのメッセージ通知



ステップ 22　メッセージの変更の有効化が終了したら、[送信（Submit）] をクリックします。

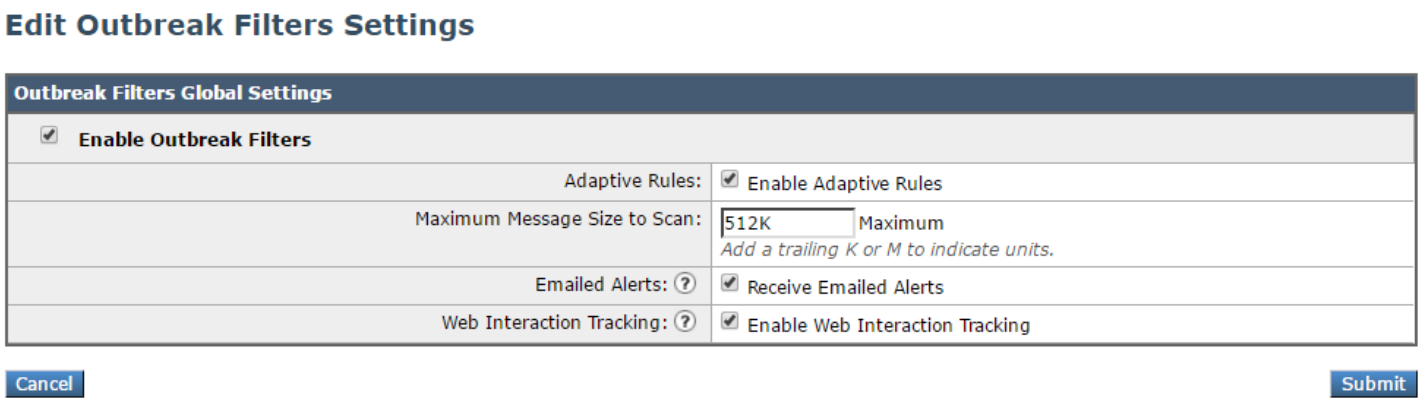
Web インタラクション トラッキング

Web インタラクション トラッキングにより、管理者は Cisco E メール セキュリティによって書き換えられた URL をクリックするエンド ユーザを追跡することができます。悪意のあるリンク付きのメッセージを、そのリンクをクリックしてしまったユーザやその結果を含めて追跡することもできます。

デフォルトでは、Web インタラクション トラッキングは無効になっています。アウトブレイク フィルタに書き換えられた URL を追跡するには、Web インタラクション トラッキングを有効にする必要があります。

ステップ 23　[セキュリティサービス（Security Services）] > [アウトブレイクフィルタ（Outbreak Filters）] > [グローバル設定を編集（Edit Global Settings）] を選択します。

図 24 - アウトブレイクの Web インタラクション トラッキング

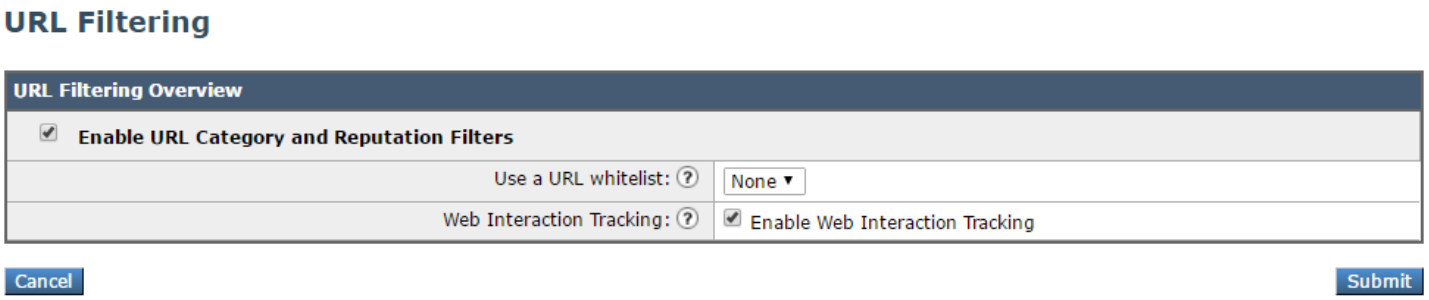


ステップ 24　[電子メールアラート（Email Alerts）] および [Webインタラクショントラッキング（Web Interaction Tracking）] チェックボックスをオンにします。そして、[送信（Submit）] をクリックします。

ポリシーに書き換えられた URL も追跡するには、URL フィルタリング設定でも Web インタラクション トラッキングを有効にする必要があります。

ステップ 25　[セキュリティサービス（Security Services）] > [URLフィルタリング（URL Filtering）] > [有効（Enable）] を選択します。

図 25 - URL フィルタの Web インタラクション トラッキング



ステップ 26　[URLカテゴリおよびレピュテーションのフィルタの有効化（Enable URL Category and Reputation Filters）] チェックボックスと [Webインタラクショントラッキング（Web Interaction Tracking）] をクリックします。そして、[送信（Submit）] をクリックします。

すべての変更が終了したら、変更を確定してこれらの新しい設定を有効にする必要があります。

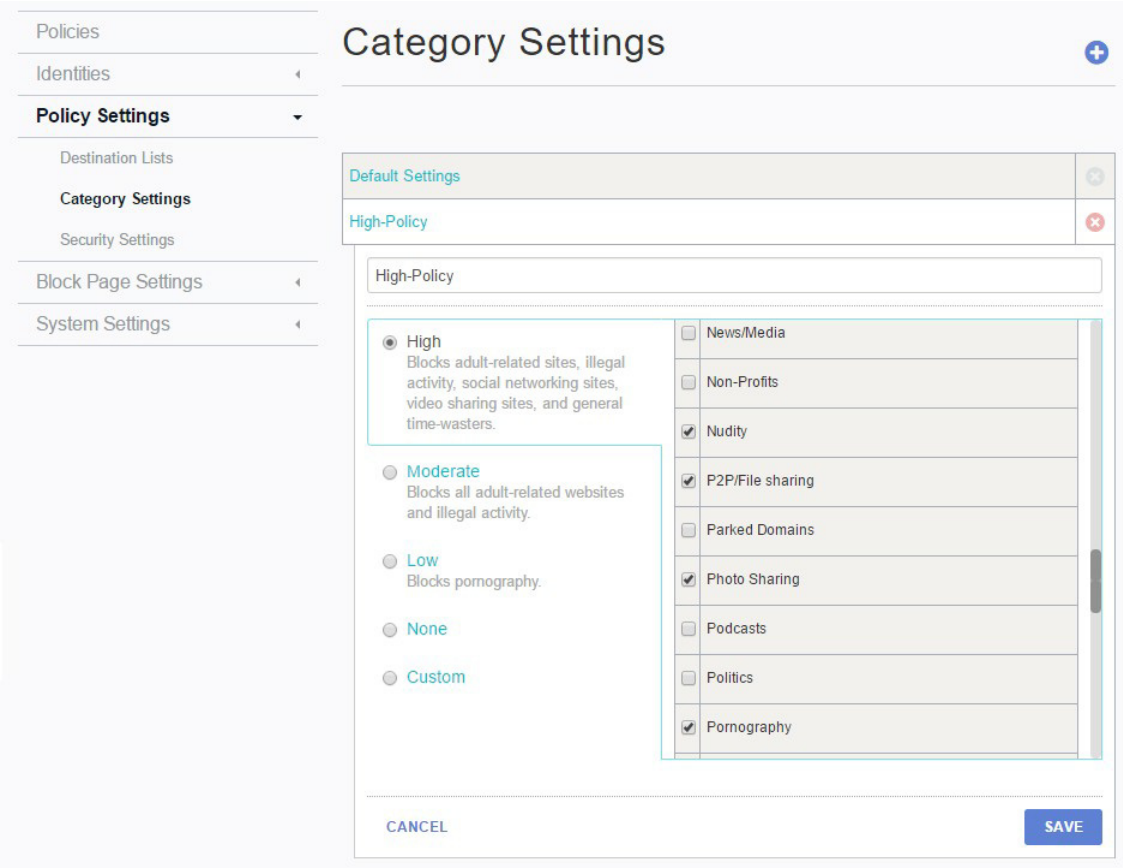
ステップ 27　　右上の [変更の確定（Commit Changes）] ボタンをクリックし、適切なコメントを入力したら、[変更の確定（Commit Changes）] をクリックして送信します。

Cisco Umbrella による DNS セキュリティ

Cisco Umbrella

完全な Cisco Umbrella サービスは、ネットワーク、ローミング、モバイル デバイスを保護することができます。このサービスは、非常に包括的な一連のポリシー オプションを提供しています。別のコンテンツ カテゴリへのアクセスの抑制オプションは、ランサムウェアがホストされている可能性があるドメイン（ギャンブル、P2P/ファイル共有、憎悪/差別など）に誘導されるリスクも低減できます。カスタム ポリシーを作成するだけでなく、設定済みの複数のポリシーを使用することもできます。図 26 に、検証テストで使用された Umbrella の高（High）ポリシーを示します。

図 26 - Umbrella の高（High）ポリシー

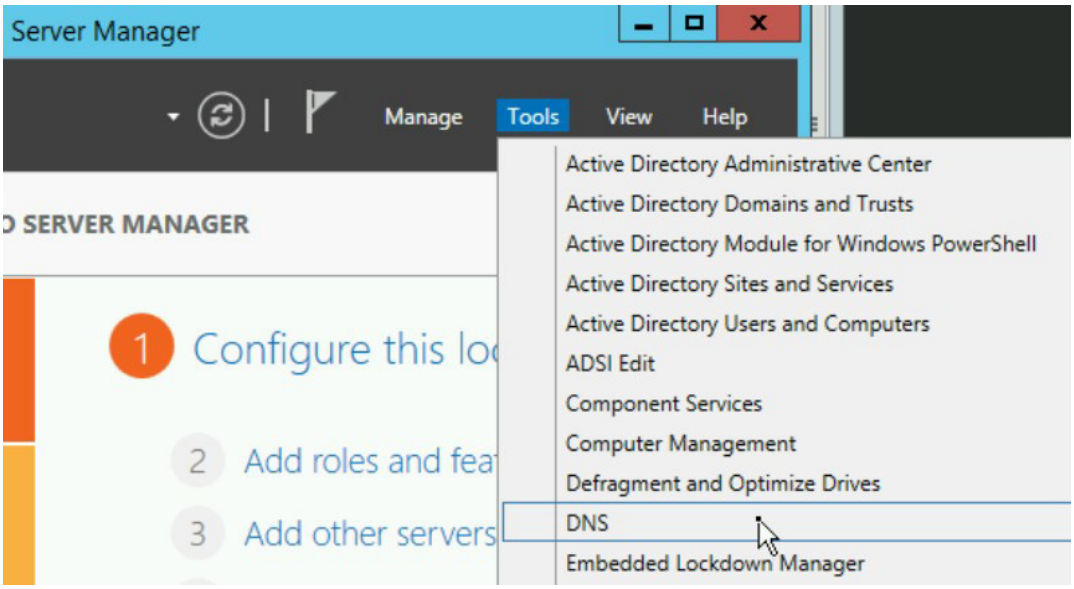


独自の内部ネットワーク DNS サーバを導入している組織では、Umbrella をネットワーク全体に簡単に有効化できます。外部ドメインのルート検索を自身で実行する代わりに、Umbrella サーバをフォワーダとして使用するように DNS サーバを設定します。これにより、内部ネットワーク システムに Umbrella クライアントを導入する必要がなくなり、ネットワーク内のすべての要素を保護するシンプルなクライアントレス環境が実現します。

以下に、検証テストと同様に Windows DNS フォワーダとして Umbrella を使用するように設定する方法の概要を示します。

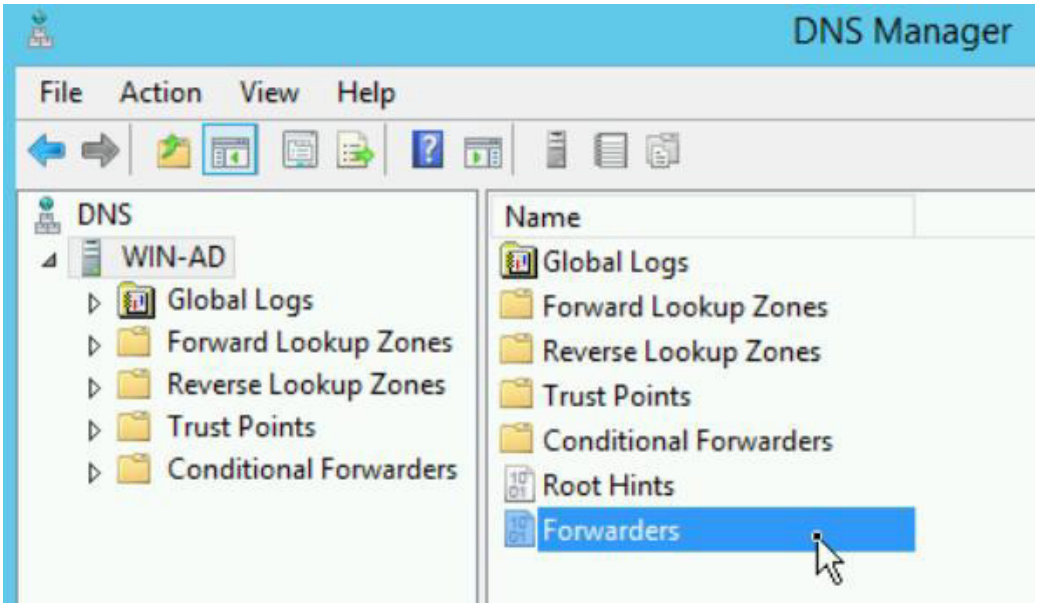
ステップ 1　　Server Tools の下で、Windows DNS Manager を開きます。

図 27 - Windows DNS Manager



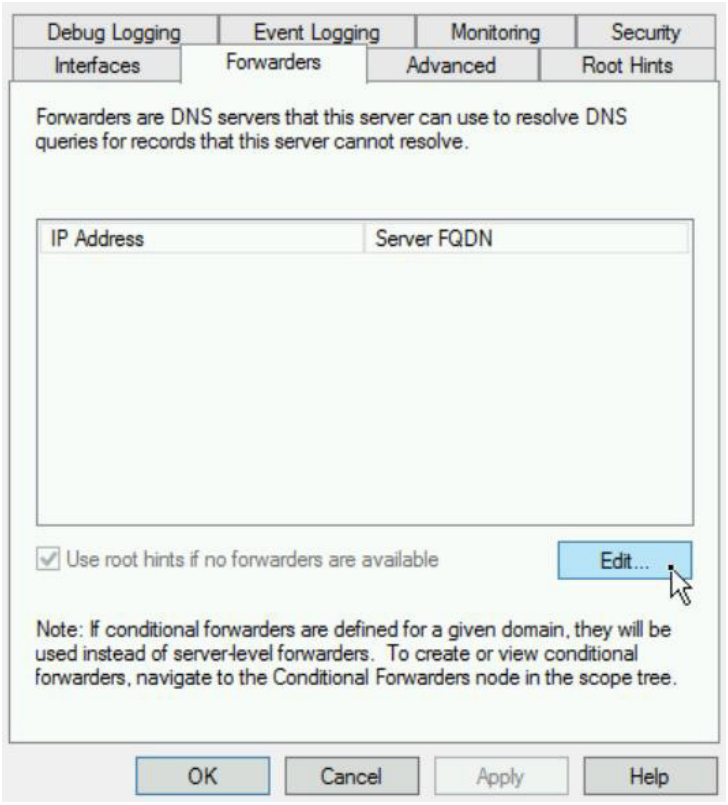
ステップ 2　　編集するサーバを選択し、次に [フォワーダ（Forwarders）] を選択します。

図 28 - Windows DNS Manager—フォワーダ



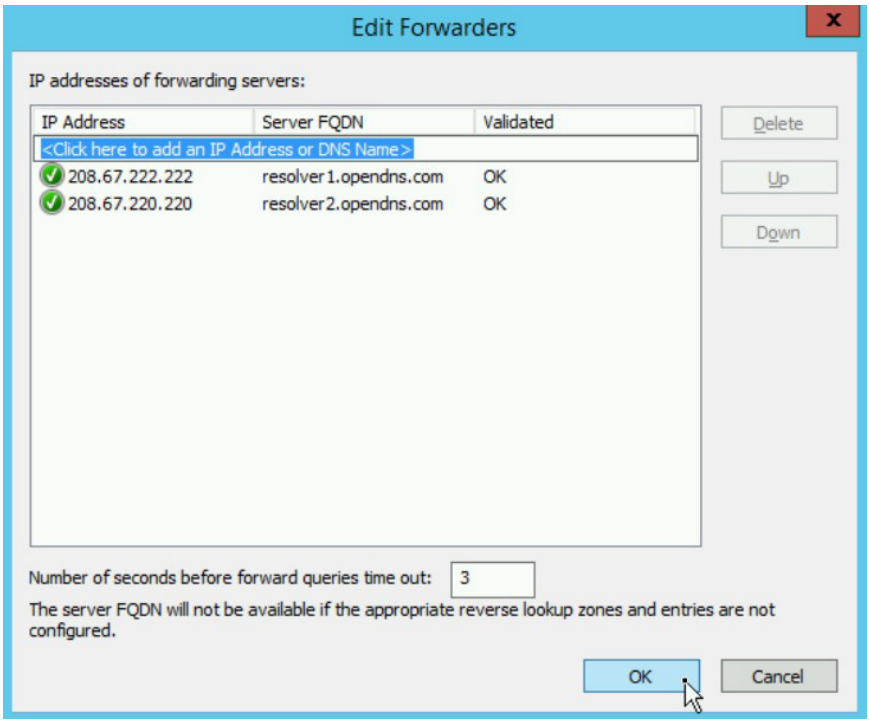
ステップ 3　　[編集(Edit)] をクリックします。

図 29 - Windows DNS—フォワーダの編集



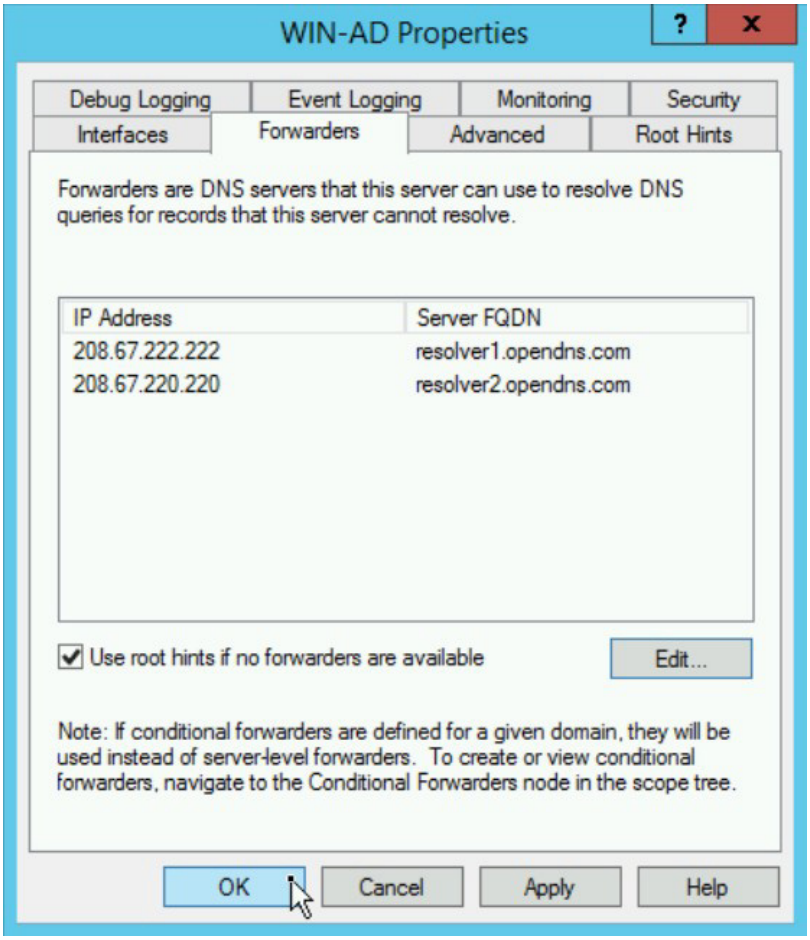
ステップ 4　　Umbrella DNS サーバのアドレス「208.67.220.220, 208.67.222.222」を入力し、[OK] をクリックします。

図 30 - Windows DNS フォワーダの追加



ステップ 5　　[OK] をクリックして変更を確定し、設定ウィンドウを閉じます。

図 31 - Windows DNS Manager への変更の完了



次に、DNS サーバが使用するパブリック IP アドレスを Umbrella のネットワーク ID に追加します。

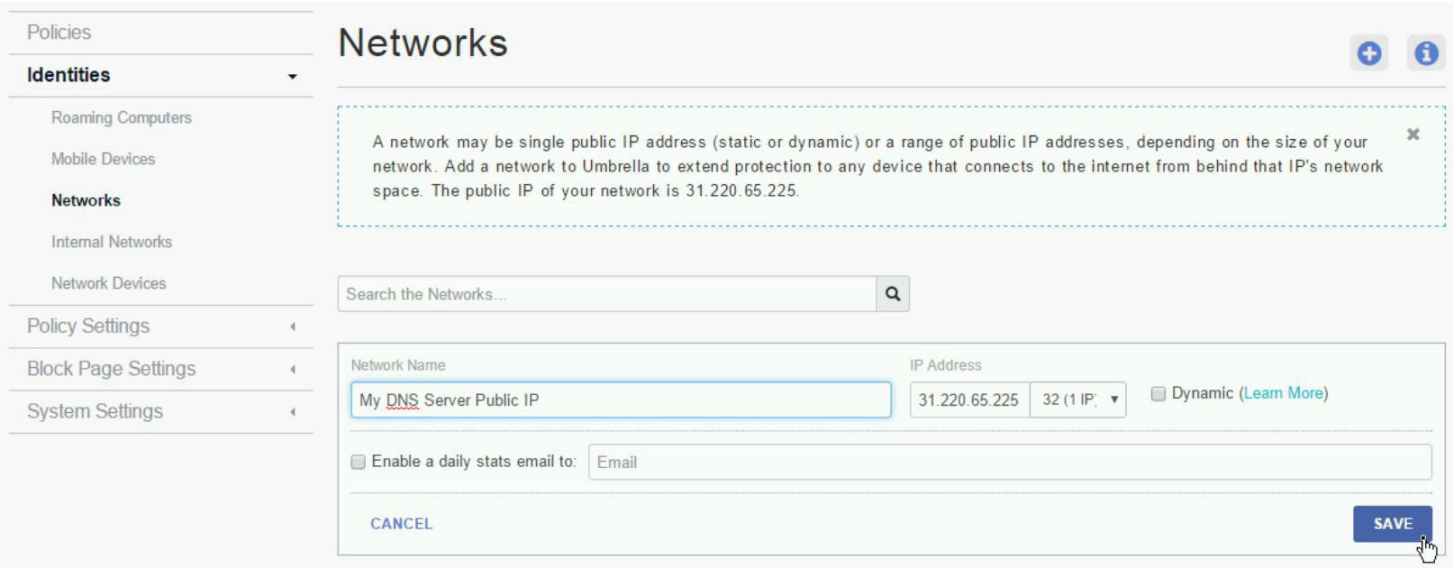
ステップ 6　　[設定（Configuration）] > [ID（Identities）] > [ネットワーク（Networks）] を選択します。

ステップ 7　　「+」アイコンをクリックし、新しいネットワークを追加します。

図 32 - Umbrella DNS ネットワークの追加

ステップ 8　　サブネット マスクとともにネットワークのパブリック IP アドレスを入力し（通常は /32 のサブネット）、記述名を選択します。次に [保存（Save）] をクリックします。

図 33 - 新しいネットワークの設定

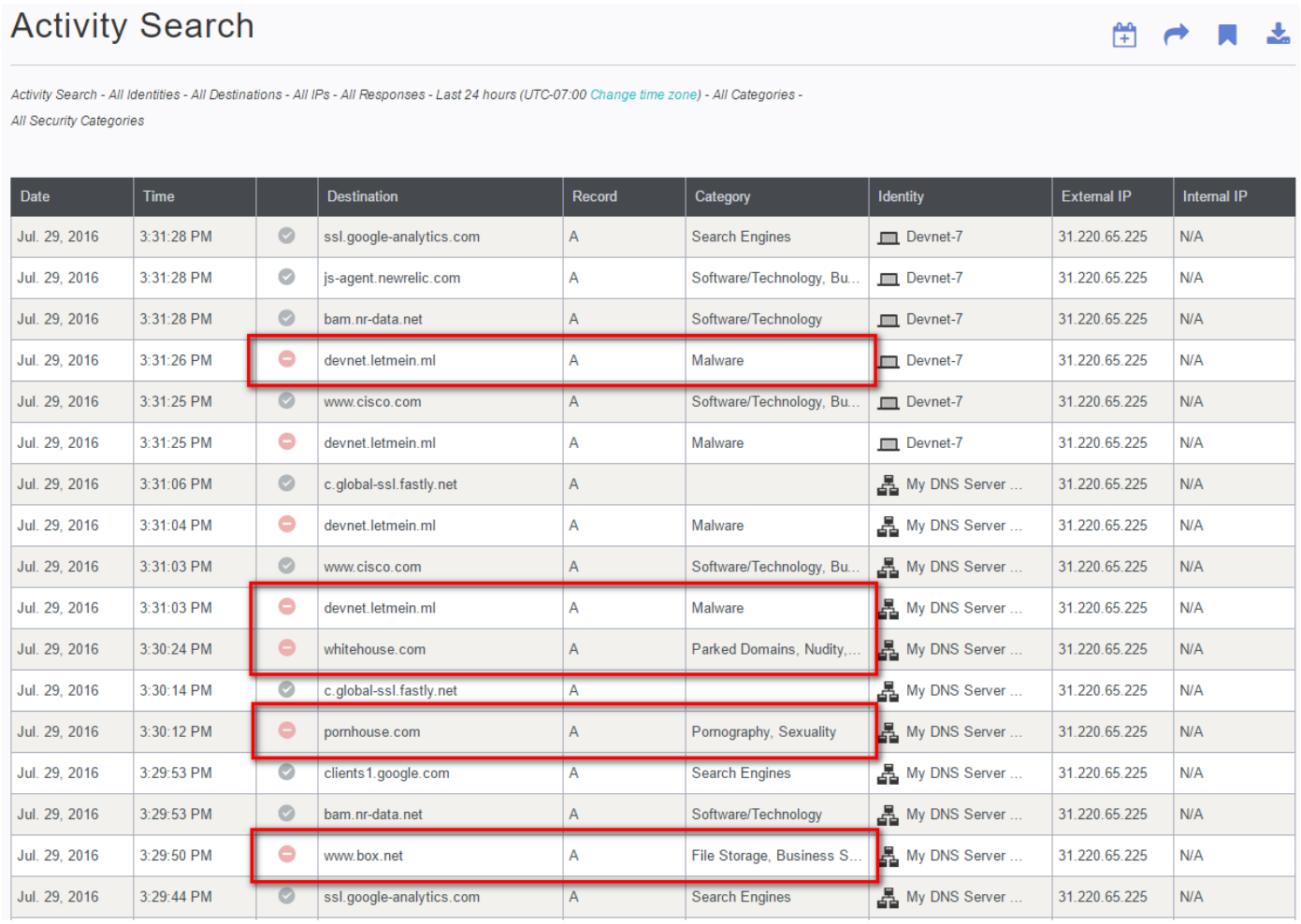


これで、内部ネットワークの DNS サーバを使用するすべてのシステムが保護され、すべてのアクティビティ レポートが内部 DNS サーバからの要求に関連するものと考えることができます。

このアクティビティ レポートには、すべての DNS 検索アクションが表示され、ブロックされた宛先ドメインと、その宛先が属するカテゴリが明示されます。

図 34 は、ランサムウェアのダウンロード、または他のブロック対象カテゴリのサイトへのアクセスを試みたときにブロックされたドメインの結果を示しています。ID 情報には、Umbrella ローミング クライアント システムと、内部 DNS サーバからの検索が含まれています。

図 34 - Umbrella にブロックされたドメイン検索



Date	Time		Destination	Record	Category	Identity	External IP	Internal IP
Jul. 29, 2016	3:31:28 PM		ssl.google-analytics.com	A	Search Engines	Devnet-7	31.220.65.225	N/A
Jul. 29, 2016	3:31:28 PM		js-agent.newrelic.com	A	Software/Technology, Bu...	Devnet-7	31.220.65.225	N/A
Jul. 29, 2016	3:31:28 PM		bam.nr-data.net	A	Software/Technology	Devnet-7	31.220.65.225	N/A
Jul. 29, 2016	3:31:26 PM		devnet.letmein.ml	A	Malware	Devnet-7	31.220.65.225	N/A
Jul. 29, 2016	3:31:25 PM		www.cisco.com	A	Software/Technology, Bu...	Devnet-7	31.220.65.225	N/A
Jul. 29, 2016	3:31:25 PM		devnet.letmein.ml	A	Malware	Devnet-7	31.220.65.225	N/A
Jul. 29, 2016	3:31:06 PM		c.global-ssl.fastly.net	A		My DNS Server ...	31.220.65.225	N/A
Jul. 29, 2016	3:31:04 PM		devnet.letmein.ml	A	Malware	My DNS Server ...	31.220.65.225	N/A
Jul. 29, 2016	3:31:03 PM		www.cisco.com	A	Software/Technology, Bu...	My DNS Server ...	31.220.65.225	N/A
Jul. 29, 2016	3:31:03 PM		devnet.letmein.ml	A	Malware	My DNS Server ...	31.220.65.225	N/A
Jul. 29, 2016	3:30:24 PM		whitehouse.com	A	Parked Domains, Nudity,...	My DNS Server ...	31.220.65.225	N/A
Jul. 29, 2016	3:30:14 PM		c.global-ssl.fastly.net	A		My DNS Server ...	31.220.65.225	N/A
Jul. 29, 2016	3:30:12 PM		pornhouse.com	A	Pornography, Sexuality	My DNS Server ...	31.220.65.225	N/A
Jul. 29, 2016	3:29:53 PM		clients1.google.com	A	Search Engines	My DNS Server ...	31.220.65.225	N/A
Jul. 29, 2016	3:29:53 PM		bam.nr-data.net	A	Software/Technology	My DNS Server ...	31.220.65.225	N/A
Jul. 29, 2016	3:29:50 PM		www.box.net	A	File Storage, Business S...	My DNS Server ...	31.220.65.225	N/A
Jul. 29, 2016	3:29:44 PM		ssl.google-analytics.com	A	Search Engines	My DNS Server ...	31.220.65.225	N/A

Cisco Umbrella ローミング クライアント

Umbrella ローミング クライアントは、所在場所やインターネットへの接続方法を問わずにラップトップを保護します。このクライアントは、インターネット向けの DNS クエリを、世界中に分散されている OpenDNS Global Network データセンターの 1 つを介して Umbrella Secure Cloud Gateway に安全にリダイレクトします。したがって、組織で選択したポリシーが施行されて保護が適用されるため、コンピュータへの侵害を防止することができます。

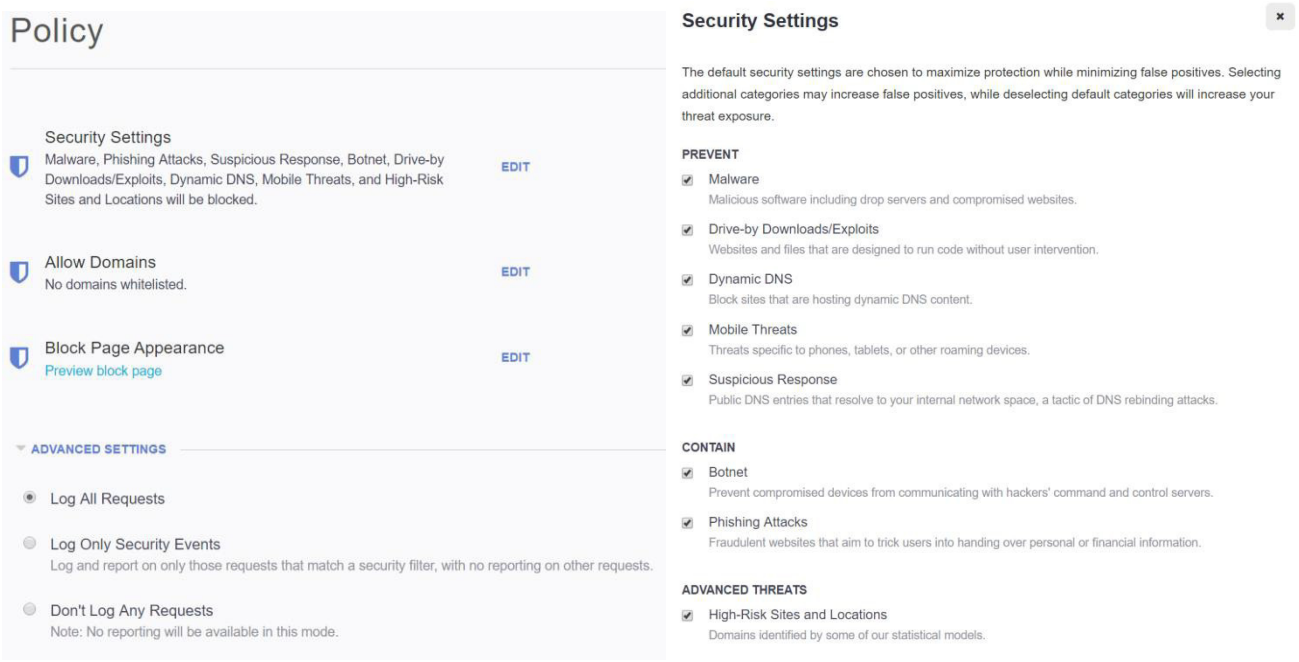
3G/4G ワイヤレス キャリア ネットワークや、Wi-Fi ホットスポット（空港、カフェ、ホテル、自宅など）を介した信頼性の低いネットワークから、または信頼性の高いネットワーク ゲートウェイや Umbrella で保護されたネットワーク背後のオフィス環境内からインターネットにアクセスするコンピュータなどのシナリオが対象になります。

ランサムウェアに対する防御のために必要な追加の設定手順はありません。ローミング クライアントのダウンロードおよびインストール手順については、
http://info.umbrella.com/rs/opendns/images/TD-Umbrella-Mobility-Roaming-Client-Guide.pdf を参照してください。

Cisco Umbrella Roaming

Cisco Umbrella Roaming のみのサービスは、図 35 に示すように重大なセキュリティの脅威をブロックするシンプルなポリシーを使用します。

図 35 - Cisco Umbrella Roaming のコンピュータ ポリシー



エンドポイント向け Cisco Advanced Malware Protection（AMP）

AMP はクラウドベースの「Software as a Service」ソリューションです。アカウントをセットアップしたら、ポリシーを設定し、次にエンドポイントに AMP の軽量コネクタを導入します。サポート対象のエンドポイントには、Windows、Mac、Linux、Android システム向けコネクタが含まれます。組織のプライバシー制限が厳しい場合の代替導入オプションには、オンプレミスのエアギャップ AMP プライベート クラウド仮想アプライアンスがありますが、この製品はこのソリューション検証の範囲外です。

最初に FireAMP コンソールにログインすると、「初めての使用」ウィザードが表示されます。このウィザードは、ウイルス対策製品の除外の作成、プロキシのセットアップ、ポリシーの設定、グループの作成など、FireAMP 環境をすばやく設定するための手順を説明します。これらの手順については『QuickStart Guide』[3]に記載されているので、ここでは説明を省略します。

以下に説明する追加の設定は、ランサムウェアに対する防御を最大限に高めるために必要です。一部の設定は、システム グループによって使用されるポリシー内で行い、それ以外の設定は AMP アカウント設定で行います。まず、ポリシー設定を編集します。Execute モードを有効にして、スキャンが完了するまでファイルの実行をブロックします。また、スキャンとアーカイブを行うファイル サイズの上限を組織の環境に合わせて増やします。このソリューション検証で収集した 1600 以上のランサムウェア サンプルのうち、保護ポリシーのデフォルトの最大スキャン ファイル サイズである 5MB より大きかったサンプルは 103 個でした（最大は 51MB）。

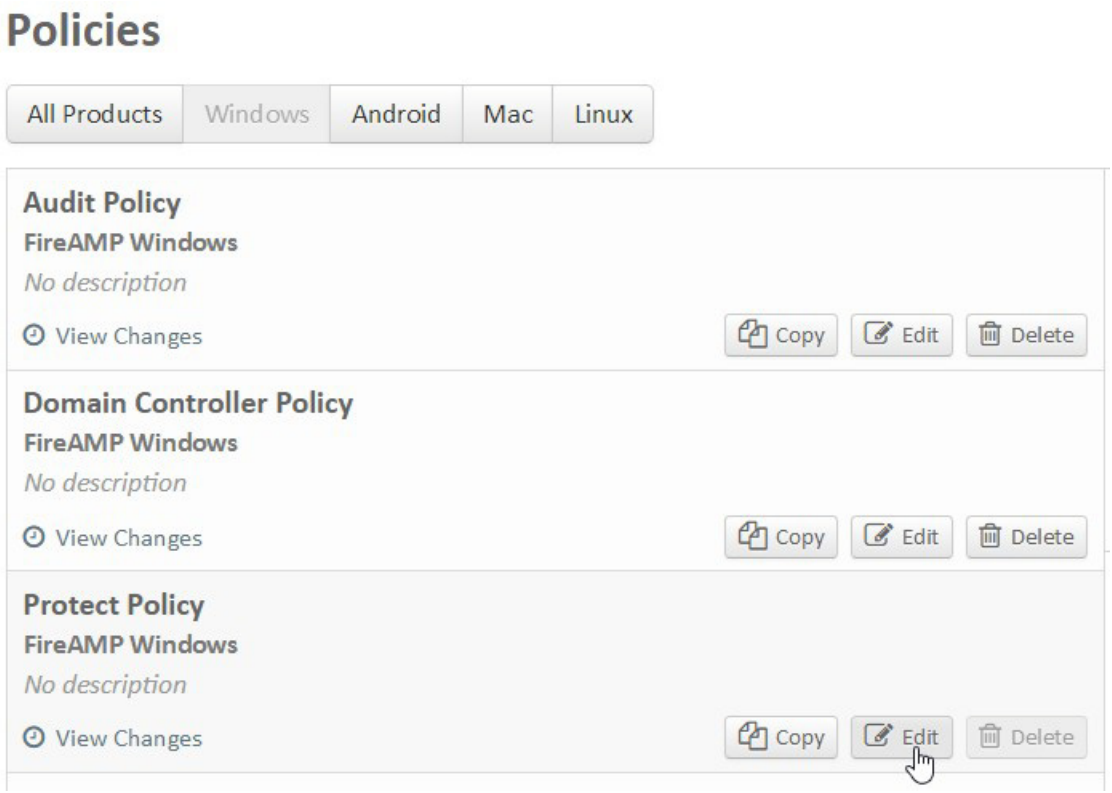
[3] https://docs.amp.cisco.com/FireAMPQuickStartGuide.pdf

注：スキャンするファイルのサイズが大きくなると、インターネットへの WAN 使用率が高まり、その他の通信に影響が及ぶ可能性があります。大規模な組織の場合は、オンサイトにスキャニング アプライアンスを導入するのが望ましいオプションです。

ステップ 1　　AMP コンソールにログイン後、[管理（Management）] > [ポリシー（Policies）] を選択します。

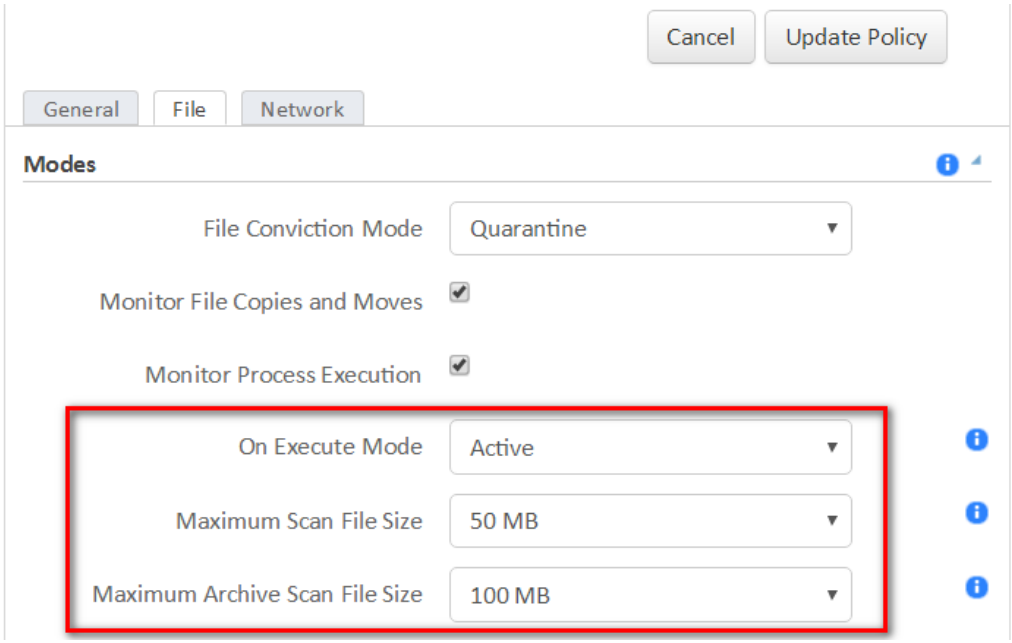
ステップ 2　　エンドポイントに導入する適切な保護ポリシーを選択し、[編集（Edit）] をクリックします。

図 36 - AMP 保護ポリシー



ステップ 3　　ポリシーの [ファイル（File）] タブに移動し、[On Executeモード（On Execute Mode）] を [アクティブ（Active）] に設定してから、最大ファイル サイズを設定します。

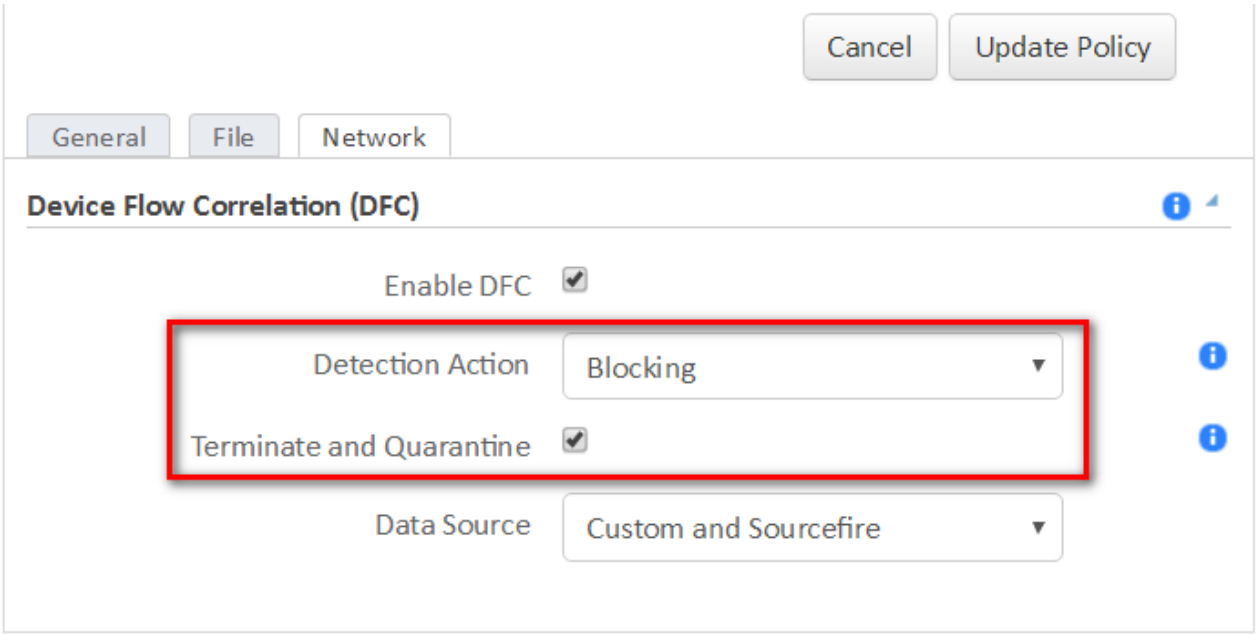
図 37 - ポリシーのファイル属性の編集



デバイス フロー コリレーション（DFC）によって、ランサムウェアによるコールバック通信を発信元で阻止します。特に、企業ネットワークの外部にあるリモート エンドポイントへのコールバック対策に有効です。

ステップ 4　　[ネットワーク（Network）] タブを選択し、DFC アクションを [ブロッキング（Blocking）] に設定し、[終了して隔離（Terminate and Quarantine）] をチェックします。

図 38 - ポリシーのネットワーク属性の編集



警告 この機能を有効にする前に、環境内で許可するアプリケーション、特に自前のソフトウェアやカスタム ソフトウェアがホワイトリストに登録されていることを確認します。

ステップ 5　　終了したら、[ポリシーの更新（Update Policy）] をクリックします。

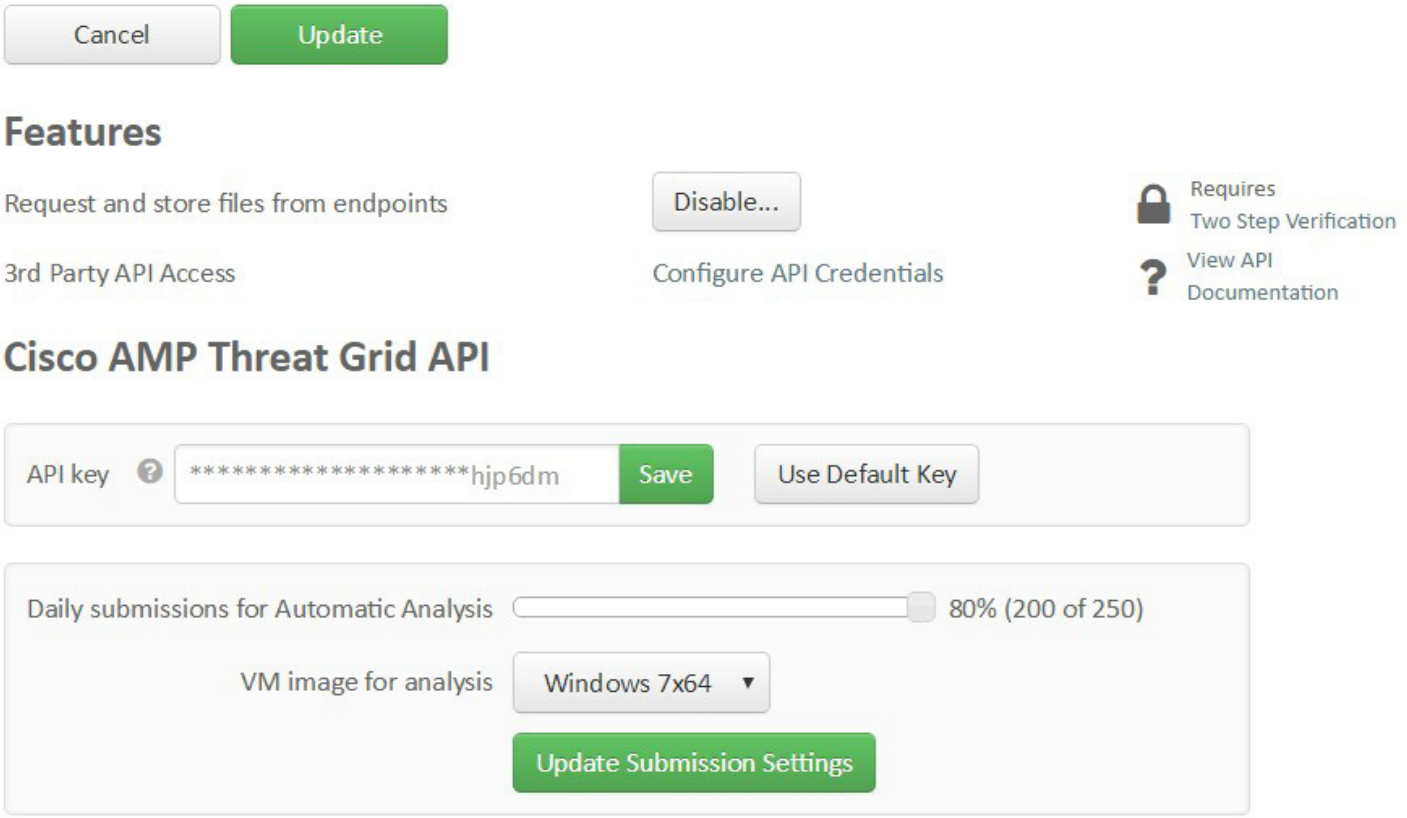
Cisco AMP Threat Grid API を使用すると、分析のために自動的にファイルを送信できます。自動分析を設定する前に、すべてのユーザのアカウントの二要素認証を有効にする必要があります。分析されるすべてのファイルは、コンソールで設定された管理ユーザによるアクセスが可能であるため、これによって最高レベルのプライバシーを維持します。

アカウントで二要素認証を有効にしたら、アカウントのビジネス設定を編集し、ファイル リポジトリ、API キー、送信設定を有効にします。

ステップ 6　　[アカウント（Accounts）] > [ビジネス（Business）] > [編集（Edit）] を選択します。

ステップ 7　　[機能（Features）] の下で、[エンドポイントからのファイルのリクエストと保管（Request and store files from endpoints）] を有効にし、別のアカウントがある場合は Threat Grid API キーを設定します。[自動分析に毎日送信（Daily submissions for Automatic Analysis）] を適切なレベルにスライドさせ、エンドポイントの多くに最も合致する VM イメージを選択します。[送信設定の更新（Update Submission Settings）] をクリックします。

図 39 - AMP アカウントのビジネス設定



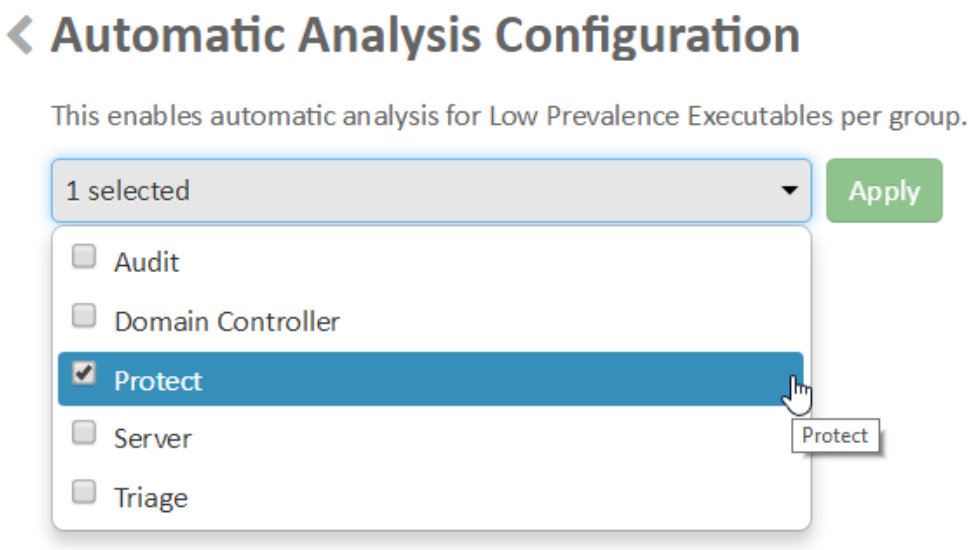
ステップ 8　　終了したら、上部の [更新（Update）] をクリックし、アカウント設定を更新します。

次に、自動分析機能が、特定のグループからファイル分析に拡散度の低い実行可能ファイルを送信できるように設定します。

ステップ 9　　[分析（Analysis）] > [拡散度（Prevalence）] > [自動分析の設定（Configure Automatic Analysis）] を選択します。

ステップ 10　　自動分析を有効にするシステム グループを選択し、[適用（Apply）] をクリックします。

図 40 - AMP 自動分析の有効化



自動分析を設定すると、低拡散度の実行可能ファイルが 4 時間ごとに送信されます。FireAMP は、FireAMP コネクタが確認したファイルが利用可能な場合、送信するよう要求します。ファイルが取得されたらファイル分析に送信されます。その後、[ファイル分析（File Analysis）] ページで分析結果を確認できます。ファイルが一定期間取得されなかった場合は、ファイル リポジトリでファイル取得ステータスを確認できます。

フェーズ 2 の高度なソリューションの実装

表 4 は、高度なランサムウェア防御ソリューションに実装され、検証テストが行われた製品を示しています。以下の各製品のセクションでは、ランサムウェアに対する防御を最大限に高めるために、通常のインストール後にどのようにカスタマイズしたかを説明します。

表 4 - 検証されたソリューションに含まれる製品

製品	説明	プラットフォーム	バージョン
Stealthwatch	NetFlow の収集と分析	仮想またはアプライアンス	6.9.0
ISE	ネットワークに接続するデバイスの認証とプロファイル作成	仮想またはアプライアンス	2.2.0.470
Cognitive Threat Analytics	SW からのフローの分析	クラウド	バージョンなし
Firepower Management Center	Firepower Threat Defense システムの管理	仮想またはアプライアンス	6.2.0
Firepower Threat Defense	Firepower Threat Defense ソフトウェア イメージを実行するセキュリティ プラットフォーム	仮想および 2100、4100、9300	6.2.0
ASA	ファイアウォール	ASA5500-X	9.7(1)4

ASA-ASDM	ローカル FW 管理	ASA5500-X	7.7(1)
ASA 上の NGIPS	保護と制御	ASA5500-X	5.4.1.8+
AnyConnect	セキュア モビリティ クライアント	すべて	4.4.02039
Catalyst スイッチ	アグリゲーション	6880 6807-XL	15.2(1)S 15.4(1)SY
	アクセス	3650、3850	16.3.3

Cisco Identity Services Engine（ISE）

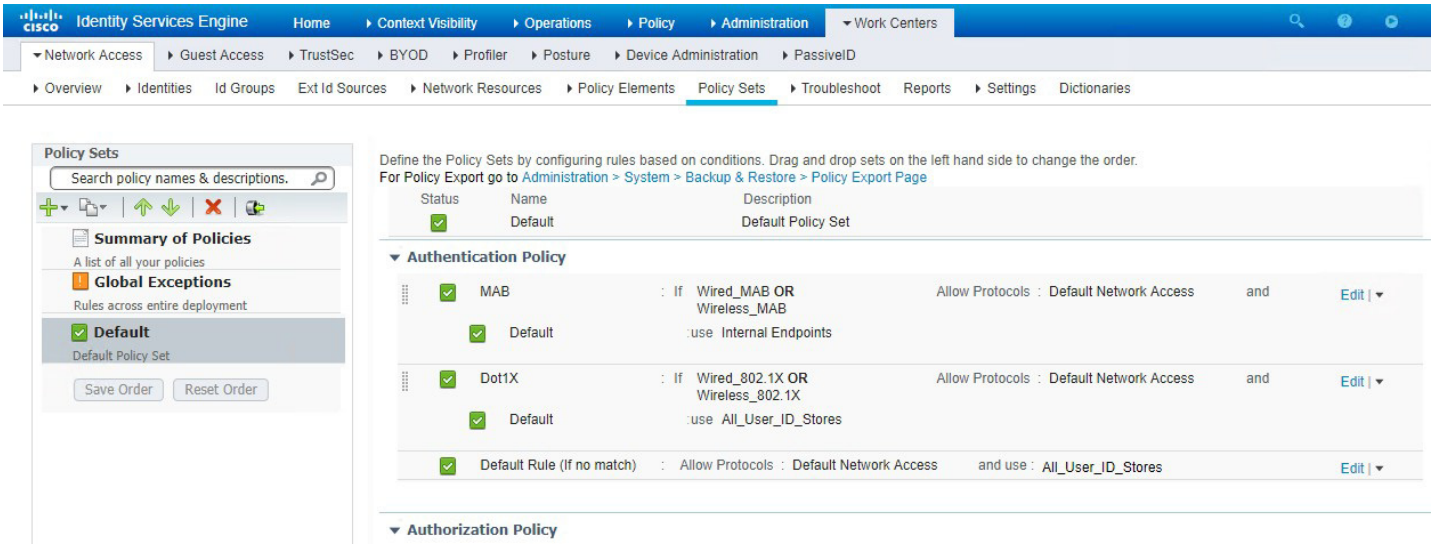
ネットワーク インフラストラクチャへの接続時のユーザとデバイスの認証は、企業の防御の第一線です。ネットワークへの接続時は、未知の要素から既知の要素を、信頼できない要素から信頼できる要素をセグメント化するチャンスです。このコンテキスト情報は、企業全体の他の多くのポリシー適用領域でも、アイデンティティと可視化された通信フローとの関連付けにも使用できます。

このガイドでは、ランサムウェアからの防御のための ISE の設定とユーザの概要に焦点を当てます。ISE の導入方法に関する情報と、代替の設定方法については、以下のリンクを参照してください：
https://www.cisco.com/c/ja_jp/support/security/identity-services-engine/tsd-products-support-series-home.html

ネットワーク認証の設定

ネットワーク管理者にとって重要なことは、ユーザがアクセスするさまざまなベクトルを問わず、ネットワークにオンボーディングするデバイスを識別することです。ユーザが有線、無線、または VPN 接続を介してアクセスする場合でも、ユーザのセキュリティ ポリシーの有効性を維持する必要があります。この環境では、AAA 認証を通じて、ISE によってセキュリティ タグを設定します。

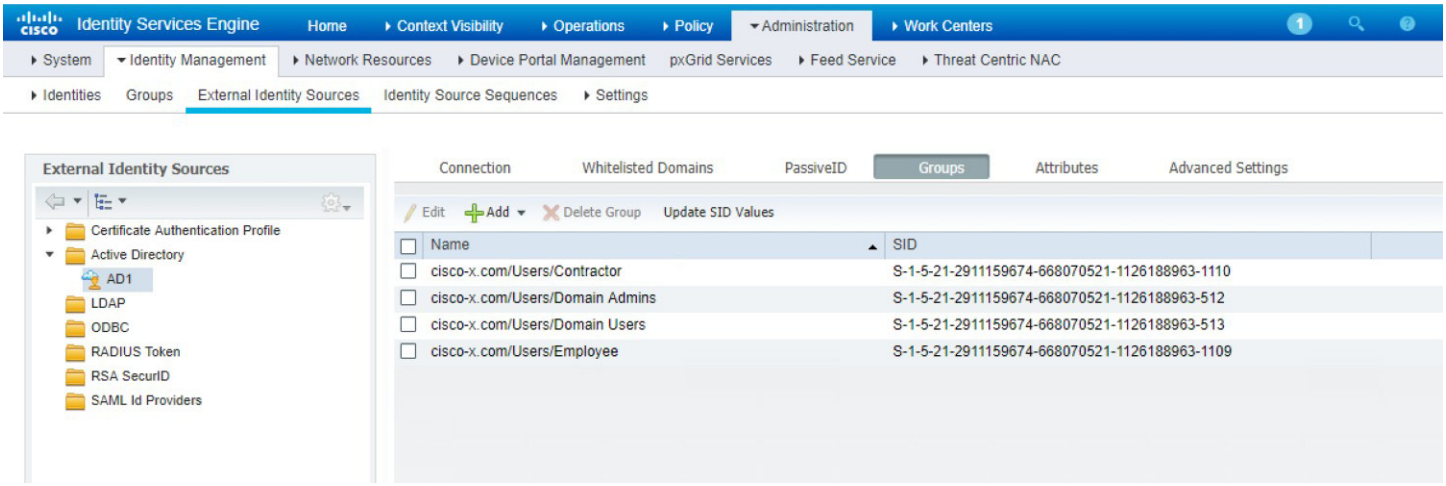
図 41 - デフォルトのポリシー セット



ISE のデフォルトの認証ポリシーでは、まずデバイスの MAC アドレスに注目し、認証フェーズを通過させるために既知の製造元とアドレスが一致するかを確認します。管理者は、ユーザやデバイスを識別する認証方式として、Dot1X も設定できます。

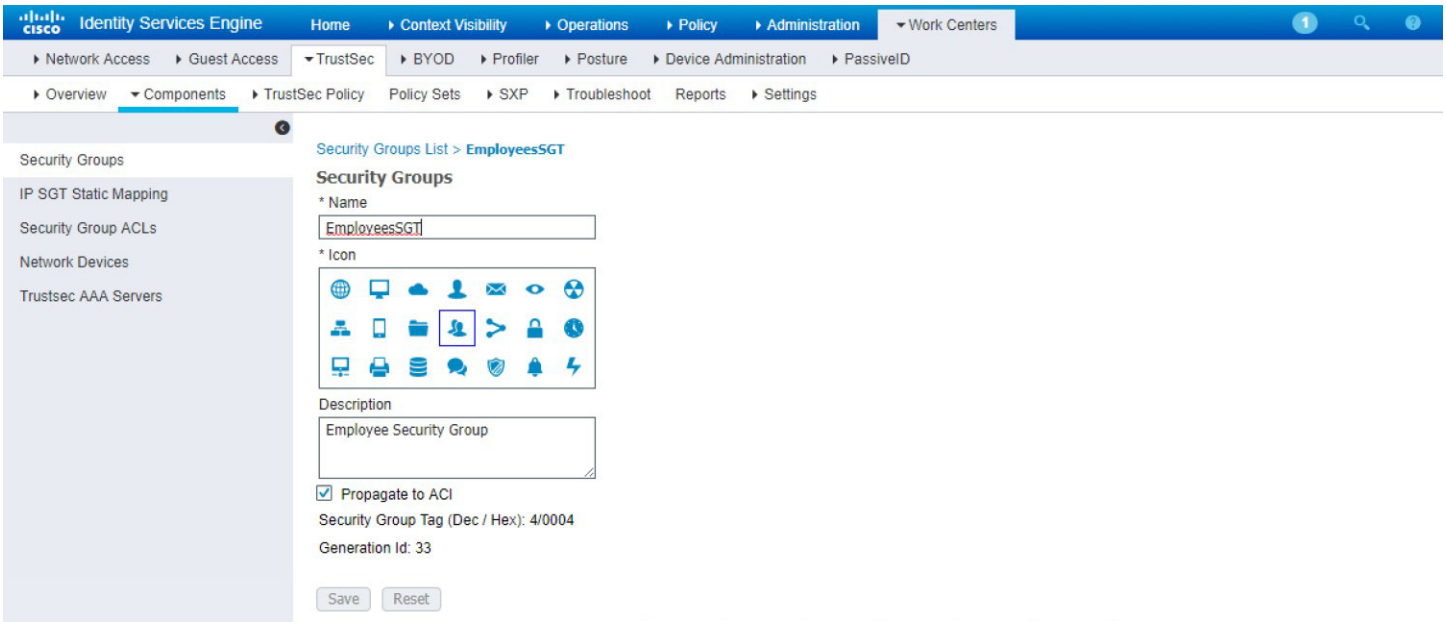
この例では、2 つのグループ、「Employee」と「Contractor」を作成しました。これらの値は、Active Directory のグループ名と関連付けられます。Active Directory を設定すると、これらの値をグループとして ISE にダウンロードできます。これらは、[管理（Administration）] > [アイデンティティの管理（Identity Management）] > [外部アイデンティティソース（External Identity Sources）] > [グループ（Groups）] でも確認できます。

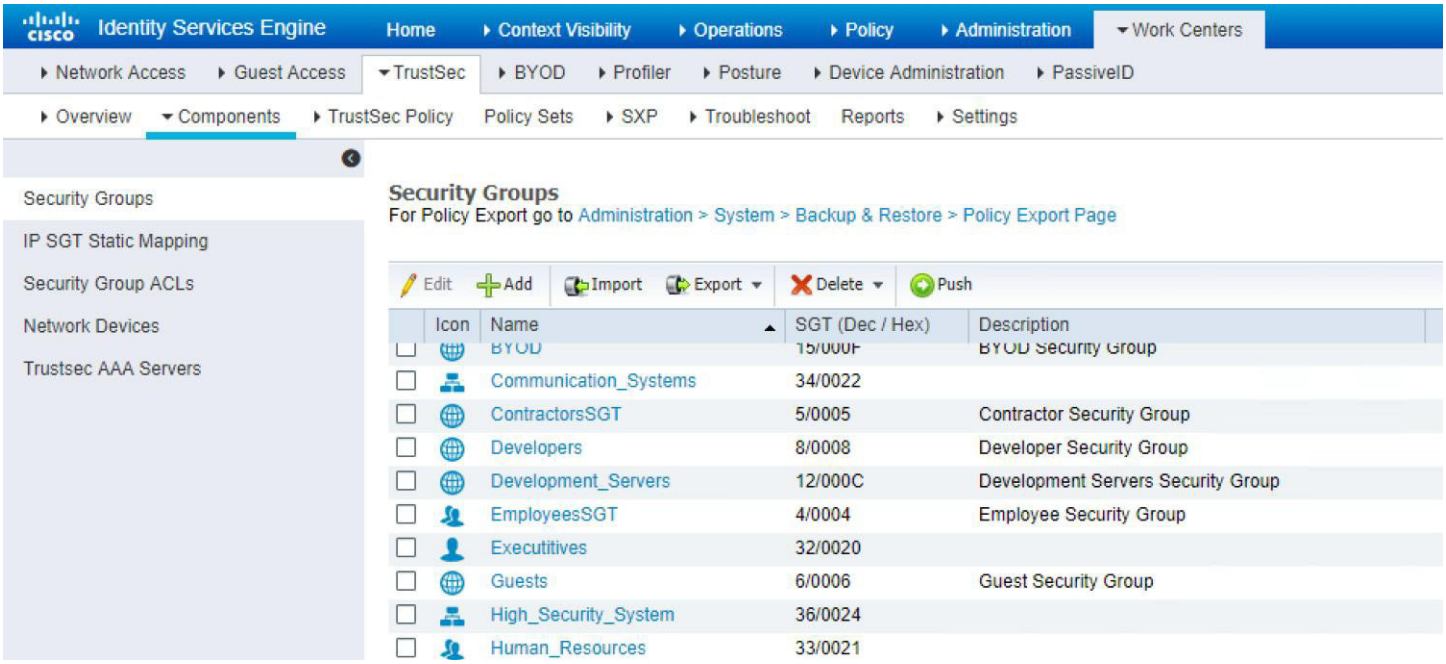
図 42 - 外部アイデンティティ ソース



ステップ 1　　Active Directory グループを認識するように ISE を設定した後、TrustSec セキュリティ グループ タギング（SGT）を作成します。この例では、EmployeeSGT と ContractorSGT を作成しました。注：SGT ID は、Employee：SGTID 4、Contractor：SGTID 5 として自動作成されます。

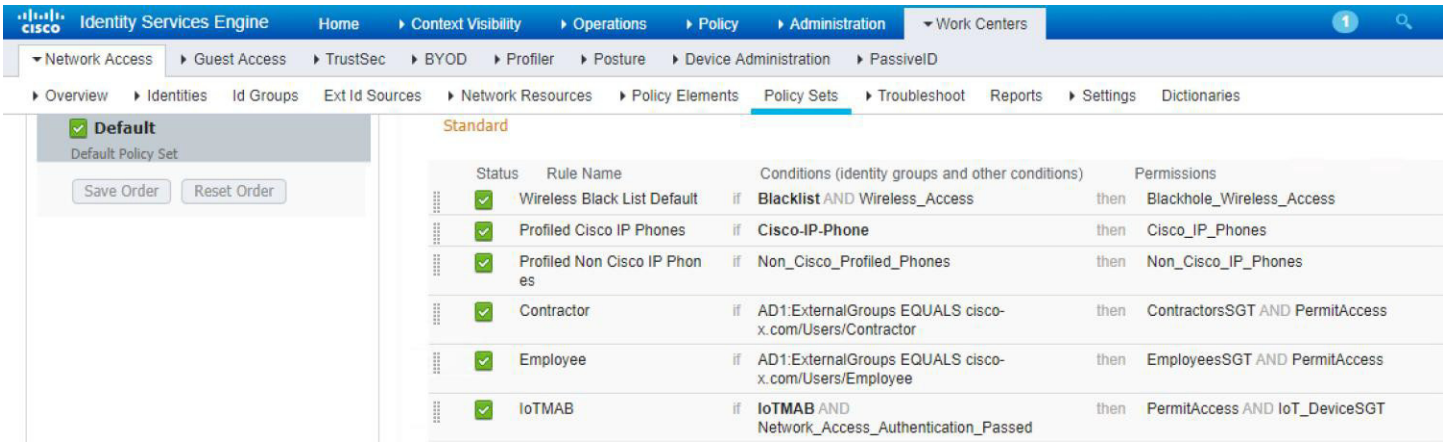
図 43 - TrustSec SGT





ステップ 2　　Employee および Contractor 用の認証ルールを作成し、アクセス許可とセキュリティ グループ タグを割り当てます。

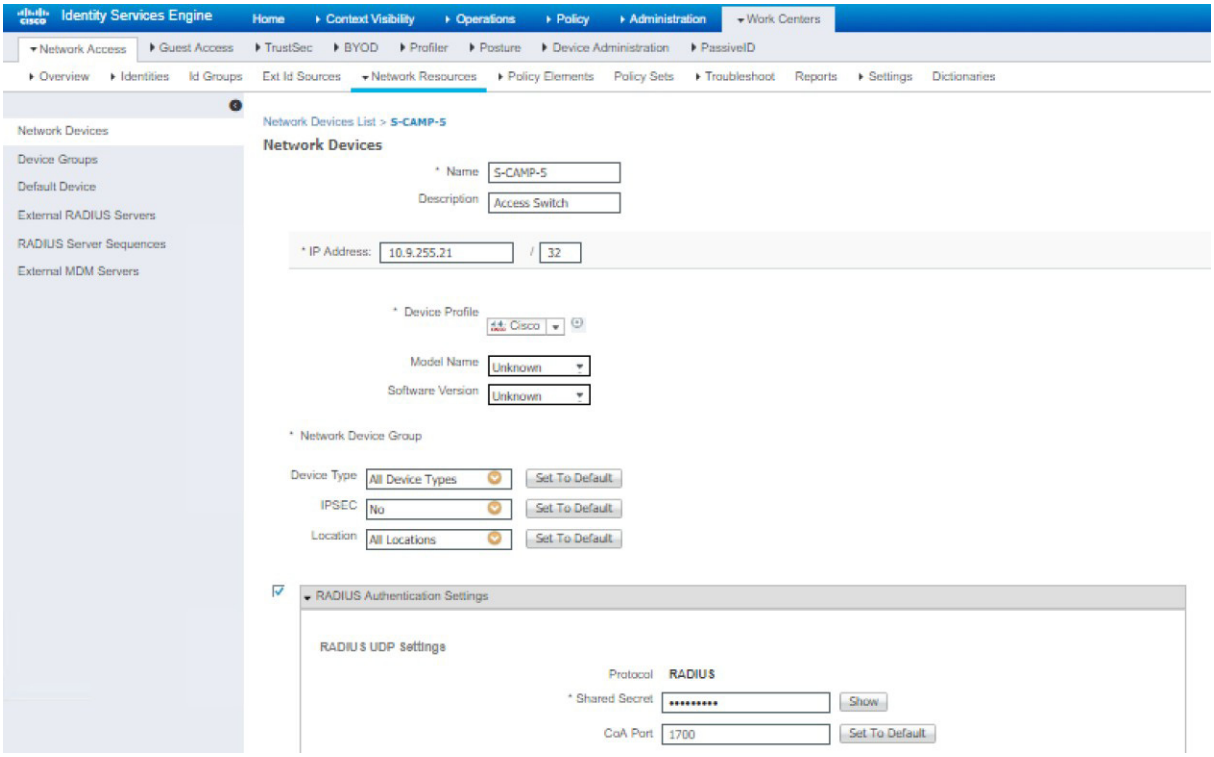
図 44 - 認証ルール



このルールの条件では、認証が Active Directory サーバ（AD1）に一致し、かつ認証されたユーザが Employee または Contractor グループに含まれている場合に、対応する SGT を割り当て、アクセスを許可します。

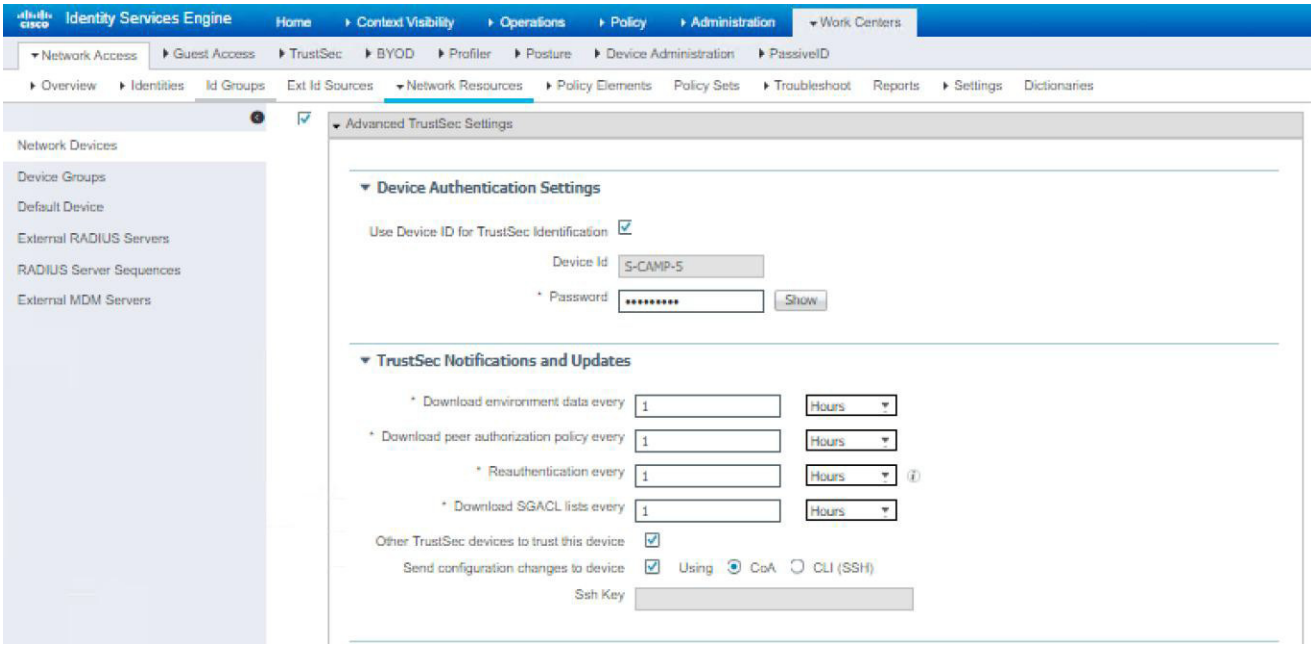
ステップ 3　　デバイスとユーザを認証する ISE に、スイッチ、ファイアウォール、ルータを追加します。[ワークセンター（Work Centers）] > [ネットワークアクセス（Network Access）] > [ネットワークリソース（Network Resources）] > [ネットワークデバイス（Network Devices）] の順に選択します。[追加（Add）] をクリックします。[名前（Name）]、[IPアドレス（IP Address）]、[説明（Description）]（オプション）を入力します。RADIUS 共有秘密鍵を設定します。

図 45 - ネットワーク デバイスの追加



ステップ 4　　デバイス名を使用して、TrustSec デバイス ID を設定します。認証に使用するパスワードを設定します。[保存（Save）] をクリックします。

図 46 - TrustSec デバイス ID の設定



スイッチの設定

各スイッチは、ネットワーク デバイス、ユーザ、その他のシステムを認証する ISE AAA サーバと通信するように設定する必要があります。全社的にエンドツーエンドでこの設定を行い、ネットワークに接続している要素を包括的に把握できるようにするのがベスト プラクティスです。

RADIUS 認証、許可、アカウンティングの設定

ステップ 1　　認証に使用される IP アドレスが ISE に設定されているインターフェイスをグローバルに指定します。dot1x control をイネーブルにします。AAA をイネーブルにします。

```
ip radius source-interface Loopback0
dot1x system-auth-control
aaa new-model
aaa authentication login default local
aaa authorization exec default local
aaa session-id common
```

ステップ 2　　次の RADIUS サーバ属性を設定します。

```
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
radius-server dead-criteria time 5 tries 3
```

ステップ 3　　RADIUS サーバ、IP アドレス、ISE に入力された共有秘密鍵を設定します。

```
radius server ISE01
 address ipv4 10.9.10.51 auth-port 1812 acct-port 1813
 pac key Cisco1234
```

ステップ 4　　RADIUS の AAA グループ名を設定し、ステップ 3 で作成したサーバを指定します。

```
aaa group server radius ISE
 server name ISE01
```

ステップ 5　　ステップ 4 で作成したグループを使用するデフォルトの認証、許可、アカウンティングを設定します。

```
aaa authentication dot1x default group ISE
aaa authorization network default group ISE
aaa accounting update periodic 2880
aaa accounting dot1x default start-stop group ISE
```

ステップ 6　　認可変更（CoA）が発生したときに、ISE がスイッチに自動的にポリシー更新を送信できるように設定します。[高度なTrustSec設定（Advanced TrustSec Settings）] の ISE デバイス設定で指定したパスワードを入力します。これにより、スイッチ ポートのバウンス、再認証、無効化が容易になります。

```
aaa server radius dynamic-author
 client 10.9.10.51 server-key Cisco1234
```

ステップ 7　　スイッチが IP アドレスを ISE に送信できるように、スイッチにデバイス追跡コマンドを設定します。デバイス追跡用コマンドは、スイッチの種類やインストールされている IOS のバージョンによって異なる場合があります。

IOS 16.1.x より前:

```
ip device tracking all
```

をグローバル コンフィギュレーション モードで使用します。

IOS 16.1.x 以降

グローバル コマンド:

```
device-tracking tracking
!
device-tracking policy IPDT
 tracking enable
```

dot1x インターフェイスで、以下を入力します。

```
device-tracking attach-policy IPDT
```

詳細については、『IOS 16.1.x コンフィギュレーション ガイド』を参照してください。

注:重要システムで使用されるスイッチの場合、バウンスおよび無効化コマンドは、以下の設定によって上書きおよび無視することができます。

```
authentication command bounce-port ignore
authentication command disable-port ignore ip device tracking
```

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_aaa/configuration/15-sy/sec-usr-aaa-15-sy-book/sec-rad-coa.html [英語]

ポートごとのポート認証の有効化

スイッチでは、以下の設定によってポートベースの認証と IP デバイスの追跡を有効化できます。エンドポイント デバイスが接続される各インターフェイスを設定します。MAB および Dot1x 方式が共存し、想定通りに機能するには、以下のアプリケーション ノートに記載されているように、順序と優先順位を適切に指定する必要があります:「MAB の設定」http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/identity-based-networking-service/application_note_c27-573287.html [英語]

ステップ 7　　各デバイス インターフェイスに次の設定を追加します。

```
interface GigabitEthernet1/1
 device-tracking attach-policy IPDT
 authentication event fail retry 0 action next-method
 authentication host-mode multi-auth
 authentication order mab dot1x
 authentication priority dot1x mab
 authentication port-control auto
 mab
 dot1x pae authenticator
```

port-control auto は適用をアクティブ化するコマンドで、テストでは追加することも削除することもできます。

TrustSec

TrustSec を全社的に設定するには、複数のステップを実行する必要があります。最初のステップは、相互の通信を許可されるグループを指定するポリシーの定義です。これらのセキュリティ グループを使用するポリシーは、ISE およびファイアウォール ポリシー マネージャ（Firepower Management Center、ASDM、CSM）の両方で個別に作成します。適切なポリシーを定義した後、Security Exchange Protocol（SXP）を使用して SGT-to-IP アドレス マッピング情報を共有するように各システムを設定します。一部の環境では、SXP への参加に加えて、パケットのインライン タギングも必要になります。最後に、スイッチおよびファイアウォール インターフェイスで適用を有効にします。

Cisco Platform Exchange Grid（pxGrid）は、異なるテクノロジー間でインテリジェンスを交換するための非常にセキュアなシステムを提供します。ISE、Firepower、および Stealthwatch 間に pxGrid を導入すると、これらのシステムはネットワークに接続しているユーザとデバイスに関する豊富なコンテキスト情報を共有できます。pxGrid をインストールする手順は、『Rapid Threat Containment 設計ガイド』に記載されています。

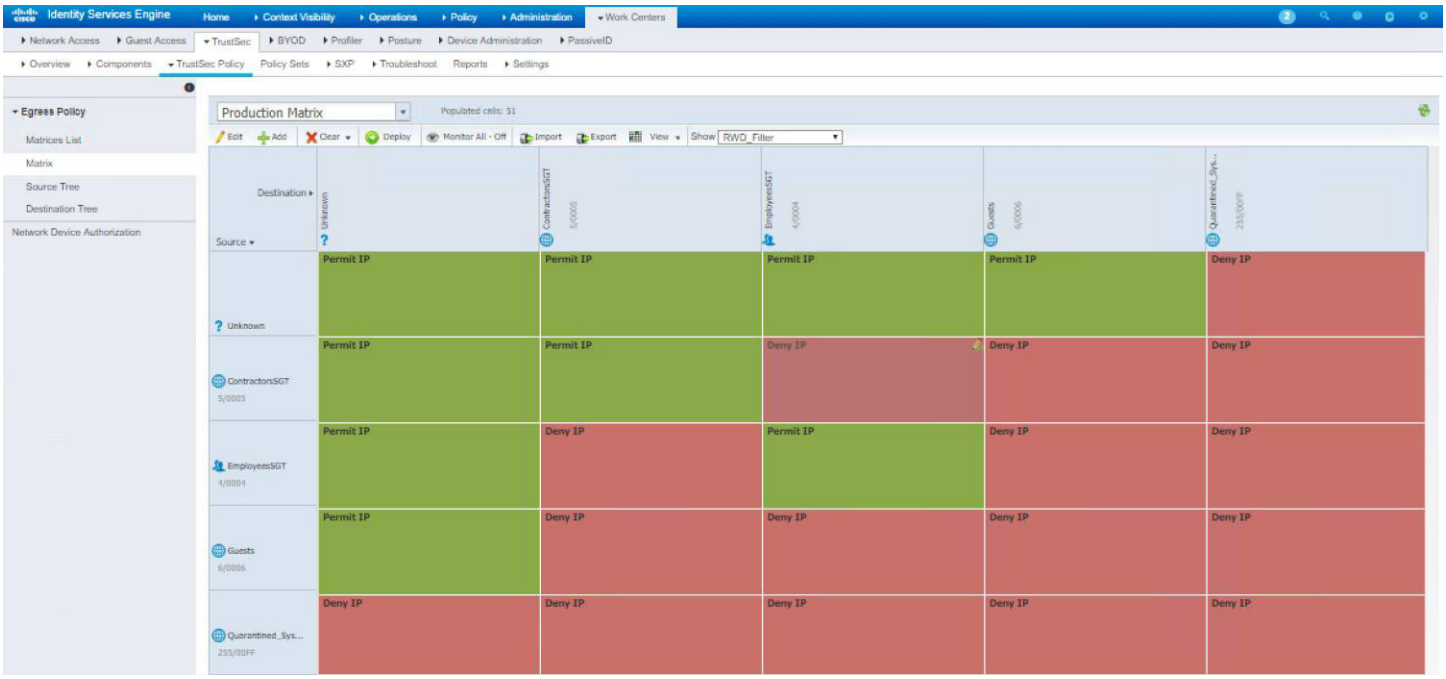
ISE ポリシー マトリックス

ISE ポリシー マトリックスによって制御され、スイッチによって実行される通信は、一方向の、ステートフルではない通信です。したがって、適切な対称性と期待される機能を実現するために、要求と応答両方を考慮する必要があります。適用が発生するのは、アクセス スイッチ ポートから宛先デバイス/セキュリティ グループが付加されたパケットが出るときです。

ISE と TrustSec は、同一スイッチ上、セル内またはセル間のデバイス間でスイッチ レベルのセキュリティを実装するのに理想的で、産業ゾーン全体に適切なセグメンテーションを作成します。

ISE ポリシー マトリックス（[ワークセンター（Work Centers）] > [TrustSec] > [TrustSecポリシー（TrustSec Policy）] > [マトリックス（Matrix）]）は、送信元および宛先セキュリティ グループを行と列で表現する視覚的に理解できるテーブルです。グループ間の通信を拒否または制限するには、ポリシー セルを編集します。デフォルトでは通信は許可されます。

図 47 - ISE ポリシー マトリックス

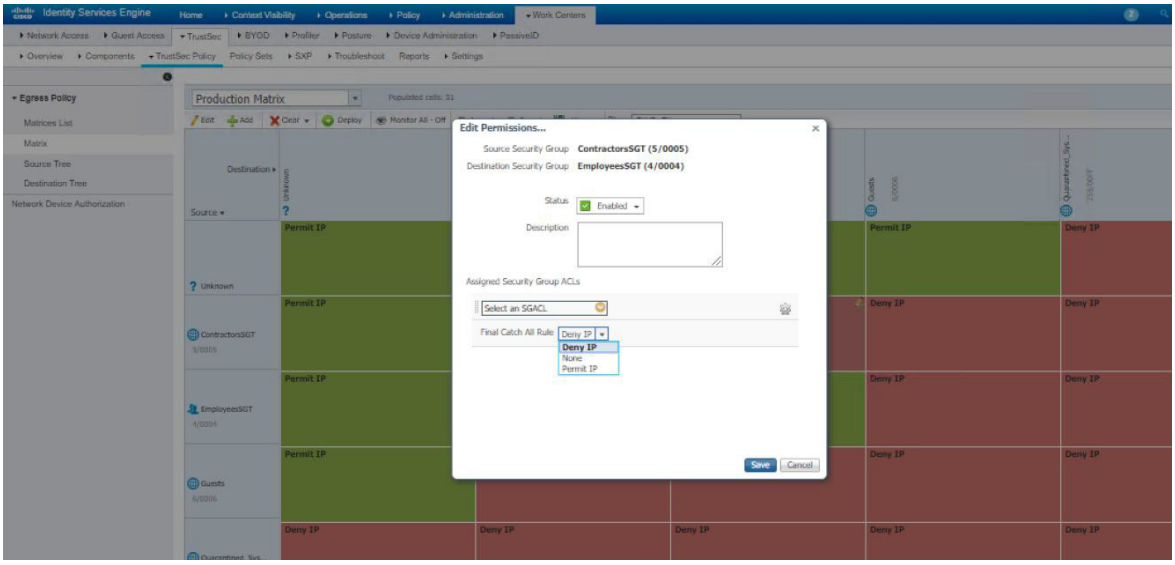


注：SGT Unknown がインターネットと考えられることを示すためのカスタム ビュー フィルタを作成しました。対応する通信フローが同一であることがわかります。TrustSec ポリシーは、ファイアウォールのように双方向ではないため、両方向を許可または拒否する必要があります。

この例では、隔離デバイスを除くすべてのデバイスが Unknown と通信できます。Contractor および Employee は、Unknown および同一の SGT とのみ通信できます。Guest が通信できるのは、Unknown のみです。隔離デバイスは誰とも通信できません（ただし、ステータスを「隔離解除」に修復するポリシーを作成します）。

ステップ 1　　デバイス間の通信を許可するようにポリシーを編集します。セルをクリックし、セルの右上の鉛筆アイコンをクリックして SGACL を選択するか、[すべてのルールを取得（Catch All Rule）] を変更します。[保存（Save）] をクリックします。

図 48 - 許可の編集



ステップ 2　　ポリシーの変更が完了したら、[展開（Deploy）] ボタンをクリックし、次に通知領域の [プッシュ（push）] ボタンをクリックします。[OK] をクリックして、CoA 通知を了承します。

例に関する注意：宛先デバイスが、TrustSec 適用が有効にされていないスイッチに接続されている場合、ポリシーにこの通信をブロックするように設定されていても、パス内の他のすべてのスイッチに TrustSec 適用が設定されていても、この通信はブロックされません。ポリシーに指定されている場合、送信元デバイスに戻されるリプライ トラフィックはブロックできます。

Security Group Tag Exchange Protocol

SXP を使用すると、TrustSec のハードウェア サポートがないネットワーク デバイスに SGT を伝播できます。SXP は、SGT 認識ネットワーク デバイス間でのエンドポイントの SGT と IP アドレスの転送に使用されます。SXP が転送するデータは、IP-SGT マッピングと呼ばれます。エンドポイントが属する SGT は、静的または動的に割り当て可能で、SGT はネットワーク ポリシーで分類子として使用できます。

SXP は、トランスポート プロトコルとして TCP を使用して、2 台の異なるネットワーク デバイス間の SXP 接続を確立します。各 SXP 接続では、一方のピアが SXP スピーカーとして指定され、もう一方のピアは SXP リスナーとして指定されます。これらのピアは、それぞれがスピーカーおよびリスナーの両方として機能する双方向モードに設定できます。

接続はどちらのピアによっても開始できますが、マッピング情報は常にスピーカーからリスナーに伝播されます。

このソリューションでは、SXP はハブ-スポーク形式で設定され、すべてのネットワーク デバイスが SXP 接続のために ISE サーバとピアリングされました。スイッチと ISE サーバ間にファイアウォールがある場合は、FTD および ASA ファイアウォール両方を通じて SXP を許可するために特別な設定を追加する必要があります。

ASA を通じた SXP の有効化

SXP 接続は、次の例に示すように、ASA によって相互接続された 2 つの SXP ピア間で初期化状態のままとなります。

（SXP ピア A）- - - -（ASA）- - -（SXP ピア B）

したがって、Cisco TrustSec と統合するように ASA を設定する場合は、SXP 接続を設定するために、ASA で、no-NAT、no-SEQ-RAND、MD5-AUTHENTICATION TCP オプションをイネーブルにする必要があります。SXP ピア間の SXP ポート TCP 64999 宛てのトラフィックに対して TCP 状態バイパス ポリシーを作成します。そして、適切なインターフェイスにポリシーを適用します。

たとえば、次のコマンド セットは、TCP 状態バイパス ポリシーの ASA の設定方法を示しています。

```
access-list SXP-MD5-ACL extended permit tcp host peerA host peerB eq 64999 access-list
SXP-MD5-ACL extended permit tcp host peerB host peerA eq 64999

tcp-map SXP-MD5-OPTION-ALLOW
 tcp-options md5 allow または tcp-options range 19 19 allow

class-map SXP-MD5-CLASSMAP
 match access-list SXP-MD5-ACL

policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
class SXP-MD5-CLASSMAP
  set connection random-sequence-number disable
  set connection advanced-options SXP-MD5-OPTION-ALLOW
  set connection advanced-options tcp-state-bypass
service-policy global_policy global
```

詳細については、次のサイトを参照してください。
http://www.cisco.com/c/en/us/td/docs/security/asa/asa96/configuration/firewall/asa-96-firewall-config/access-trustsec.html [英語]

FTD を通じた SXP の有効化

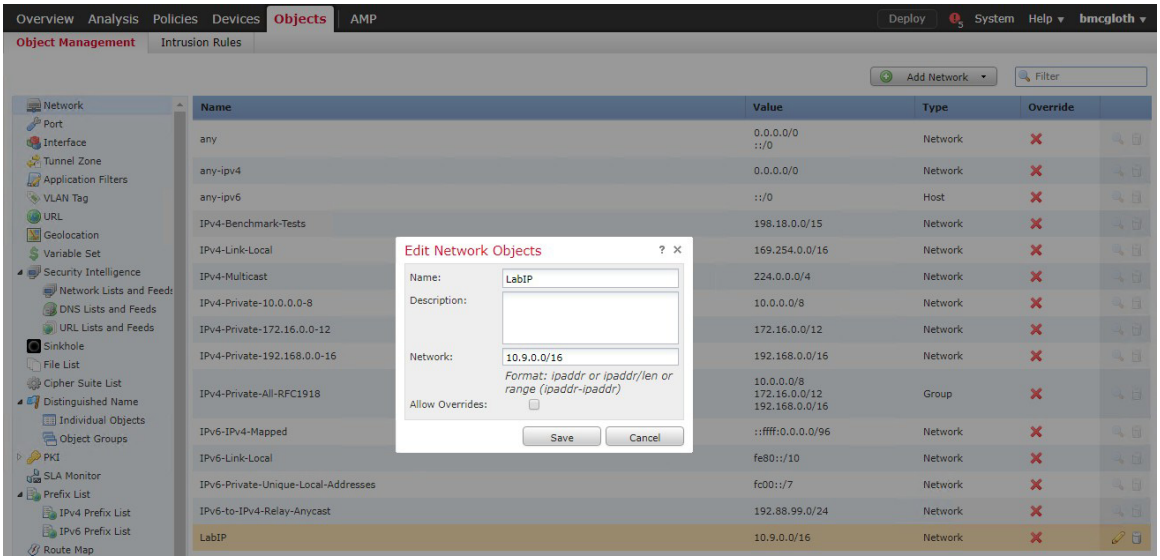
FTD で次の操作を実行します。

1. ネットワーク オブジェクト（ネットワークとプロトコル）の作成
2. 拡張 ACL の作成
3. Flex-config オブジェクトの作成
4. FTD デバイスへの Flex config オブジェクトの追加

拡張アクセス リストに、すべての適切なスイッチの IP および ISE にポート 64999 を許可するオブジェクトを追加します。この例では、ラボ IP ブロック用のネットワーク オブジェクトを作成しました。

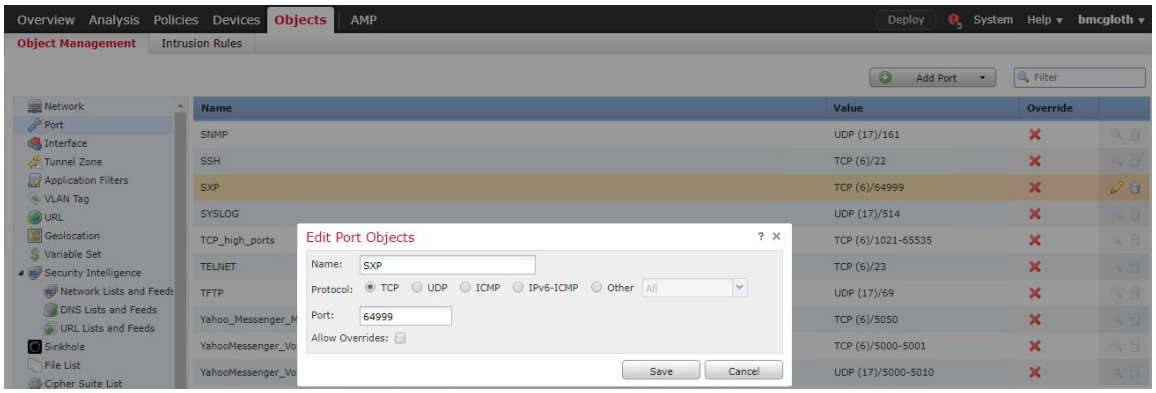
ステップ 1　　FMC で、[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [ネットワーク（Network）] に移動します。右上の [ネットワークを追加（Add Network）] ボタンをクリックします。[名前（Name）]、[説明（Description）]、[ネットワーク（Network）] を入力します。[保存（Save）] をクリックします。

図 49 - ネットワーク オブジェクトの編集



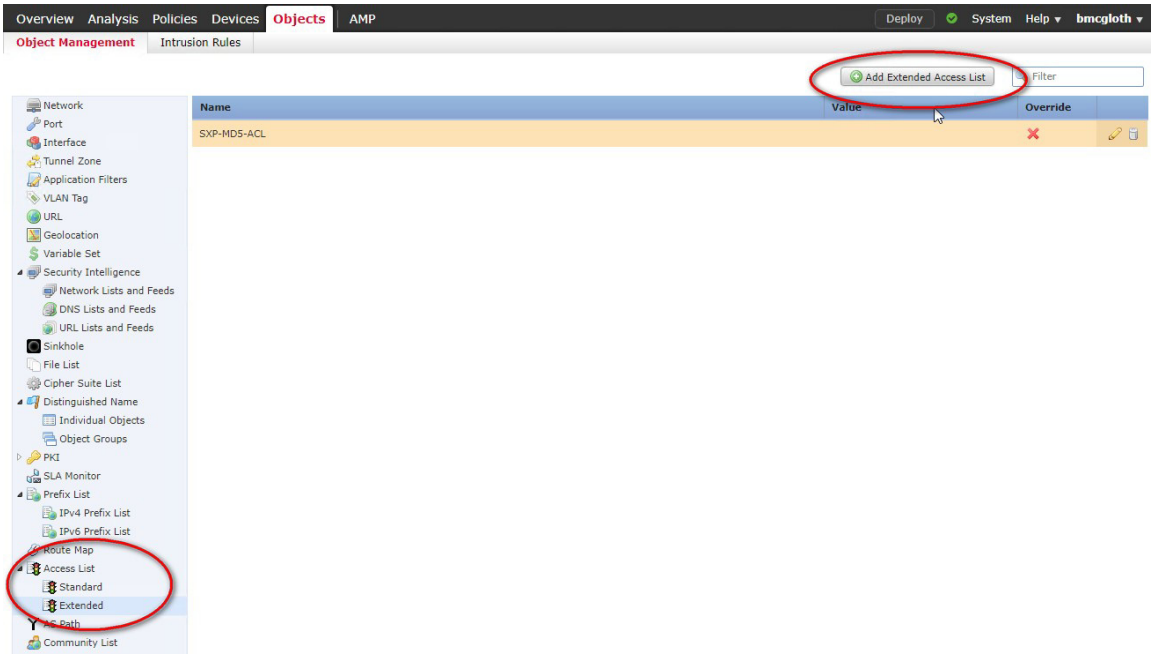
ステップ 2　　[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [ポート（Port）] に移動します。右上の [ポートの追加（Add Port）] ボタンをクリックします。[名前（Name）] に「SXP」を入力し、[TCP] を選択し、[ポート（Port）] に「64999」を入力します。[保存（Save）] をクリックします。

図 50 - ポート オブジェクトの編集



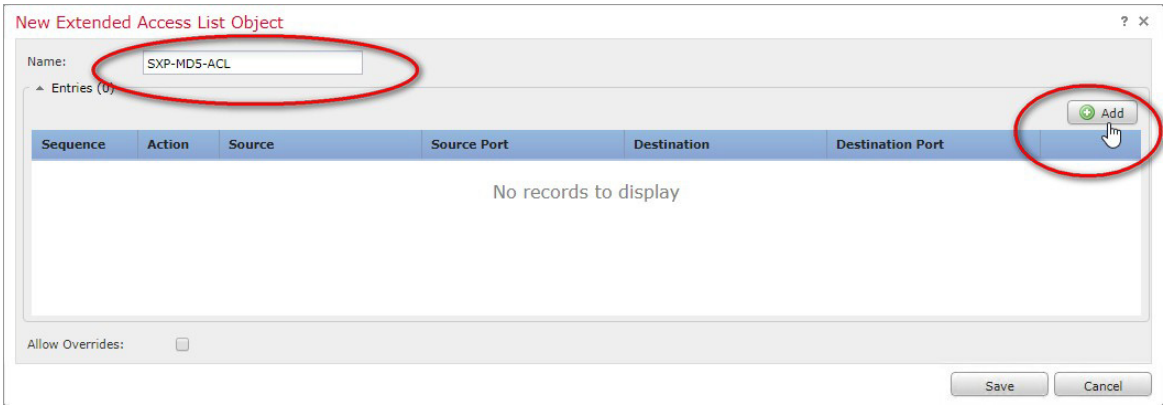
ステップ 3　　[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [アクセスリスト（Access List）] > [拡張（Extended）] に移動します。右上の [拡張アクセスリストの追加（Add Extended Access List）] ボタンをクリックします。

図 51 - 拡張アクセス リストの追加



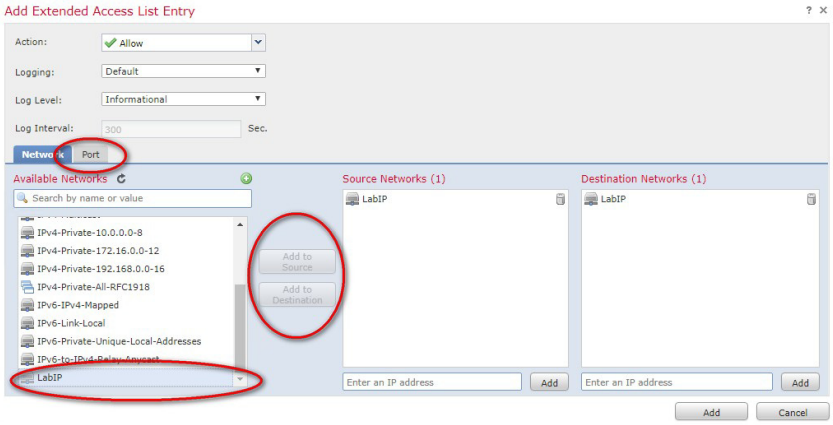
ステップ 4　　[名前（Name）] を入力します。[追加（Add）] をクリックし、アクセス リスト エントリの作成を開始します。

図 52 - 新しい拡張アクセス リスト オブジェクト



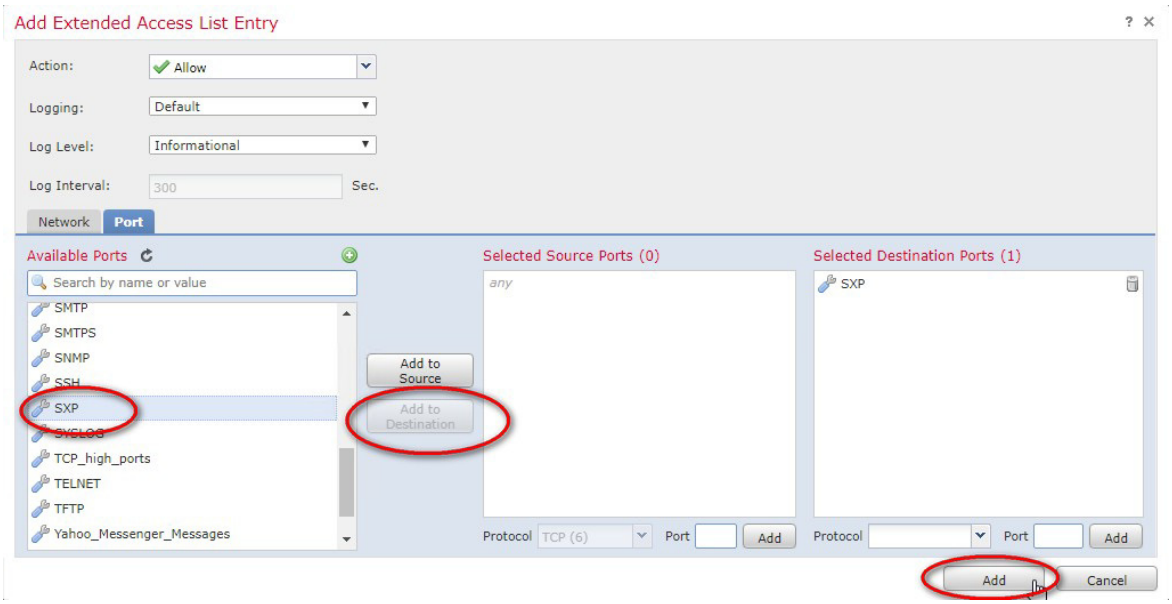
ステップ 5　　前のステップで作成した適切なネットワーク オブジェクトを選択し、お使いの環境に適切な送信元および宛先ネットワークにこのオブジェクトを追加します。[ポート（Port）] タブをクリックします。

図 53 - 拡張アクセス リスト エントリの追加 - ポート



ステップ 6　　使用可能なポートのリストから「SXP」を選択し、[宛先に追加（Add to Destination）] をクリックします。[追加（Add）] をクリックし、アクセス リスト エントリを完了します。

図 54 - 拡張アクセス リスト エントリの追加 - SXP



ステップ 7　　[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [FlexConfig] > [FlexConfigオブジェクト（FlexConfig Object）] に移動します。右上の [FlexConfigオブジェクトの追加（Add FlexConfig Object）] ボタンをクリックします。[名前（Name）] を入力します。設定に、tcp-map、tcp- options、class map を貼り付けます。

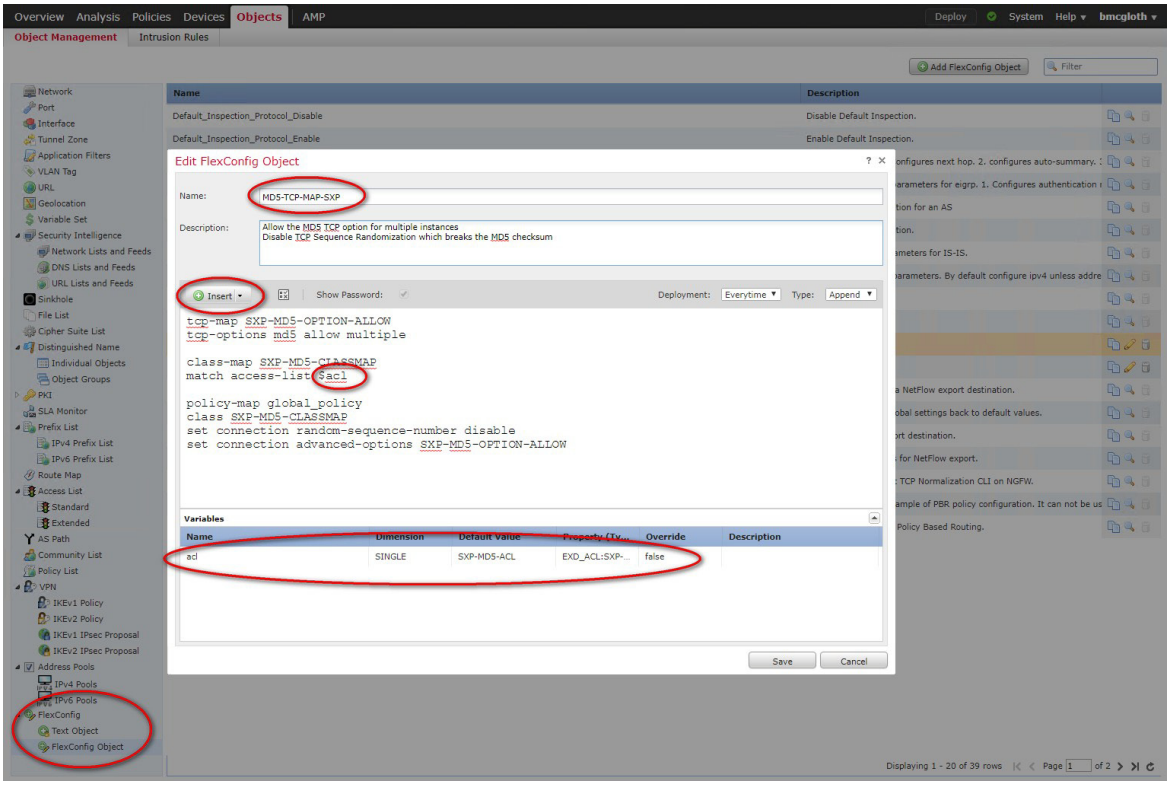
```
tcp-map SXP-MD5-OPTION-ALLOW
  tcp-options md5 allow multiple

class-map SXP-MD5-CLASSMAP
  match access-list $acl
```

[挿入（Insert）] をクリックして、ステップ 4 で作成した拡張アクセス リストを変数 **$acl** として割り当てます。global policy-map と特別な接続オプションを貼り付けます。

```
policy-map global_policy
 class SXP-MD5-CLASSMAP
  set connection random-sequence-number disable
  set connection advanced-options SXP-MD5-OPTION-ALLOW
```

[保存（Save）] をクリックします。

図 55 - FlexConfig オブジェクトの編集

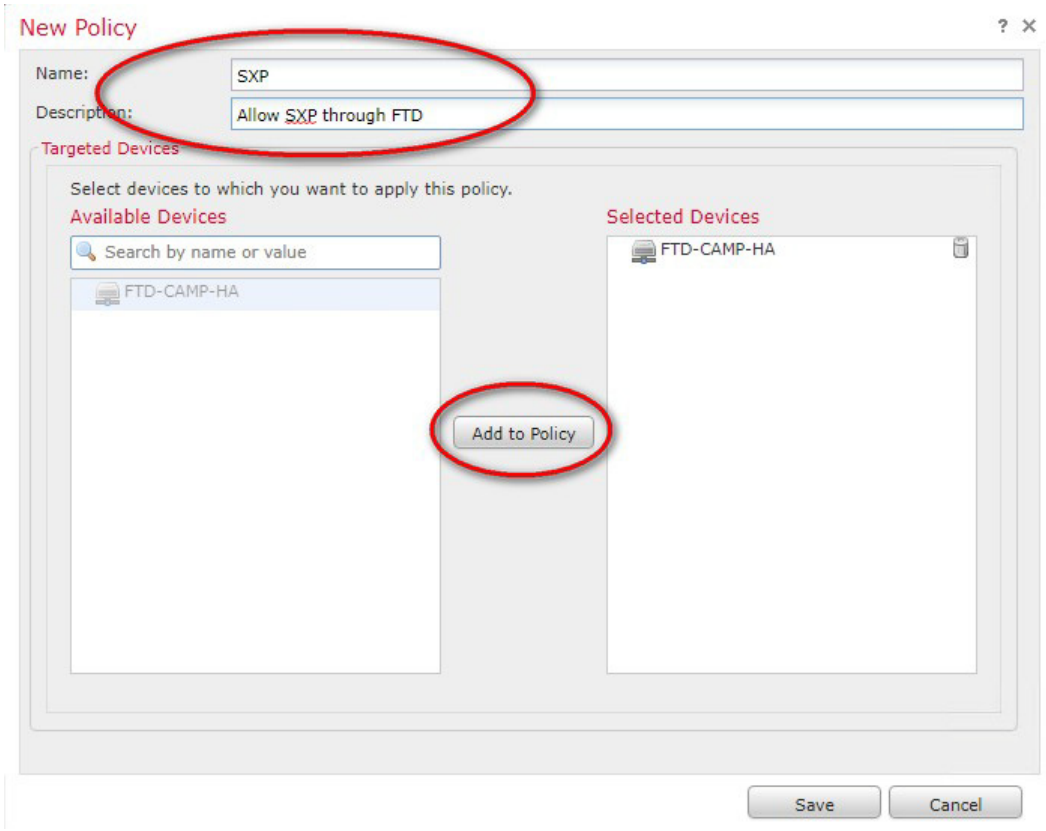


ステップ 8　　ネットワーク内のデバイス用に新しい FlexConfig ポリシーを作成します。[デバイス（Devices）] > [FlexConfig] に移動します。右上の [新しいポリシー（New Policy）] ボタンをクリックします。

図 56 - デバイス

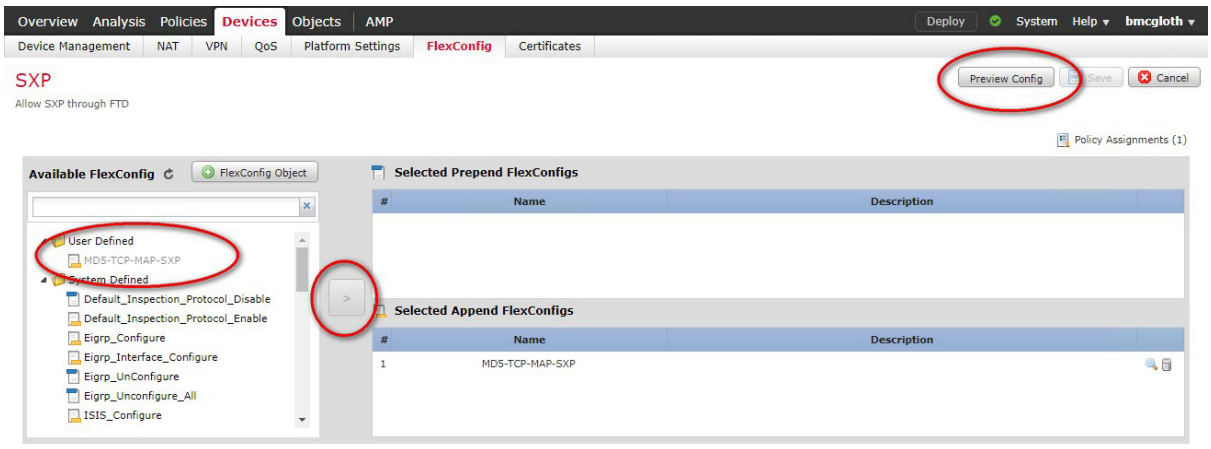
ステップ 8　　[名前（Name）] と [説明（Description）]（オプション）を入力します。使用可能なデバイスから該当のデバイスを選択し、[ポリシーに追加（Add to Policy）] ボタンをクリックします。[保存（Save）] をクリックします。

図 57 - 新しいポリシー



ステップ 9　　左側のメニューから、新たに定義された FlexConfig を選択し、矢印をクリックしてポリシーに追加します。右上の [保存（Save）] をクリックし、次に [設定のプレビュー（Preview Config）] をクリックして結果を確認します。

図 58 - FlexConfig の追加



ステップ 10　　[展開（Deploy）] をクリックし、ファイアウォールに新しい設定をインストールします。

http://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/flexconfig_policies.html [英語]

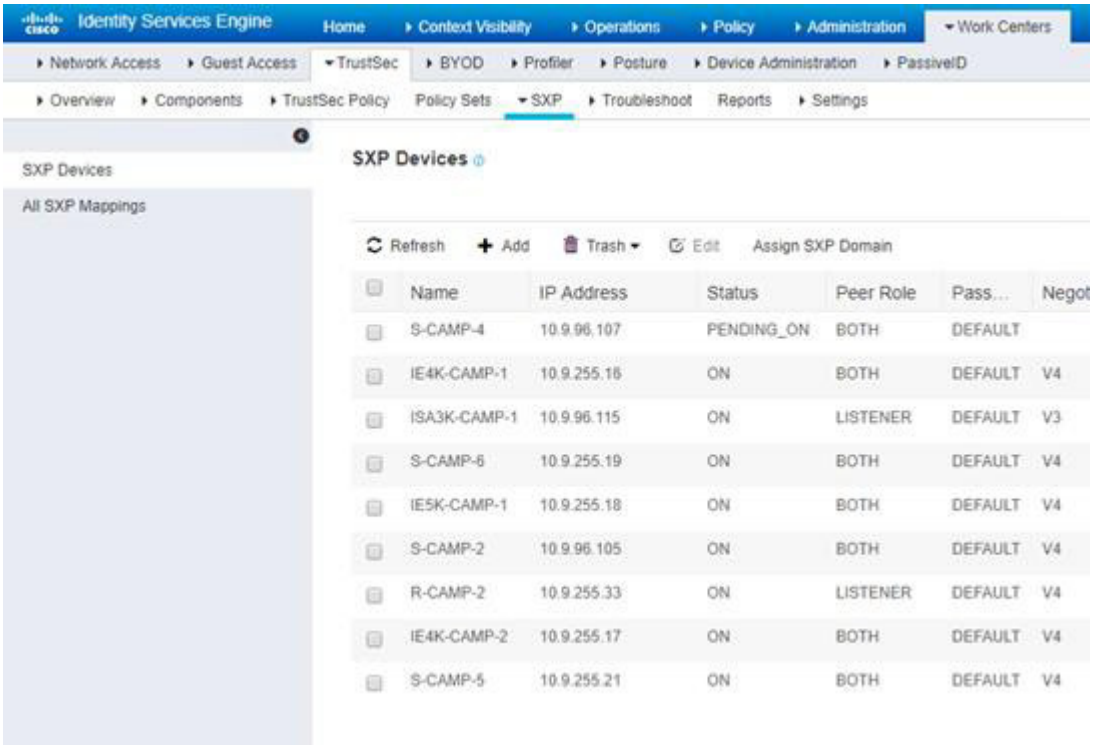
ISE での SXP デバイス ピアの設定

各 SXP 接続では、一方のピアが SXP スピーカーとして指定され、もう一方のピアは SXP リスナーとして指定されます。それぞれのピアがスピーカーおよびリスナーの両方として機能できる双方向モードに設定するのがベスト プラクティスです。接続はどちらのピアによっても開始できますが、マッピング情報は常にスピーカーからリスナーに伝播されます。Cisco ISE に追加済みの SXP ピア デバイスを表示するには、[ワークセンター（Work Centers）] > [TrustSec] > [SXP] > [SXPデバイス（SXP Devices）] の順に選択します。

SXP を使用して通信するネットワーク デバイスを ISE に追加します。

ステップ 1　　ISE で、[ワークセンター（Work Centers）] > [TrustSec] > [SXP] > [SXPデバイス（SXP Devices）] に移動します。

図 59 - SXP デバイス

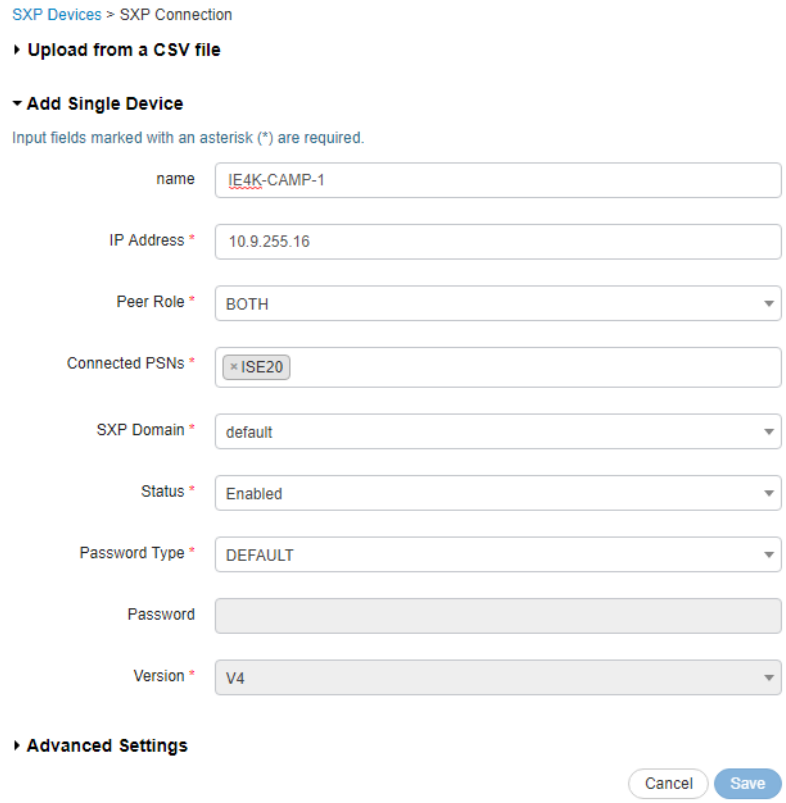


注：対応するネットワーク デバイスに SXP 通信がまだ設定されていない場合、ステータスは ***PENDING_ON*** として表示されます。

ステップ 2　　リストの上部にある [追加（Add）] ボタンをクリックします。

ステップ 3　　SXP を使用して ISE に接続する各スイッチまたはファイアウォールの [名前（Name）]、[IPアドレス（IP address）]、[ピアロール（Peer Role）]、[PSN]、[パスワード（Password）] を入力します。

図 60 - SXP デバイス



注：デバイスごとに異なるパスワードを使用する代わりに、SXP グローバル デフォルト パスワードを指定できます。グローバル パスワードを設定するには、[ワークセンター（Work Centers）] > [TrustSec] > [設定（Settings）] > [SXP設定（SXP Settings）] に移動します。

ステップ 4　　[Save（保存）] をクリックします。

ネットワーク デバイスの SXP の設定

以下に、SXP を有効にし、ISE PSN（スピーカー）とスイッチまたは ASA（リスナー）間に SXP ピア接続を設定する方法の例を示します。

ステップ 1　　ISE で認証し、PAC ファイルを確立するときに使用する、このスイッチの Cisco TrustSec デバイス ID とパスワードを指定します。このパスワードと ID は、前のステップで指定した ISE ネットワーク デバイス設定と一致する必要があります。デバイスのコマンド ラインで、次のように入力します。

```
cts credentials id {switch ID} password Cisco123
```

ステップ 2　　ピアの接続を設定する前に、Cisco TrustSec SXP をイネーブルにする必要があります。

```
cts sxp enable
```

ステップ 3　　ベスト プラクティスとして、送信元 IP アドレスを指定し、デフォルト パスワードを設定します。

```
cts sxp default source-ip {loopback or interface IP}
     cts sxp default password Cisco123
```

注：デフォルトの SXP 送信元 IP アドレスが設定されておらず、かつ接続の SXP 送信元アドレスが設定されていない場合、Cisco TrustSec ソフトウェアは既存のローカル IP アドレスから SXP 送信元 IP アドレスを抽出します。SXP 送信元アドレスは、スイッチから開始される TCP 接続ごとに異なる場合があります。

ステップ 4　　ISE PSN への SXP ピア接続を設定します。デバイスがピア モード

BOTH をサポートしていない場合は、ピアを **SPEAKER** として設定します。必ず両エンドに同じパスワードを使用してください。

```
cts sxp connection peer ISEPSN password default mode peer both
```
または
```
cts sxp connection peer ISEPSN password default mode peer speaker
```

ステップ 5　　SXP 接続が確立されたことを確認します。

```
 show cts sxp connections
```

SXP ステータスと接続に関する詳細情報を表示します。

```
IE4K-CAMP-2#sh cts sxp connections
 SXP              : Enabled
 Highest Version Supported: 4
 Default Password : Set
 Default Source IP: 10.9.255.17
Connection retry open period: 120 secs
Reconcile period: 120 secs
Retry open timer is not running
Peer-Sequence traverse limit for export: Not Set
Peer-Sequence traverse limit for import: Not Set
----------------------------------------------
Peer IP          : 10.9.10.51
Source IP        : 10.9.255.17
Conn status      : On (Speaker) :: On (Listener)
Conn version     : 4
Conn capability  : IPv4-IPv6-Subnet
Speaker Conn hold time   : 120 seconds
Listener Conn hold time   : 120 seconds
Local mode       : Both
Connection inst# : 1
TCP conn fd      : 1(Speaker) 2(Listener)
TCP conn password: default SXP password
Keepalive timer is running
Duration since last state change: 19:03:19:52 (dd:hr:mm:sec) :: 19:03:19:28
(dd:hr:mm:sec)

Total num of SXP Connections = 1
```

TrustSec 適用の有効化

以下の設定により、スイッチに適用機能を追加します。

ステップ 1　すべてのネットワーク関連のサービス要求に RADIUS 認証を使用するようにスイッチを設定します。

```
aaa authorization network cts-list group ISE
```

ステップ 2　cts 認証に TrustSec AAA サーバ グループを指定します。

```
cts authorization list cts-list
```

ステップ 3　スイッチがトラフィックに使用する SGT を指定します。

```
cts sgt 2
```

ステップ 4　グローバルおよび VLAN ごとのロールベースの適用をイネーブルにします。

```
cts role-based enforcement
cts role-based enforcement vlan-list 115-117
```

ステップ 5　スイッチのグローバルなルーティングをイネーブルにします。

```
ip routing
```

ステップ 6　スイッチ インターフェイスでインライン タギングをイネーブルにする前に、SDM モードを「routing」に変更する必要もあります。**show sdm prefer** コマンドを使用して、現在のモードを確認します。

```
IE4K-CAMP-2#sh sdm prefer
 The current template is "default" template.
 The selected template optimizes the resources in
 the switch to support this level of features for
 8 routed interfaces and 1024 VLANs.

       number of unicast mac addresses:                  16K
       number of IPv4 IGMP groups + multicast routes:    1K
       number of IPv4 unicast routes:                    18K
         number of directly-connected IPv4 hosts:        16K
         number of indirect IPv4 routes:                 2K
       number of IPv6 multicast groups:                  0
       number of IPv6 unicast routes:                    0
         number of directly-connected IPv6 addresses:    0
         number of indirect IPv6 unicast routes:         0
       number of IPv4 policy based routing aces:         0.125k
       number of IPv4/MAC qos aces:                      1.875k
       number of IPv4/MAC security aces:                 1.875k
       number of IPv6 policy based routing aces:         0
       number of IPv6 qos aces:                          0
       number of IPv6 security aces:                     0
```

ステップ 7　　SDM モードが「routing」に設定されていない場合、設定モードに入り、次のグローバル コマンドを入力します。

```
sdm prefer routing
```

このコマンドを入力すると、次の通知を受信します。

```
Changes to the running SDM preferences have been stored, but cannot take effect until
the next reload.
Use 'show sdm prefer' to see what SDM preference is currently active.
```

ステップ 8　　スイッチの設定を保存し、スイッチをリロードします。

```
Copy running-config startup-config
reload
```

ステップ 9　　スイッチがリロードされたら、アップリンクへの手動の TrustSec タギングをイネーブルにします。学習した SGT の伝播をイネーブルにし（デフォルト）、不明のトラフィックに定義済みの SGT を手動でタグ付けし、受信したタグ付きのパケットを信頼します。

```
interface GigabitEthernet1/16
 cts manual
  propagate sgt
  policy static sgt 37 trusted
```

「trusted」は、インターフェイス上の入力トラフィックでは、タグを上書きしてはいけないことを示します。

注：ISE では、システム間を移動する可能性があるタグなしトラフィックを識別するための SGT を作成する必要があります。インライン タギングを行う場合は、OTHER_UNTAGGED トラフィック用の SGT を作成します。この例のタグ 37 は、ISE プールから動的に割り当てられました。ISE で [ワークセンター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [セキュリティグループ（Security Groups）] に移動し、新しいセキュリティ グループを追加します。

ステップ 10　　TrustSec 適用は、デバイスが接続されたスイッチの入力ポートで発生するため、スイッチ間およびアップリンク Trunk ポート インターフェイスでは適用を無効にする必要があります。次に、ロールベースの適用を無効にする例を示します。

```
interface GigabitEthernet1/16
 switchport trunk allowed vlan 115-117
 switchport mode trunk
 ip flow monitor StealthWatch_Monitor input
 cts manual
  propagate sgt
  policy static sgt 37 trusted
 no cts role-based enforcement
```

TrustSec のトラブルシューティング コマンドは次のとおりです。

- show cts interface brief
- sh cts sxp sgt-map brief
- sh cts role-based counters
- sh cts role-based permissions
- show cts role-based sgt-map all
- cts refresh policy
- cts refresh environment-data

show authentication interface gigabitEthernet 2/1
show mab interface gigabitEthernet 2/1 details

『TrustSec トラブルシューティング ガイド』
https://communities.cisco.com/docs/DOC-69479 [英語]

pxGrid 設定

pxGrid の設定と導入のベスト プラクティスは、以下で確認できます。

- Cisco Platform Exchange Grid（pxGrid）は、異なるテクノロジー間でインテリジェンスを交換するための非常にセキュアなシステムを提供します。
- Firepower―脅威の迅速な封じ込め [英語]

Firepower Threat Defense（FTD）ポリシー

前半で登場した「迅速な防止」ランサムウェア防御ソリューションでは、DNS と Web 両方のセキュリティのために Cisco Umbrella と AMP for Endpoint を使用しました。高度なランサムウェア防御ソリューションは、これらのエンドポイント保護に加え、分類された URL フィルタリングおよび Talos と連動するセキュリティ インテリジェンス機能を使用してネットワーク Web セキュリティを提供します。

URL フィルタリング ブロック/インタラクティブ ブロックとセキュリティ インテリジェンス ブロックの相違点

セキュリティ インテリジェンスによる判定は、NGFW で最初に実行されるステップのひとつです。IP アドレス、ドメイン、または URL のいずれであっても、禁止条件に単純一致するパケットが検出されると接続がブロックされます。URL フィルタリングによる判定は、アクセス制御ポリシーで定義します。これは検出プロセスの後半の機能であり、AC ポリシーの作成方法によって大きく異なる場合があります。URL フィルタリング データとセキュリティ インテリジェンス データは、2 つの異なるデータ セットです。URL フィルタリング データは、分類と潜在リスク（ギャンブル、アダルト、ハッキング、ニュース、リストに関連するリスクのレベルなど）に基づいています。セキュリティ インテリジェンス データは Talos によって公開されており、観察された既知の脅威を基にしています。

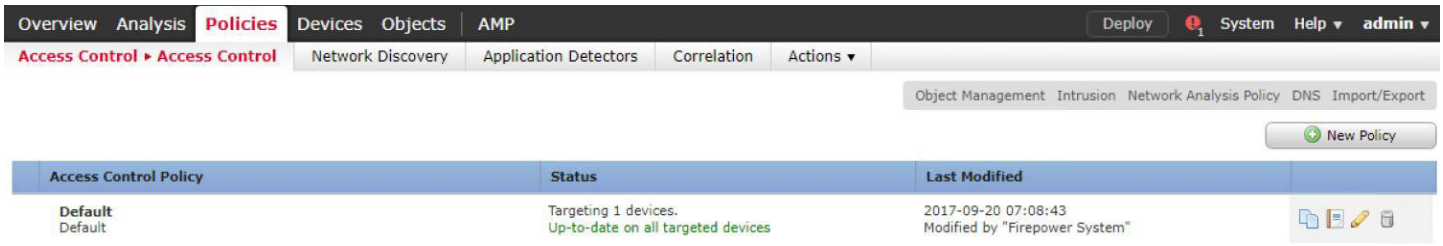
サンプルのポリシーでは、Employee は企業ポリシーでブロックされているカテゴリ（ギャンブル、ピア ツー ピア、マルウェア、ハッキング）を除き、すべてのインターネット URL にアクセスできます。システムが隔離されている場合、企業サポート サイトである「cleanme.cisco-x.com」宛てのものを除くすべての送信 Web 接続がブロックされます。pxGrid により、SGT をトラフィック送信元として使用できるので、ネットワークおよびデバイスの IP アドレスの指定を必要とせずに、非常にシンプルなポリシーを作成できます。

ここで、デバイスに HTTP または HTTPS を介してクラウド内の企業データ レイクにテレメトリの送信を許可するルールを追加します。

Firepower Management Center では、次世代ファイアウォールおよび次世代 IPS システムのポリシーは、[ポリシー（Policies）] > [アクセス制御（Access Control）] > [アクセス制御ポリシー（Access Control Policy）] > [デフォルト（Default）] を選択して設定します。

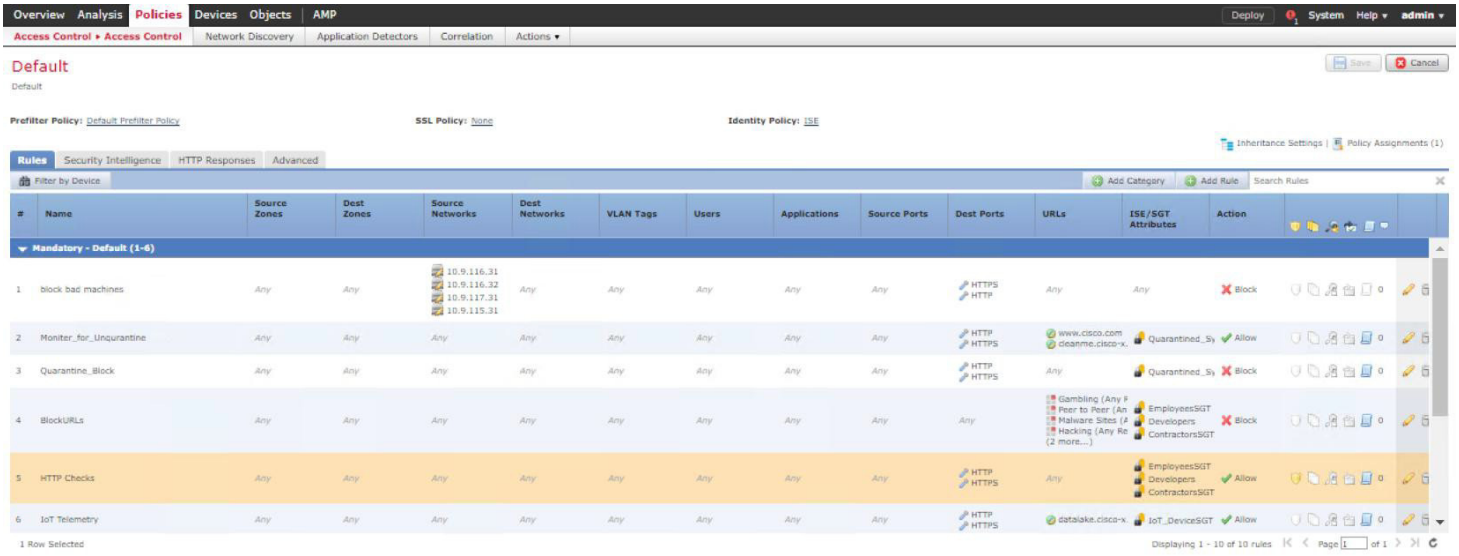
ステップ 1　　右側の鉛筆アイコンをクリックして既存のポリシーを編集するか、新しいポリシーを作成します。

図 61 - ポリシー



ステップ 2　　ポリシー ルールの上部にある [ルールの追加（Add Rule）] ボタンをクリックします。

図 62 - ポリシー―ルールの追加



ステップ 3　　[デフォルトポリシー（Default Policy）] で次のようにポリシーを作成します。

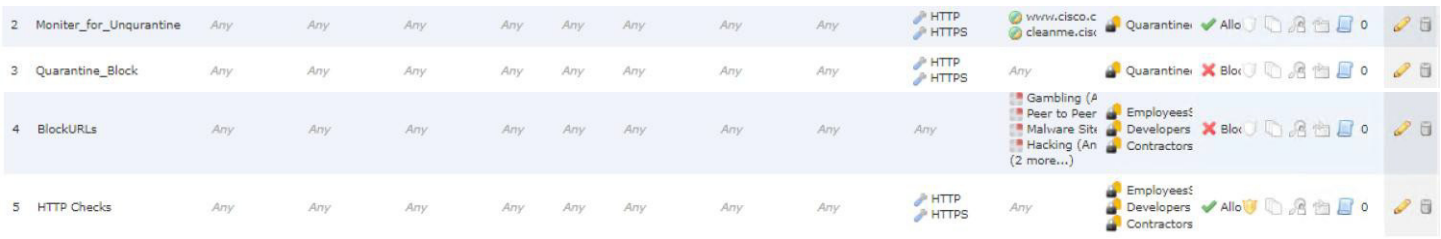
名前	アクション	送信元	宛先	プロトコル
Allow Internal	許可	内部および外部ゾーン	内部および外部ゾーン	任意

図 63 - デフォルト ポリシー—ポリシー

[必須ポリシー（Mandatory Policy）]（上から下）：
（基準として [SGT] を選択するには、ISE から SGT データを取得するように pxGrid を設定する必要があります）

名前	アクション	宛先ポート	URL	ISE/SGT 属性	注：
Monitor_for_ Unquarantine	許可	HTTP/ HTTPS	www.cisco.com/ cleanme.cisco-x.com	Quarantined.System	特定の URL にアクセスすることにより、quarantined.system に隔離解除を許可する
Quarantine_Block	ブロック	HTTP/ HTTPS	任意	Quarantined.System	quarantined.system に他のすべてのことを拒否する
Block URLs	ブロック	任意	カテゴリ：ギャンブル/ ピア ツー ピア/ マルウェア/ハッキング	EmployeeSGT DevelopersSGT ContractorSGT	Employee/Developer と Contractor SGT に、分類された URL グループをブロックする
HTTP Checks	許可	任意	任意	EmployeeSGT DevelopersSGT ContractorSGT	HTTP/HTTPS 上で他のすべてのことを許可する

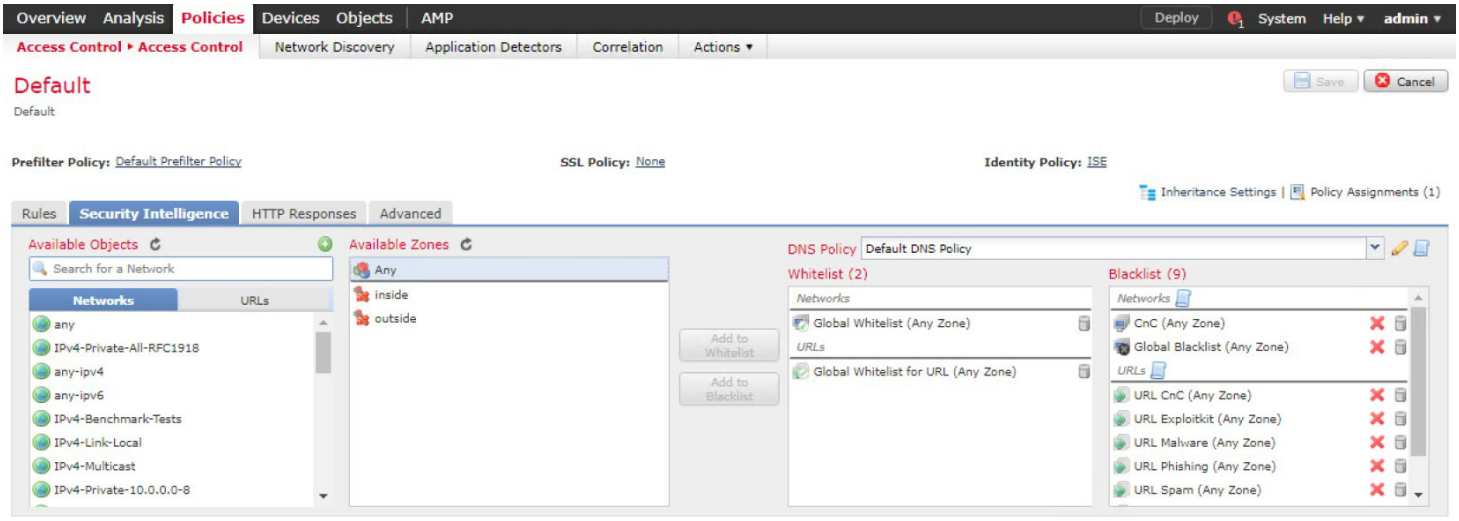
図 64 - ポリシー



ステップ 4　　[ルール（Rule）] タブの隣の [セキュリティインテリジェンス（Security Intelligence）] タブを選択し、[ポリシー（Policies）] > [アクセス制御（Access Control）] > [アクセス制御ポリシー（Access Control Policy）] > [デフォルト（Default）] の下で脅威インテリジェンス ポリシーを作成します。

[使用可能なオブジェクト（Available Object）] 検索ボックスで、[ネットワーク（Networks）] から [CnC] および [グローバルブラックリスト（Global Blacklist）] を検索します。これらをブラックリストに追加します。[URL] から該当の URL を検索します。ブラックリストに追加します（[URL CnC]、[エクスプロイトキット（Exploitkit）]、[マルウェア（Malware）]、[フィッシング（Phishing）]、[スパム（Spam）]、[疑わしい（Suspicious）]、[URLのグローバルブラックリスト（Global Blacklist for URL）] をすべてのゾーンに適用）。

図 65 - セキュリティ インテリジェンス



Stealthwatch

Cisco Stealthwatch は、NetFlow を使用してネットワーク、データセンター、ブランチ オフィス、クラウド全体の可視性を提供します。その高度なセキュリティ アナリティクス機能により、拡張ネットワーク上のステルス型攻撃を発見できます。Stealthwatch は、既存のネットワークをセキュリティ センサーおよびエンフォーサとして活用し、脅威に対する防御を飛躍的に向上させる上で役立ちます。

脅威インテリジェンスが組み込まれた Cisco Stealthwatch

Cisco Stealthwatch は、NetFlow のデータを入力として使用し、Advanced Persistent Threat（APT）、分散型サービス妨害（DDoS）、インサイダーの脅威など、さまざまな攻撃に関連する動作の検出を支援します。

可視性の向上とコンテキストに応じた脅威インテリジェンス

Cisco ISE は、ネットワーク アクティビティに関する高度な可視性とコンテキスト情報を提供します。NetFlow と ISE のコンテキスト データを Cisco Stealthwatch と共有することで、脅威の特定を加速します。どのユーザまたはデバイスが、いつどこでどのように接続したか、およびどのようにネットワーク リソースにアクセスしたかに基づき、IP アドレスのマッピングから脅威のベクトルの把握まで行うことができます。

シスコ ネットワーク インフラストラクチャをセキュリティ センサーとして使用することで、詳細な可視性、制御、アナリティクスを可能にするパワフルでスケーラブルなソリューションがもたらされます。

説明した環境は、リファレンス ネットワーク アーキテクチャを構成する複数の設計と導入ガイドに基づいています。

- 『シスコ サイバー脅威対策（v2.0）設計ガイド』 [英語]
- 『ISE 分散環境における pxGrid 設定ガイド』 [英語]
- 『Cisco Stealthwatch 6.7.1 および Cisco pxGrid 導入ガイド』 [英語]
- 『TrustSec を利用したユーザからデータセンターへのアクセス制御導入ガイド』 [英語]
- 『Stealthwatch を利用したセンサーとしてのネットワーク、および脅威の可視化と防御のための Stealthwatch 学習ネットワーク導入ガイド』 [英語]

以下に、Cisco Catalyst 3850 スイッチでの NetFlow レコードの設定の例を示します。
他のデバイスの設定については、NetFlow 設定ページ [英語] を参照してください。

NetFlow レコードを定義するには、次のコマンドを使用します。

```
flow record StealthWatch_Record
    description NetFlow record format to send to StealthWatch
    match datalink mac source address input
    match datalink mac destination address input
    match datalink vlan input
    match ipv4 ttl
    match ipv4 tos
    match ipv4 protocol
    match ipv4 source address
    match ipv4 destination address
    match transport source-port
    match transport destination-port
    match interface input
    collect interface output
    collect counter bytes long
    collect counter packets long
    collect timestamp absolute first
    collect timestamp absolute last
```

NetFlow エクスポータを定義するには、次のコマンドを使用します。

```
flow exporter StealthWatch_Exporter
    description StealthWatch Flow Exporter
    destination <FlowCollector_Address>
    source <Loopback_Interface>
    transport udp 2055
```

NetFlow モニタを定義するには、次のコマンドを使用します。

```
flow monitor StealthWatch_Monitor
    description StealthWatch Flow Monitor
    record StealthWatch_Record
    exporter StealthWatch_Exporter
    cache timeout active 60
```

最後に、トラフィックを監視するすべてのインターフェイスに Flow モニタを割り当てます。

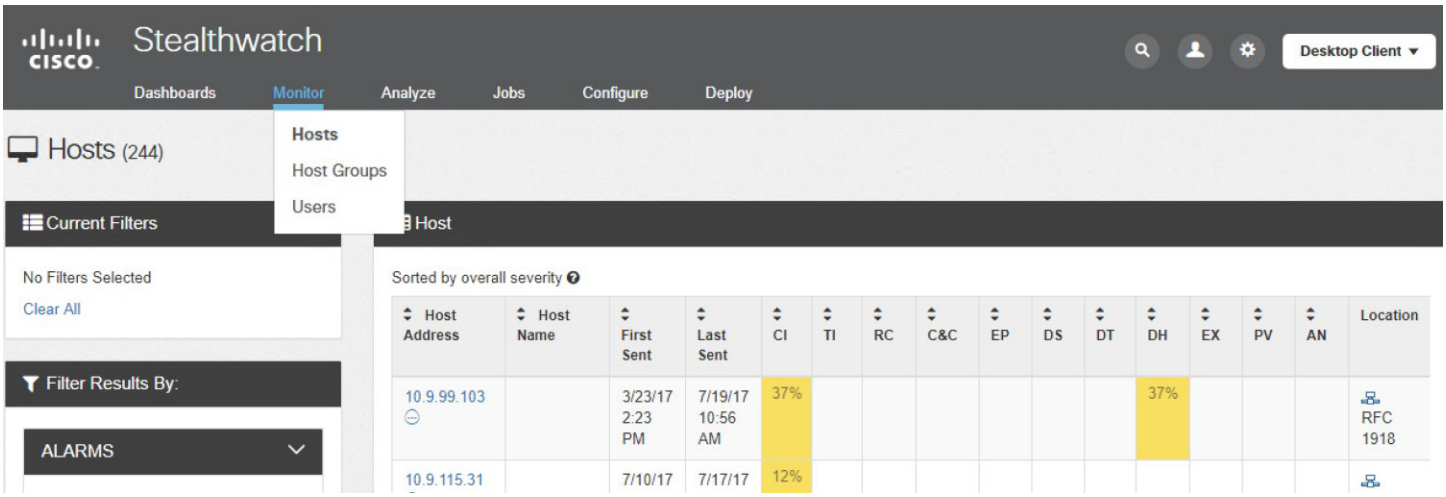
```
interface <Interface_or_VLAN>
    ip flow monitor StealthWatch_Monitor input
```

Stealthwatch と ISE の 統合

pxGrid を ISE と Stealthwatch の間に導入することで、ネットワーク管理者は、ISE から特定のユーザ名や SGT 名などの情報を入手し、ホストベースのアクティビティを監視して分析することができます。分析では、疑わしいホストのアクティビティを特定することができるので、管理者は対象を容易に隔離し、それ以降はネットワークでその脅威を防止できます。

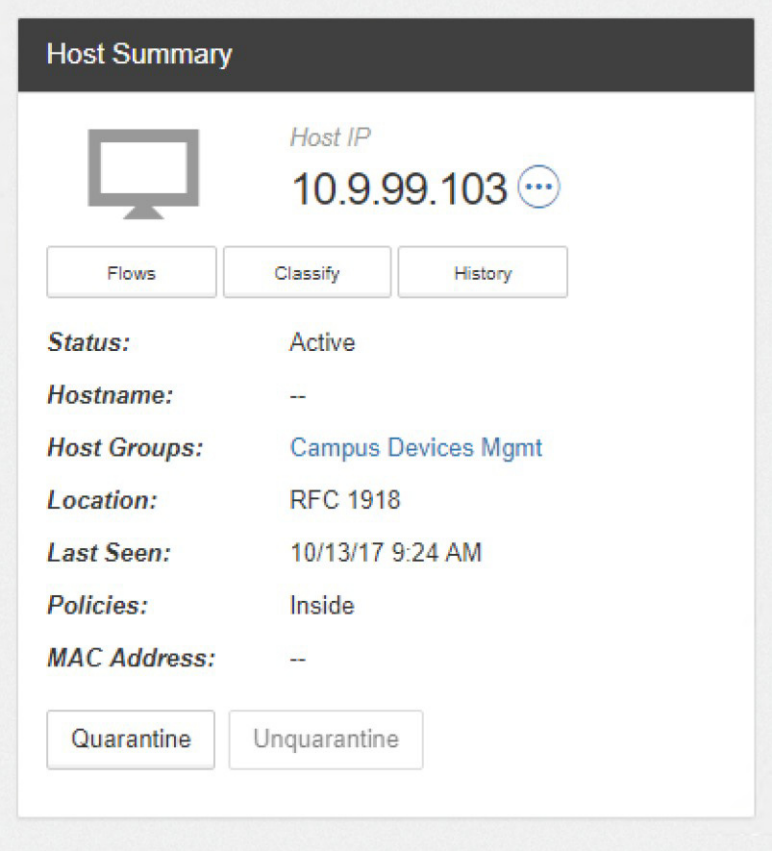
[モニタ（Monitor）] > [ホスト（Hosts）] の下で、SMC ダッシュボードを開きます。

図 66 - [モニタ（Monitor）] > [ホスト（Hosts）]



IP アドレス リンクのひとつを選択し、ホストのサマリーにアクセスすると、隔離ボタンが表示されます。このボタンを選択すると、SGT を変更する要求を ISE に対して開始できます。

図 67 - [ホストのサマリー（Host Summary）]



検証テスト

この設計の最初のフェーズのソリューション検証テストは、インターネットへの完全な接続性を持つ Windows サーバとクライアント ワークステーションで構成される企業ネットワークを作成して実施しました。

テストでは、Cisco クラウド E メール セキュリティ、Umbrella による DNS セキュリティ、エンドポイント製品向け AMP を使用しました。

ランサムウェアのサンプルをテストする前に、サーバとワークステーションを導入し、Active Directory ドメインに参加させました。ワークステーションからファイル サーバへのファイル共有を設定し、ドライブ文字にマッピングしました。電子メール サーバには Microsoft Exchange を導入し、各ワークステーションの一意のユーザに対して電子メール アカウントを作成しました。システムには、導入されている一般的な数世代のインフラストラクチャを最もよく表す各種ソフトウェア パッケージをインストールし、表 5 に示すように管理しました。

表 5 - テスト システムへのソフトウェア インストール

テスト システムにインストールされたソフトウェアのバージョン:							
	XPsp3x86	Win7sp1x64 Enterprise	Win10x64 Enterprise	2008R2 LOW-FS	2012R2 HIGH-FS	2012R2 AD	2012R2 Exchange
Java	Jre-6u45	Jre-7u80	Jre-8u91				
MS Office	2007	2013	2016				
Firefox	5	20	47				
MS IE	8	10	11	8	11	11	11
Acrobat Reader	10	11	DC				
Adobe Flash	12	18	21				
MS .net	2	3.5	4.5	3.5	3.5+4.5		3.5+4.5
MS Silverlight	3	4	5.1				
C++	9.0.3	9.0.3	9.0.3				
ホスト FW	オフ	オフ	オフ	オフ	オフ	オフ	オフ
DNS から AD	○	○	○	○	○	○	○
AD への参加	○	○	○	○	○	○	○
静的 IP および GW	○	○	○	○	○	○	○

ランサムウェア サンプルの 21 のファミリをこれらのシステム上で実行し、各システム ビルドに感染するランサムウェア、管理ユーザ権限の必要性、ローカルおよびネットワーク共有の暗号化の完了時間のベースラインを作成しました。

システムを暗号化する前の DNS 検索を実行するために、ランサムウェア サンプルは必要ありませんでした。その理由は、使用された既知のサンプルは、C2 ドメインがすでにシャットダウンまたは移動されているためで、これらのサンプルはベースライン システムでは機能せず、その後のテストから削除されました。

すべてのテスト サンプルは Threat Grid ファイル分析リポジトリから取得されたため、コネクタによってファイルの SHA-256 ハッシュ値が計算され、チェックされると、これらのファイルは AMP に即座に認識されました。テスト用のランサムウェアの一意のバージョンを作成するために、再ハッシュ ユーティリティを使用して、実行可能ファイルを変更し、無害なスペースやアノテーションを挿入することにより、ランサムウェア サンプルの動作に影響を与えずに結果ファイル ハッシュを変更しました。これにより、すべての製品の低拡散度ファイルの自動ファイル分析機能をテストしました。

高度なランサムウェア ソリューションの検証テスト

「迅速な防止」ランサムウェア防御ソリューションでは、Cisco クラウド E メール セキュリティ、Cisco Umbrella、エンドポイント向け Cisco AMP を使用しましたが、高度なランサムウェア ソリューションには、さらに表 6 に示すほぼアプライアンスベースのシスコ セキュリティ製品ラインを使用しました。

表 6 – 高度なランサムウェア ソリューション検証テスト

製品	説明	プラットフォーム
Stealthwatch	NetFlow の収集と分析	仮想またはアプライアンス
ISE	ネットワークに接続するデバイスの認証とプロファイル作成	仮想またはアプライアンス
Cognitive Threat Analytics	SW からのフローの分析	クラウド
Firepower Management Center	Firepower Threat Defense システムの管理	仮想またはアプライアンス
Firepower Threat Defense	Firepower Threat Defense ソフトウェア イメージを実行するセキュリティ プラットフォーム	仮想および 2100、4100、9300
ASA	ファイアウォール	ASA5500-X
ASA-ASDM	ローカル FW 管理	ASA5500-X
ASA 上の NGIPS	保護と制御	ASA5500-X
AnyConnect	セキュア モビリティ クライアント	すべて
Catalyst スイッチ	アグリゲーション	6880 6807-XL
	アクセス	3650、3850

ソリューション コンポーネントの実装

この高度なフェーズでは、次のコンポーネントと機能をセットアップしました。

1. Firepower Threat Defense と脅威インテリジェンス機能
2. Cisco Identity Service Engine（ISE）
3. Cisco TrustSec
4. Cisco Stealthwatch

高度なランサムウェアのテストでは、Windows ベースのクライアントと、メール、ファイル、Active Directory サーバを含む少数のサーバで構成されるグループを構築しました。これらの Windows ベースのクライアントには、Windows XP、Windows 7、Windows 10 が搭載されました。電子メールとファイル共有を介してランサムウェアを配信するために、Windows 2008 サーバおよび Windows 2012 サーバも構築しました。

テストの目標

この高度なランサムウェア ソリューションのテストは、企業クライアント/サーバと、マルウェアやランサムウェア、またはデバイス/ネットワークを感染させるエクスプロイト キットなどのコンポーネントをホストしている可能性がある外部インターネット サーバとの悪意のある通信を効率的に識別できるかを検証するために構築されました。

さらに、複数のセグメンテーション ポイント レイヤを設定して、ワームベースのランサムウェアがネットワークの各セグメントに感染するのを防止しました。

テストのセットアップと各コンポーネントの役割

FTD と ISE

FTD と ISE はともにセキュリティ ポリシー適用ポイントです。FTD には、特定の顧客要件に応じて設定できる基本の受信/発信アクセス制御を含む複数のアクセス ポリシーを設定しました。FTD のアクセス ポリシーには、送信元および宛先を ISE セキュリティ タギングで管理できるポリシーも含まれました。セキュリティ タギングをベースとするポリシーは、特定のホストが ISE の「認可変更」（隔離済み）の対象になったときに、適用に使用されます。

さらに、FTD には Talos Threat Intelligence 機能を利用するポリシーを設定しました。この機能により、FTD は悪質な可能性があるすべての送信トラフィック（主に HTTP と HTTPS）を監視できます。

脅威の迅速な封じ込め機能を提供するために、FTD と ISE の間に pxGrid 関係を設定しました。

ISE および TrustSec

基本のセキュリティ グループ タギング セグメンテーションを提供するために、ISE のセキュリティ タグ ポリシー セットをサポート対象の Cisco スイッチにダウンロードしました。これらの SGACL を、スイッチのさまざまなレイヤに入念に設定しました。これらの SGACL には、「隔離済み」送信元タグも含まれました。この SGACL は、適用されたタグ付きパケットが転送された場合にのみ有効になります。

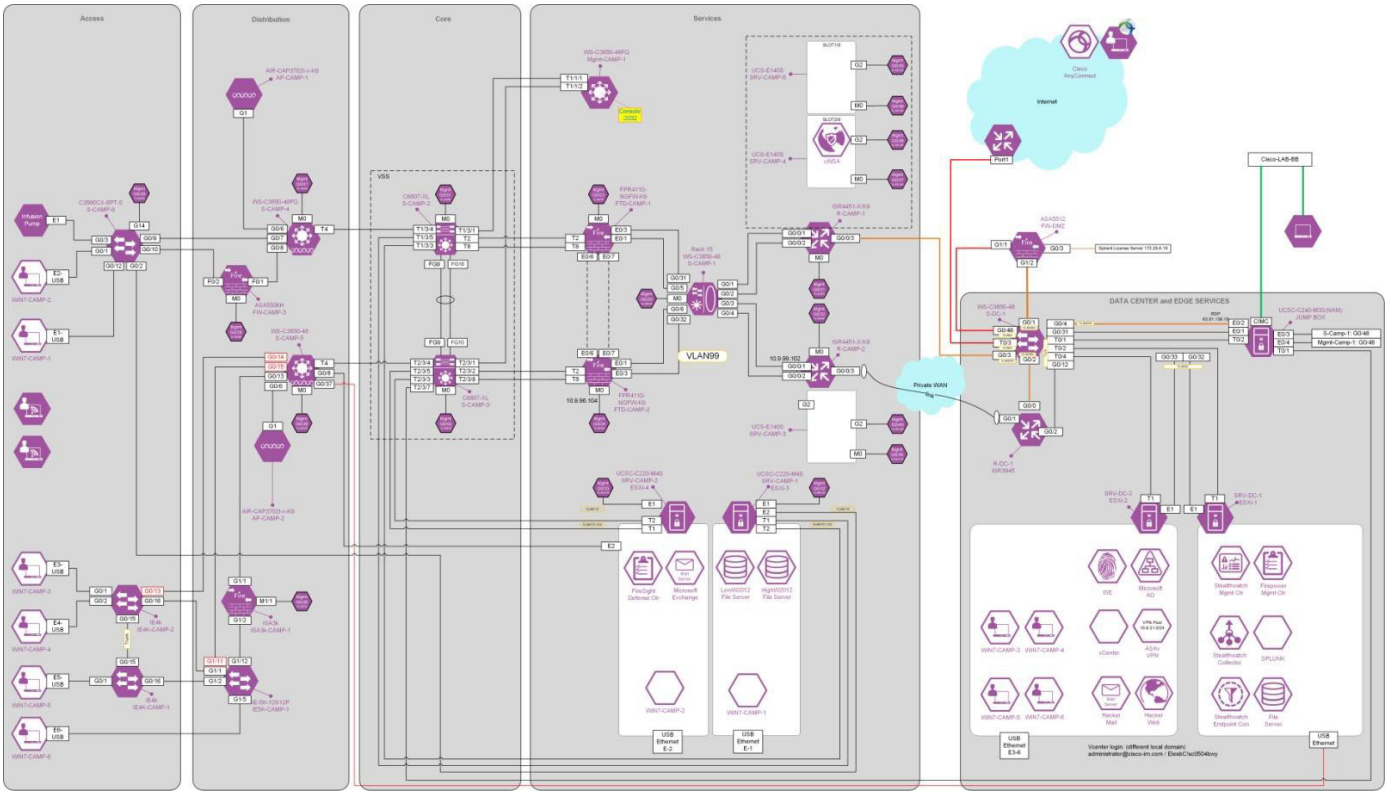
ISE と Stealthwatch

FTD と ISE 間の関係と同様に、ISE と Stealthwatch との間にも PXGrid を設定しました。この設定により、管理者は Stealthwatch トラフィック分析レポート内で、実際のクライアント認証済みのユーザ名（ISE データベースからプッシュ配信された情報）を使用して送信元オブジェクトを識別できます。さらに、StealthWatch のホストの詳細レポートから、ISE への認可変更を開始することもできます。その後 ISE は、ホストのタグを「隔離済み」に変更できます。

ネットワークトポロジ

ネットワークトポロジには、上記で説明したすべてのコンポーネントが含まれます。

図 68 - ネットワークトポロジ



検証テスト

実施したテストの概要

このテストは、ランサムウェアに対するさまざまなシスコ セキュリティ製品の統合と一般的な機能を検証することを目的としています。検証プロセスの手法は、ネットワークを介して適用されるサービスのレイヤに基づいています。

以下の表に、環境の検証のために実施したテストの概要を示します。

表 2. テスト シナリオ

テスト	手法
ISE を使用してセキュリティ グループ タグ ACL をスイッチに導入して適用する	ポリシーを ISE に作成し、サポート対象のシスコ スイッチに SGACL を伝播する。動的な割り当てのために SXP を使用する。
ISE ローカル認証を使用して内部ホストにタグ付けする	ISE は Active Directory に基づいてユーザを認証し、適用のために「Employee」タグを割り当てる。 VPN クライアントを介してネットワークにアクセスしたすべてのユーザに、「VPN User」としてタグ付けする。
ユーザが悪意のある C2 Web サイトにアクセスした際の、ISE による COA を検証する	FTD を使用して、悪意のあるコマンド/コントロール Web サイトへの内部デバイスからのアクセスを監視する。FTD は、そのアクションにフラグを立てると、COA を ISE に要求する。ISE は特定のホストのタグを「Employee」から「Quarantine」に変更する。
隔離解除方法を検証する	隔離デバイスのアクセスを制限するポリシーを FTD に設定する。また、証拠として特定のサイトにアクセスすることによって隔離デバイスの隔離を解除するポリシーを ISE に設定する。
Stealthwatch 管理コンソールのホスト デバイス レポート ページを使用して、手動で隔離/隔離解除する	タグが付けられているホストを特定し、SMC から隔離/隔離解除アクションを実行する。
VPN タギング	リモート アクセス VPN 接続によってネットワークにオンボーディングするユーザにセキュリティ グループ タギングを適用する。
Cisco Identity Services Engine（ISE）の統合	以下のコンポーネントが PXGrid によって ISE と統合されていることを確認する。 ● インフラストラクチャ全体の ISE 認証および許可サービス - Nexus スイッチング - UCS ドメイン - FTD プラットフォーム - Stealthwatch

結果の概要

次の表に、テスト結果の概要を示します。

表 3. 結果の概要

テスト内容	コンポーネント	結果
内部ホストへのタグ付け	ISE、RADIUS、Active Directory	ユーザは認証時に正常にタグ付けされました
VPN ユーザへのタグ付け	ISE、RADIUS、Active Directory	ユーザは認証時に正常にタグ付けされました
TrustSec のセットアップ（SGACL ダウンロード）	ISE、サポート対象スイッチ	ISE の SGACL 設定は、サポート対象のシスコ スイッチに正常にアップロードされました。
スイッチ セットアップ時の SXP とポリシー適用	ISE、サポート対象スイッチ	ISE サーバに設定された TrustSec ポリシー セットに基づいて、トラフィックを許可または拒否できました
FTD と ISE による COA	FTD、ISE	FTD の脅威インテリジェンス機能を通じて、悪意のある C2 サイトにアクセスしたクライアント デバイスを FTD と ISE によって特定し、デバイスを「隔離済み」に認可変更（COA）できました。隔離されたデバイスのアクセスを、SGACL（スイッチ レベル）および FTD によって管理できました。
デバイスの自動隔離解除	ISE、FTD、隔離デバイス、隔離解除 Web サイト	隔離解除のための ISE ポリシーに含まれる Web サイトにアクセスすることで、デバイスを正常に隔離解除できました。
StealthWatch 管理コンソールを使用した手動での隔離/隔離解除	Stealthwatch 管理コンソール、ISE	StealthWatch 管理コンソールから手動で正常にデバイスを隔離/隔離解除できました

まとめ

ランサムウェアは、拡大を続ける、組織に与える影響が肥大している問題です。攻撃に成功した攻撃者は、組織のビジネスに大きな悪影響をもたらします。

このソリューションは、組織の継続という目標を達成するとともに、重要なシステムの制御を失い、人質に取られる可能性を最小限に抑えることで安心感をもたらします。

シスコのランサムウェア防御ソリューションを使用すると、新しい悪意のあるキャンペーンの開始から脅威インテリジェンスベースの保護までの時間を、業界平均の 100 日間よりはるかに短い 30 分～ 4 時間に抑えることができます。[4]シスコのランサムウェア防御は、可能な場所での防止、迅速な検出、すばやい封じ込めに焦点を当てることにより、防御が破られた場合のランサムウェアの影響を低減します。

[4] http://www.cisco.com/c/m/ja_jp/offers/sc04/2016-annual-security-report/index.html?KeyCode=001031927

参考資料

Cisco SAFE でセキュリティをシンプル化：
www.cisco.com/jp/go/safe

Cisco クラウド E メール セキュリティ：
https://www.cisco.com/c/ja_jp/products/security/email-security/index.html
Cisco E メール セキュリティ：
https://www.cisco.com/c/ja_jp/products/security/email-security/index.html
Cisco E メール URL コンテンツ フィルタリングのベスト プラクティス：
https://www.cisco.com/c/ja_jp/support/docs/security/email-security-appliance/118775-technote-esa-00.html

Cisco DNS セキュリティ [英語]：
https://www.opendns.com/enterprise-security/threat-enforcement/
Cisco Umbrella ローミング クライアントのインストール [英語]：
http://info.umbrella.com/rs/opendns/images/TD-Umbrella-Mobility-Roaming-Client-Guide.pdf
DNS のベスト プラクティス [英語]：
https://www.cisco.com/c/en/us/about/security-center/dns-best-practices.html
Windows Server 2012 および 2012 R2 の DNS フォワーディングの設定 [英語]：
https://support.opendns.com/entries/47071344-Windows-Server-2012-and-2012-R2

エンドポイント向け Cisco AMP：
https://www.cisco.com/c/ja_jp/products/security/fireamp-endpoints/index.html
Cisco Advanced Malware Protection：
https://www.cisco.com/c/ja_jp/products/security/advanced-malware-protection/index.html

Cisco Talos - 包括的な脅威インテリジェンス：
https://www.cisco.com/c/ja_jp/products/security/talos.html
Cisco ThreatGrid：
https://www.cisco.com/c/ja_jp/solutions/enterprise-networks/amp-threat-grid/index.html

Cisco Web セキュリティ：
https://www.cisco.com/c/ja_jp/products/security/web-security/index.html

Network as a Sensor：
https://www.cisco.com/c/ja_jp/solutions/enterprise-networks/enterprise-network-security/net-sensor.html
Cisco Stealthwatch：
https://www.cisco.com/c/ja_jp/products/security/stealthwatch/index.html
Cisco Identity Services Engine と TrustSec（Network as an Enforcer）：
https://www.cisco.com/c/ja_jp/solutions/enterprise-networks/enterprise-network-security/net-enforcer.html
Cisco Rapid Threat Containment ソリューション [英語]：
https://www.cisco.com/c/en/us/solutions/enterprise-networks/rapid-threat-containment/index.html

Cisco Firepower Management Center：
https://www.cisco.com/c/ja_jp/products/security/firesight-management-center/index.html