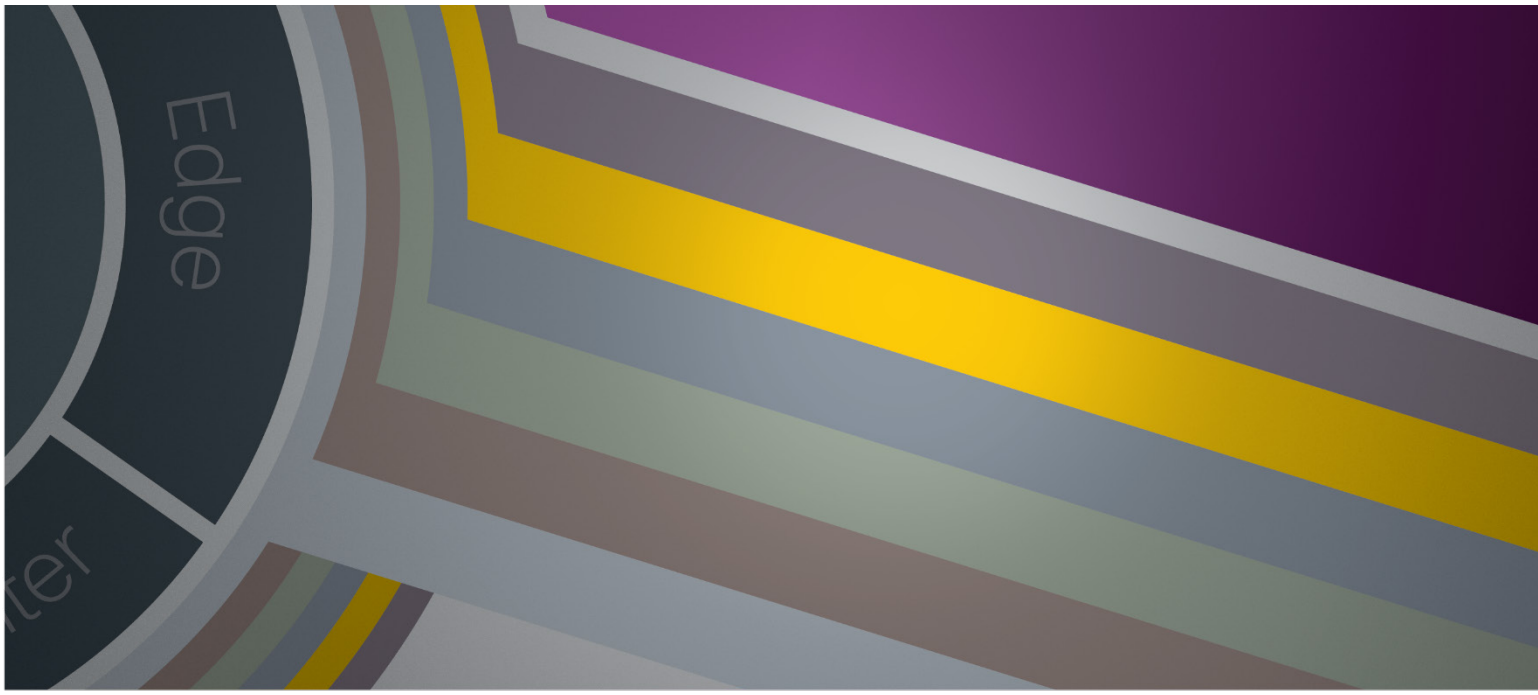


IoT Threat Defense for Manufacturing

SAFE 設計ガイド

セキュリティ ドメイン：脅威に対する防御

2018 年 5 月更新

目次

概要

Internet of Things（IoT）はすべてのビジネスに影響を与え、企業に接続するデバイスに対する考え方を根本から変えつつあります。これらのモノは、企業の攻撃対象領域を大きく広げます。製造業は最も標的となることが多いセクターの 1 つであり、32% のサイバー攻撃が製造業で起きています。[1]

IoT デバイスや制御システムは脆弱です。製造業の IoT デバイスはセキュリティ機能をほとんど、またはまったく搭載していないため、ハッカーの標的となっています。暗号化を使用している IoT デバイスはほとんどなく、パッチの適用や脆弱性のアップデートの観点から見ると、多くが適切に管理されていません。IoT デバイスの設計には、単にセキュリティが組み込まれていませんでした。そのため、IoT デバイスは DDoS やネットワーク侵入などの高度な攻撃に関与したり、ゾンビに変換されたり、永続的なエージェントとして使用されたり、ビジネス全体を停止または中断して身代金を要求する目的で使用されたりする可能性があります。最悪のケースとして、IoT デバイスは身体的危害を与えるために使用されることがあります。

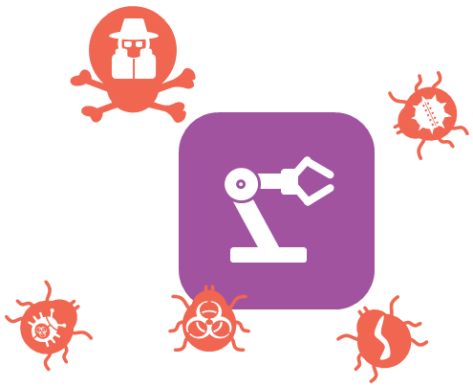
多くの製造業者は、運用テクノロジー（OT）環境と今日の IT 環境に存在する脅威の対策に取り組んでいます。

1. 脆弱性が見つかるシステム、アプリケーション、および機器が増えつつあります。2009 年以降、発見された脆弱性の数は 2,400% 増加しています。
2. 一部の自動化ベンダーは、今もなお（Windows 98 などの）サポートを終了したプラットフォームが必要なアプリケーションを出荷しています。
3. 基本的な制御プロトコル（最も広く導入されている E/IP ベースの制御プロトコル）では、2015 年の終わり頃まで認証が取り入れられていませんでした。

こうした問題があるにもかかわらず、製造業者は、効率化を図ったり、幅広い機器のインテリジェンスを活用したり、運用を改善したり、顧客満足度を向上させたりするために Internet of Things（IoT）を利用しています。そのため、このような非常に脆弱な環境の接続が 3 年以内にほぼ 2 倍に増加したのです。

[1] https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2015_Final_S508C.pdf [英語]

つ目次に戻る

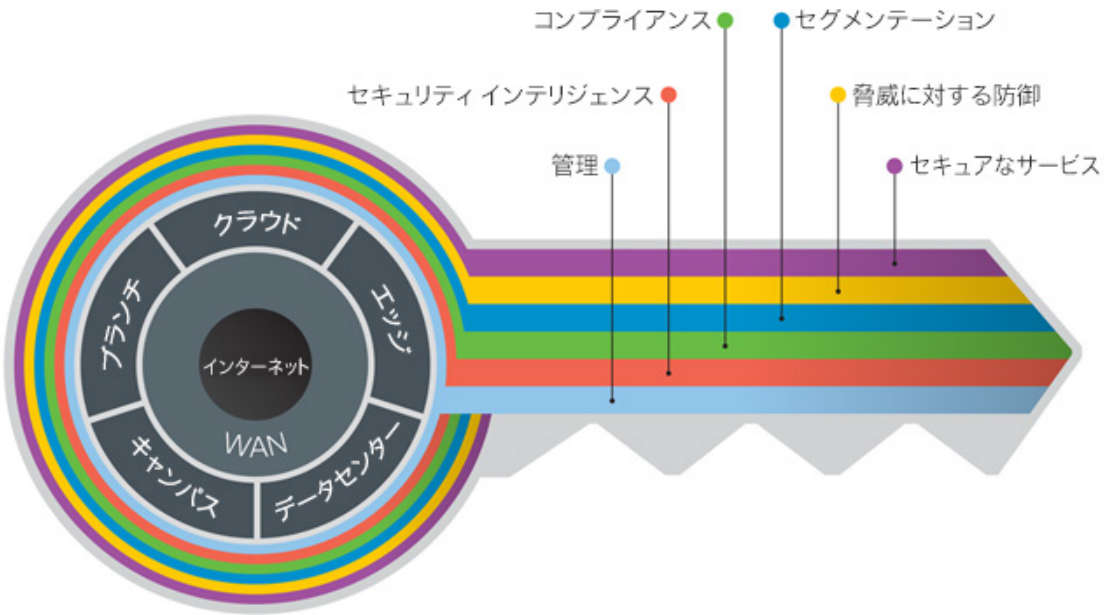


より多くのデバイスの接続を求める声が高まりつつある中、攻撃対象領域が大幅に増加していることからセキュリティは複雑化しています。OT と IT のプロフェッショナルは、製造業者のネットワークとデバイスを保護してビジネスの安全性と継続性を確保したいと考えています。

シスコの IoT Threat Defense ソリューションは、このような製造業者の課題を解決します。

シスコの IoT Threat Defense ソリューションは、ビジネス フローと使用例から始まるセキュリティのための SAFE モデルを使用して、構造的アプローチで IoT を保護します。この設計ガイドでは、本アーキテクチャの検証に使用するコンポーネントと設定について詳しく説明しており、インダストリ 4.0 や産業用 IoT を実現するためにデジタル変革に着手する製造業者を保護していきます。このアーキテクチャは、SAFE セキュリティ リファレンス アーキテクチャに含まれています。

図 1：SAFE の鍵

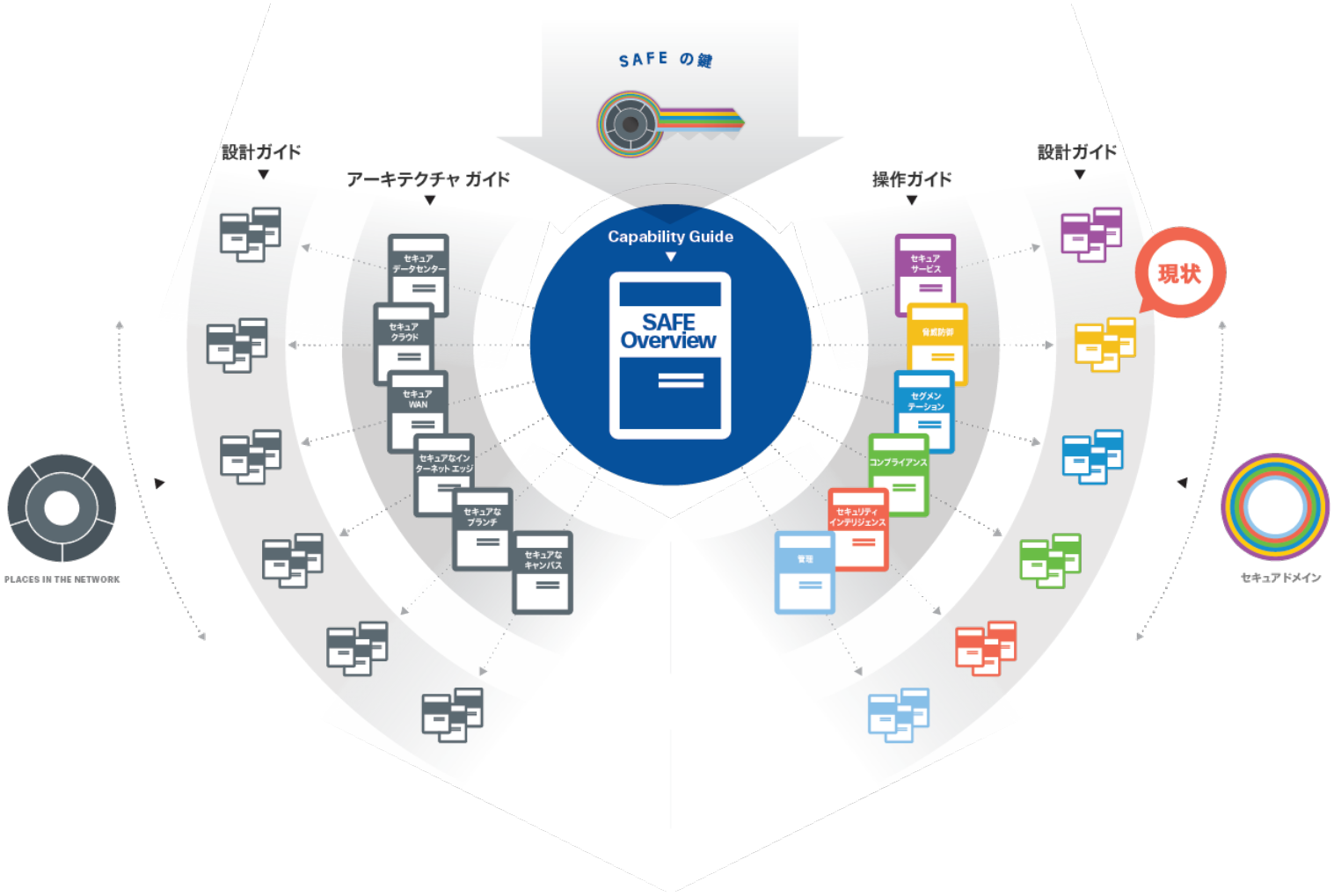


SAFE では、複雑で全体的なセキュリティを Places in the Network（PIN）とセキュア ドメインに切り分けます。

ちょ目次に戻る

SAFE は、対象者のニーズに基づき複雑なビューが利用されているエンドツーエンドのセキュリティをシンプルにします。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。

図 2：SAFE のガイダンスの階層



Cisco SAFE でセキュリティをシンプルにする方法とこれらのシスコ検証済みデザイン（CVD）の詳細については、https://www.cisco.com/c/ja_jp/solutions/enterprise/design-zone-security/landing_safe.html を参照してください。

つ目次に戻る

6

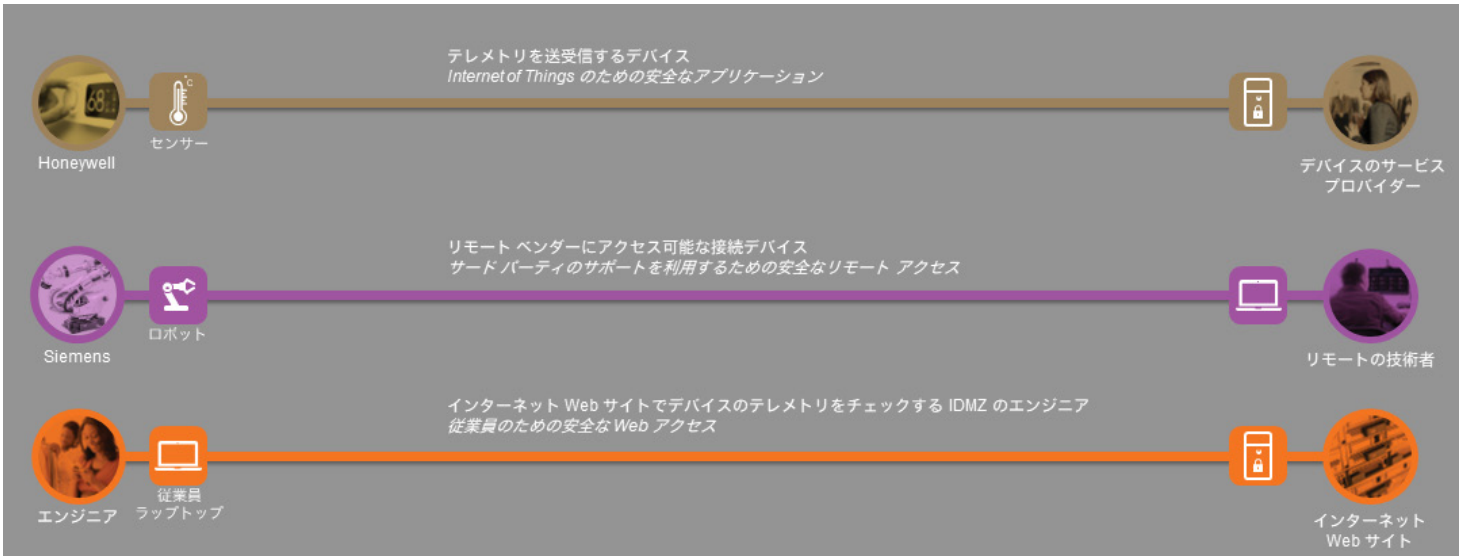
製造業者のビジネス フロー

SAFE は、ビジネス フロー（通信フロー）の概念を使用して、これらのアクティビティに影響を与える可能性がある脅威を特定し、それに従ってビジネス機能を保護するためにセキュリティを対応させます。

製造業の IoT 領域のセキュリティに影響するビジネス使用例は、以下のとおりです。

- ネットワーク上のデバイスとアプリケーションの保護
- サポートを行うためのリモート アクセスの提供
- 同じネットワーク上のリスクの高いアクティビティに対する防御

図 3：ビジネス使用例



ちょ目次に戻る

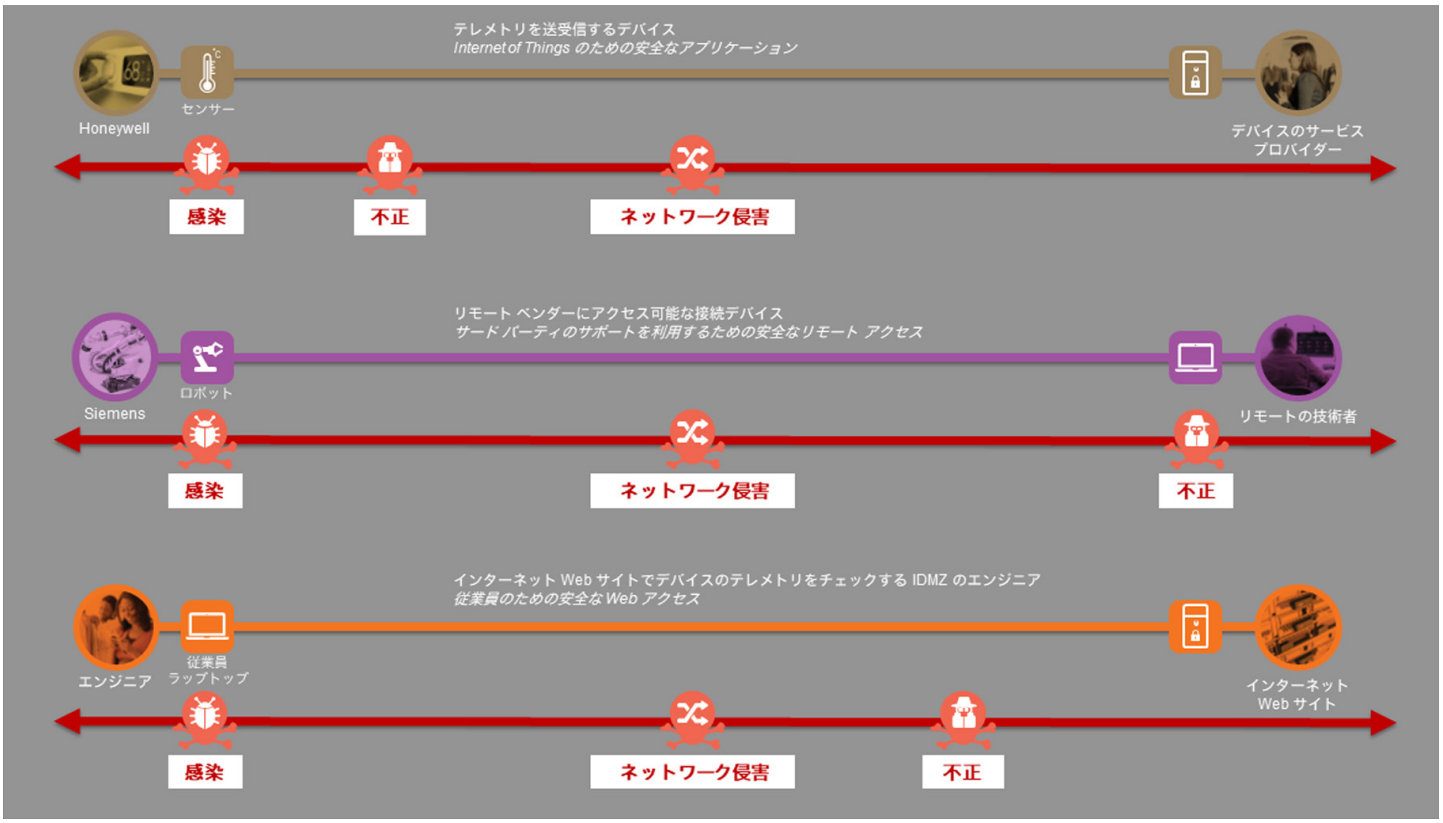
7

製造業の攻撃対象領域

IoT Threat Defense ソリューションは、製造業者のネットワークで見つかった、すべてのビジネス使用例にわたる攻撃対象領域にセキュリティ制御を適用することでシステムを保護します。製造業者のネットワークに対する脅威とリスクは、デバイス、人、およびネットワークの周辺に存在します。

ハッカーは、不正 ID、マルウェア感染および持続的標的型攻撃により、デバイスやネットワークを支配できます。デバイスへの従来のリモート管理アクセス（モデムなど）は、リスクを増大させます。ゼロデイ脆弱性攻撃は、既存の制御をすり抜けることができます。

図 4：製造業の攻撃対象領域



つ目次に戻る

ソリューション概要

IoT Threat Defense for Manufacturing は、以下に示す 4 つの重要な領域でこれらの脅威が IoT にもたらす課題に対処します。

Cisco IoT Threat Defense は、ネットワークにいくつかのポイント オブ プレゼンスを設置して IoT デバイスの周辺に保護膜を作る、テスト済みの階層化されたアーキテクチャとサービスです。IoT デバイスの安全なセグメンテーションにより、IoT デバイスが正常に機能するために必要なすべてのデータと通信がスムーズに流れ、ビジネス目標を安全に実現できるようになります。それと同時に、シスコは脅威を検出して防御し、サービスの復元力を維持するための可視性と分析機能を提供します。安全なリモート アクセスにより、お客様は自社のネットワークに対する第三者のアクセスを可視化して制御できます。このソリューションのコンサルティングおよびサービス コンポーネントは、お客様が IoT のリスクを評価するとともに、安全な IoT 環境を設計して導入し、継続的に運用するうえで役に立ちます。

つ目次に戻る

セキュリティ機能

IoT デバイスや IoT システムを保護するには、適切な防御層を構築するための特定の機能が必要です。このような防御に最適な SAFE の方法論における各機能（青色の円）は、これらの各領域に対応しています。これらの機能は連携していくつかの防御層を形成し、組織と IoT インフラストラクチャを保護します。

セグメンテーション

セキュリティでは、一般に可視性することから着手します。ただし、導入済みの管理されている IoT システムについては、最初にセグメンテーションを行います。セグメンテーションとは、ロールと機能に基づいてネットワーク アクセスを制限し、ネットワークを分割することです。

組織のセキュリティを侵害したり、このような非常に脆弱な IoT デバイスにアクセスしたりする方法は数多くあります。最も一般的なのは、ユーザのシステムを感染させ、妨げになるものが何もない IoT デバイスに接続された企業のインフラストラクチャ全体に拡散する、メールによるフィッシング攻撃や Web ホスト型のマルバタイジングです。そのため、こうした IoT デバイスはユーザの環境や他の IoT デバイスから分離する必要があります。

以下の機能は、ロールと機能に基づいてネットワーク アクセスを制限し、ネットワークを分割します。

アイコン	機能	説明
	アイデンティティ	コンテキストに基づくデバイスとユーザの識別：時刻、場所、ポスチャなどのコンテキスト項目を含む、既知のユーザとデバイスへの接続を制限します。
	プロファイル	デバイスのプロファイリング：ネットワークにデバイスが接続されたときに、プロファイリングによってデバイスの区分と分類に必要なコンテキスト要素を定義します。
	TrustSec	アイデンティティに基づくソフトウェア定義のセグメンテーション：ロールとポリシーに基づいて IoT システムとユーザを分離し、既知の IoT デバイスによるネットワークへの接続を阻止します。
	ファイアウォール	アイデンティティに基づくファイアウォール セグメンテーション：運用業務を妨げることなく IO と OT を統合し、ロールとポリシーに基づいてトラフィックを分離します。

つ目次に戻る

可視性と分析

既知の IoT デバイスとユーザに対する初期レベルのセグメンテーションを行ったら、改善された可視性のメソッドを追加することにより、ネットワーク上の未知のデバイスを特定できます。すべてのデバイスを特定して把握すると、既存の制御をすり抜ける脅威の検出と修復が容易になります。

以下の機能は、ネットワーク全体にわたる広範な優れた可視性を提供します。

アイコン	機能	説明
	アイデンティティ	コンテキストに基づくデバイスとユーザの識別：時刻、場所、ポスチャなどのコンテキスト項目を含むユーザとデバイス。
	DNS セキュリティ	DNS ベースのセキュリティ：名前解決に基づいてネットワークで動作するすべてのデバイスのインターネット通信を特定し、悪意のあるドメインをブロックするとともにコマンド & コントロール コールバックを遮断します。
	侵入防御	侵入防御：ディープ パケット インスペクションで IoT を可視化し、攻撃、エクスプロイト、および情報収集をブロックします。
	ネットワーク モニタリング	インフラストラクチャの通信フローの監視：情報を活用してネットワークの問題をより的確に特定し、異常なデバイスのトラフィック フローを明らかにしてアラートを出します。
	分析および異常検出	正常な IoT のネットワーク動作を分析し、運用とネットワークに接続された既知のデバイスのベースラインを作成します。異常なアクティビティが開始されたらアラートを生成します。
	脅威インテリジェンス	脅威インテリジェンス：既存のマルウェアと通信ベクトルの知識、および取得した新たな脅威の動作に関する知識を提供します。

つ目次に戻る

リモート アクセス

高額かつ高度な最新化への投資を維持するために、デバッグとメンテナンスをベンダーに頼らなければならなくなる可能性があります。そのためには、ベンダーがリモートから工場にアクセスできるようにする必要があります。安全なリモート アクセスは、従来のモデムやベンダーがこれまで使用していた他の接続方法に代わるものであり、デジタル接続ネットワークのバック ドアを排除します。

以下の機能は、企業への安全なリモート接続を提供して守ります。

アイコン	機能	説明
	アイデンティティ	コンテキストに基づくデバイスとユーザの識別：時刻、場所、ポスチャなどのコンテキスト項目を含む、既知のユーザとデバイスへの接続を制限します。
	VPN	安全なリモート アクセス VPN：ロールとポリシーに基づいて、リモートのオペレータ、ベンダー、およびプロバイダーに暗号化された安全なアクセスを提供します。
	マルウェア対策	クライアントとネットワークのセキュリティ：脅威が広がって脆弱な IoT システムに感染する前に、短時間でファイルのマルウェアやウイルスを調べて隔離を行い、すべての脅威を排除します。

つ目次に戻る

サービス

IoT は技術的進歩を実現していますが、最も重要なのは人的要因です。人々を支援するためにこのようなテクノロジーは開発されており、IoT 環境を保護することが求められています。IoT の保護が非常に困難なタスクであるのは確かですが、適切なプランニングとガイダンスにより、効果的な IoT セキュリティ プログラムを確立できる可能性は大幅に高まります。

前述の機能はどれも安全なネットワークの構築に役立ちます。これらを導入するにあたっては、環境を十分に評価する必要があります。以下のサービスの多くは、不可能ではないにしても、企業が独自に作り出すのは容易ではありません。

- セキュリティ ネットワーク侵入評価
- 自動化および制御システム リスク評価
- プライバシー影響評価
- ファイアウォールおよび Stealthwatch 導入
- セキュリティ セグメンテーション サービス
- ISE 設計および POC
- ソリューションサポート
- インシデント対応サービス

セキュリティ ネットワーク侵入評価や自動化および制御システム リスク評価などのサービスは、現状を把握するのに役立ちます。プロジェクトの早い段階で導入サービスとインシデント対応サービスを利用すれば、投資から最高の成果を得ることができます。

シスコ サービスの詳細については、以下を参照してください。

https://www.cisco.com/c/en/us/services/overview.html

シスコのパートナー エコシステムの活用方法については、以下を参照してください。

https://www.cisco.com/c/ja_jp/solutions/partner-ecosystem.html

シスコが提供する IoT 向けソリューションの最新情報については、以下を参照してください。

https://www.cisco.com/c/ja_jp/solutions/internet-of-things/overview.html

つ目次に戻る

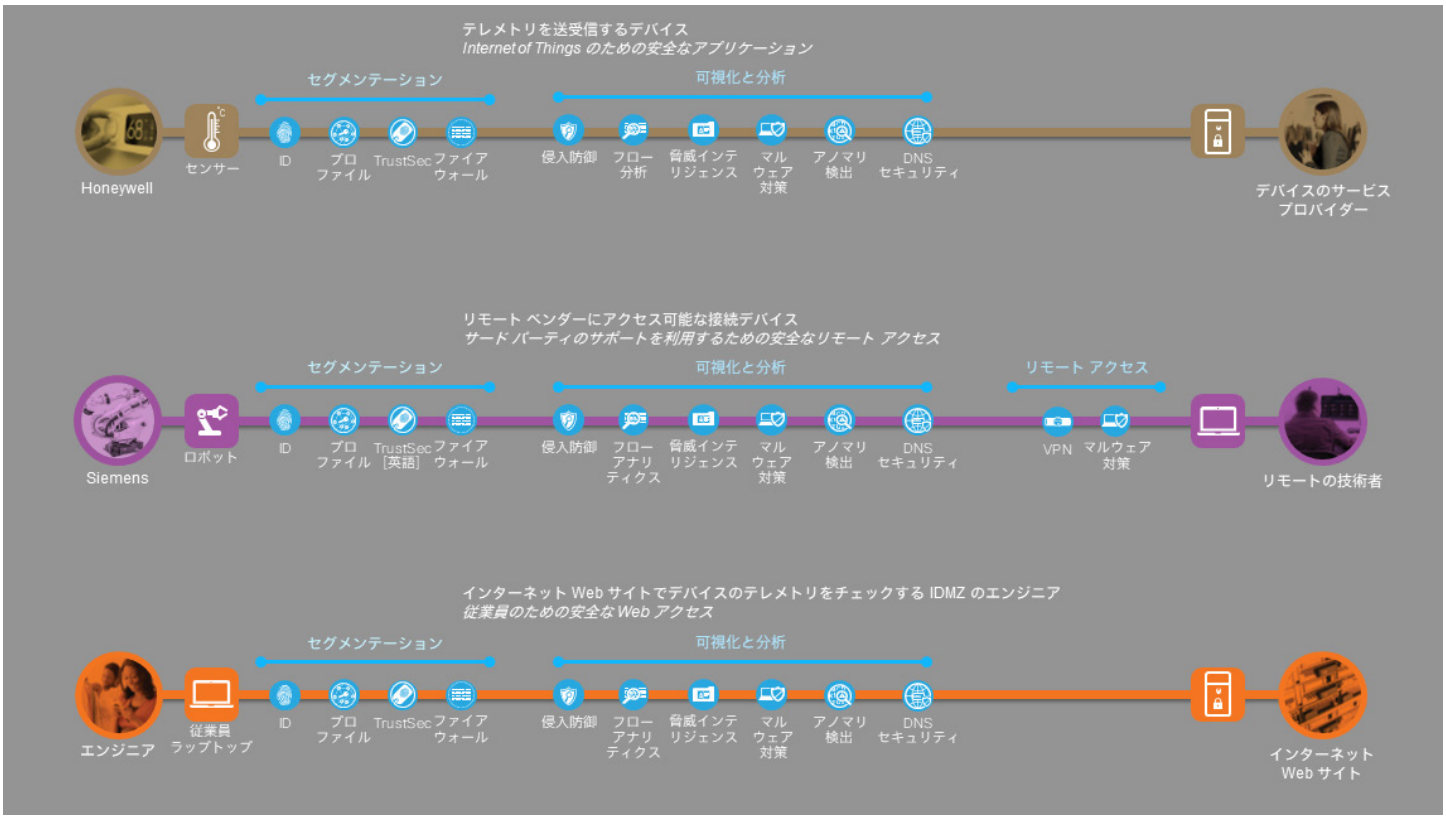
13

ソリューション アーキテクチャ

多層防御アーキテクチャ開発の最初の一歩は、脅威を阻止できるすべての機能を利用し、一般的な業界環境で使用される実際のビジネス機能/フローに対応付けることです。

図 5 に、前述のセクションで定義した 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主な機能を示します。

図 5：SAFE のビジネス フローと機能



各機能は、セグメンテーション、可視性と分析、およびリモート アクセスという重点領域で分類されます。これらの機能は、製品を通じて実装されます。次のセクションでは、各領域とそれぞれの機能に対応する製品について簡単に説明します。

つ目次に戻る

セグメンテーション

セキュリティでは、一般的に可視性することから着手します。ただし、導入済みの管理されている IoT システムについては、最初にセグメンテーションを行います。セグメンテーションとは、ネットワーク上で使用しているものを既知のリスクや未知のリスクから守る安全な場所を作るということです。このような場所を作れば可視性が向上し、IoT デバイスを特定して保護することが可能になります。セグメンテーションを行うと、デバイスが攻撃者の手が届かない場所に置かれるため、それらのデバイスが侵害された場合でも、ネットワーク内を移動するピボット ポイントとして利用されることがなくなります。

米国国土安全保障省、国家安全保障局、国際的な防衛機関、および主要なネットワーク関連の出版物やネットワーク アナリストは、ネットワークのセグメンテーションによって侵害の範囲を制限し、ネットワーク内で攻撃者が移動できる領域を狭めることを推奨しています。これらのセグメントは、デバイスがトラフィックを送受信できる制御ポイントとなり、セグメンテーションによって可視性に重点が置かれるようになります。Cisco TrustSec と Identity Services Engine（ISE）およびシスコの次世代ファイアウォールは、ノースサウスとイーストウェストのネットワーク セグメンテーションにより、ネットワーク最新化プロジェクトの安全性とセキュリティを確保します。

機能		ソリューション コンポーネント
	アイデンティティ	Cisco Identity Services Engine、エンタープライズ ディレクトリ サービス
	プロファイル	Cisco Identity Services Engine
	TrustSec	Cisco Identity Services Engine、ネットワーク スイッチ、ファイアウォール、およびルータ
	ファイアウォール	Cisco ASA および Cisco Firepower Next-Generation Firewall（NGFW）

つ目次に戻る

Cisco Identity Services Engine（ISE）と Cisco TrustSec によるセグメンテーション

ISE は、ネットワーク全体の IoT デバイスとユーザを対象とする、アイデンティティ ベースのアクセス制御、追加コンテキスト、および可視性（ユーザ、デバイス、場所、時間など）を提供します。ISE は、TrustSec ベースのソフトウェア セグメンテーション ポリシーのコントローラとオーケストレータでもあります。TrustSec テクノロジーを活用すれば、既存のスイッチ、ルータ、およびファイアウォールを利用し、ネットワーク セグメンテーションによるリソースへのアクセスを制御できます。これらのロールベースのアクセス制御ポリシーにより、VLAN の複雑性、スイッチのマニュアル設定を必要とせず、動的にネットワークをセグメント化することが可能になります。

TrustSec は、同じスイッチ上、セル内、またはセル間の IoT デバイスの間でスイッチ レベルのセキュリティを実装するのに理想的なテクノロジーであり、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。Cisco TrustSec は ISE により一元的に管理され、IoT 環境のためにスケールすることができます。また、デバイスのロールに基づいた論理的な Security Group を作成することにより、トポロジに依存しない真のセグメンテーション アーキテクチャを実現します。この設計では、これまでと同じように VLAN（レガシー インフラストラクチャ）、ポートベースのアクセス コントロール リスト、および Security Group Tag（SGT）により、セキュリティ制御を行います。

これらの TrustSec ポリシーは、異なるロケーションにある 2 つのネットワーク リソース（デバイス）間でやり取りされる特定のトラフィックに適用できます。ISE で定義される TrustSec ポリシー マトリックスにより、セキュリティ管理者は単一のウィンドウで組織全体のポリシーを簡単に確認できます。

TrustSec ポリシーを使用すれば、ネットワーク トポロジに関係なく感染したデバイスを隔離し、他の機密性の高い領域へのアクセスをブロックすることが可能です。

つ目次に戻る

Cisco Firepower Next-Generation Firewall（NGFW）によるセグメンテーション

Firepower は、統合された管理機能を備えた、脅威重視型の次世代ファイアウォールです。ネットワークからデバイスに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実現します。これらの各機能は、IoT の脅威に対する防御の追加レイヤーを提供します。また、運用業務を妨げることなく IT と OT のセキュリティ可視性を統合するアンカー ポイントも提供します。

図 6 に、IoT 環境のファイアウォールの機能を示します。ここでは、ラボおよび利用例向けの 2 つの重要な機能であるセグメンテーションとアプリケーション制御について詳しく説明します。

図 6：IoT の機能と NGFW

SCADA ネットワークにおける IoT のセグメンテーションに関する Tips

1. 基本ルール セットは、「DENY ALL, PERMIT NONE」にすべきです。
2. ゾーン環境と外部ネットワーク間のポートとサービスを有効にし、ケースごとに権限を付与すべきです。各々の受信または送信データフローの許可については、リスク分析および責任者の元に、ビジネス上の正当性評価を文書化する必要があります。
3. すべての「Permit」ルールは、IP アドレスと TCP/UDP ポートによる特定のルールであるべきです。
4. すべてのルールは特定の IP アドレス、アドレス範囲でトラフィックを制限することがあります。
5. ゾーンのすべてのトラフィックは、一般的にルーティング可能な IP プロトコル（TCP/IP または UDP/IP）に基づきます。そのため、IP 以外のプロトコルはすべてドロップするべきです。
6. SCADA ネットワークからエンタープライズ ネットワークへの直接通信を防ぎます。すべてのトラフィックを DMZ で終端させるべきです。
7. セルからエンタープライズ ネットワークへのアウトバウンド トラフィックはすべて、ファイアウォール ルールを経由してサービスとポートで送信元と宛先を制限するべきです。
8. セル デバイスに正しい IP アドレスが割り当てられている場合にのみ、DMZ からのアウトバウンド パケットを許可します。

セル ゾーンのデバイスからインターネットへのアクセスは許可すべきではありません。

つ目次に戻る

可視性と分析

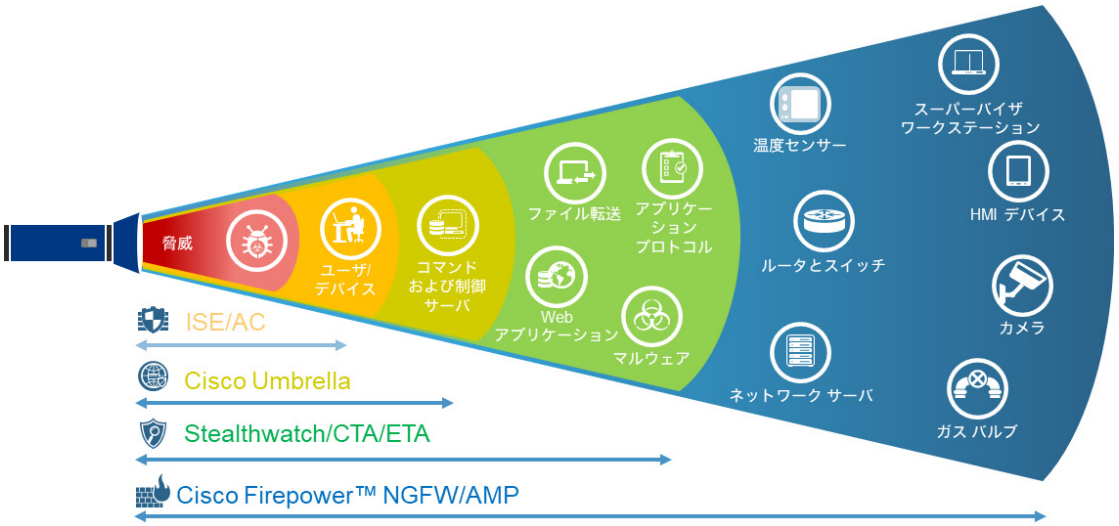
見えないものを守ることはできません。ネットワークと接続デバイスにわたる可視性は、いくつかの方法によって実現されます。企業や工場の製造現場では、各機能を使用することで可視性が向上し、幅広いコンテキストが提供されます。これらの機能は、攻撃前、攻撃中、および攻撃後のフェーズにて、組織全体への可視性とセキュリティ インテリジェンスを提供します。絶えずネットワークを監視し、リアルタイムでの異常検出およびインシデント レスポンスのフォレンジック機能を提供します。

機能		ソリューション コンポーネント
	アイデンティティ	Cisco Identity Services Engine、エンタープライズ ディレクトリ サービス、Cisco AnyConnect、Cisco Industrial Network Director
	DNS 可視性	Cisco Umbrella Secure Internet Gateway
	侵入防御	Cisco ASA および Cisco Firepower Next-Generation Firewall（NGFW）
	ネットワーク モニタリング	Cisco Stealthwatch、ネットワーク スイッチ、ファイアウォール、NetFlow を送信するルータ
	分析および異常検出	Cisco Stealthwatch with Cognitive Threat Analytics（CTA）、Cisco Firepower Next-Generation Firewall（NGFW）、Umbrella Investigate
	脅威 インテリジェンス	Cisco Talos

つ目次に戻る

脅威を明らかにするために、複数のテクノロジーでさまざまなレベルの可視性を実現できます。

図 7：さまざまなレベルの可視性



ここからは、可視性のレベルを向上させるテクノロジーの各レイヤについて説明します。

ISE は、誰（ユーザとシステムのアイデンティティ）と何（IoT デバイスなどのデバイスのタイプ）がネットワークに接続しているのか、拡張された可視化を提供します。特定のセキュリティ ポリシーに従って、ユーザやデバイスのロール、時刻、ポスチャ、場所といったコンテキスト エレメントを作成します。これらの各コンテキストは、TrustSec で使用するロールベースのアクセス制御の定義と適用に利用されます。

Umbrella は、インターネット接続時にクライアントレスでセキュリティを確保し、IoT デバイスが通信しているサービスを可視化します。IoT デバイスからの DNS リクエストにより、最小限の設定とともに、適切に管理されていないことが多い IoT デバイスの認可済みの通信と非認可のコミュニケーションを詳細に把握できます。Umbrella の高度な機能には、疑わしいドメインを明らかにする Secure Internet Gateway のプロキシ機能があります。

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 として収集したトラフィック メタデータの調査と分析を行い、組織と組織内ユーザの正常な IoT 通信のベースラインを作成します。このベースラインにより、感染やネットワークに侵入を試みる洗練された攻撃者の特定がはるかに容易になります。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。North - South（インターネットとサーバ間のトラフィック）および East - West（データセンター内のサーバ間のトラフィック）の状況を監視して非常に広範な攻撃を検出します。また、ISE との統合を活用して攻撃者を隔離できます。Cognitive Threat Analytics を追加することにより、インターネットコミュニケーションはさらに既知の、または新規に認識されたアウトブレイクを分析します。

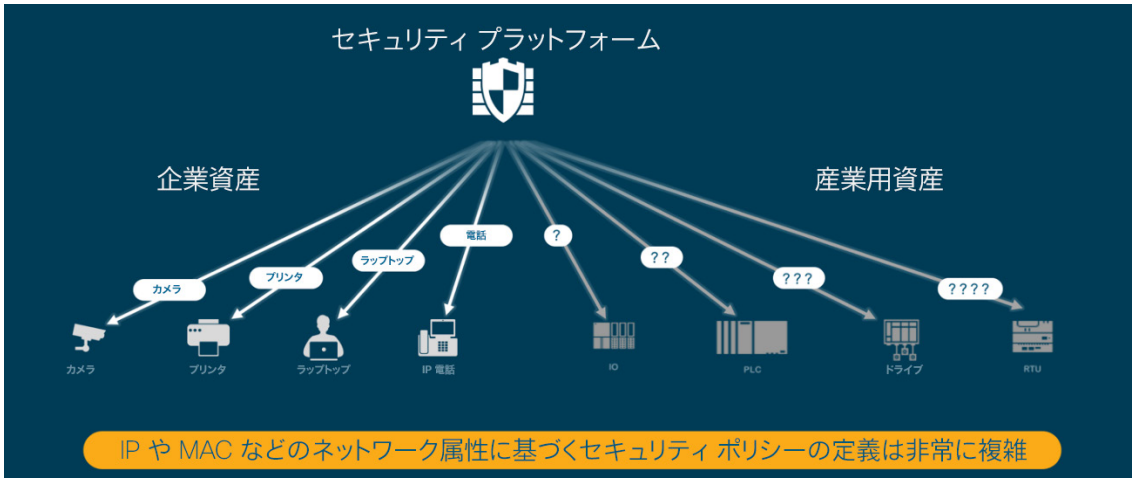
セグメンテーション機能に加え、Firepower と次世代侵入防御システム（IPS）は、ディープ パケット プロトコルとペイロード インスペクションを実行することによって最高レベルの可視性を提供します。作業者の運用業務を妨げることなく IT と OT のセキュリティを統合するアンカー ポイントを形成します。これらの統合ネットワーク ディスカバリ機能を活用すれば、産業ゾーンを出入りするすべてを可視化し、きめ細かいセキュリティ ポリシーを作成して適用できます。さらに Cisco Firepower Next-Generation Firewall（NGFW）は、最新で高度な形式のマルウェアを検出すると同時に、エンドポイント アプリケーションとオペレーティング システム、OT デバイス、およびブラウザなどのクライアント アプリケーションを独自に識別し、監視します。

このような高度な可視化の手段により、脅威検出を強化するとともに、ネットワーク環境全体（工場、モバイル、リモート サイト）に合わせてポリシーをきめ細かく制御することが可能になります。

OT のセキュリティの課題

産業環境の課題は、大部分の OT のエンドポイントに、IT のエンドポイントが 802.1x サプリカントなどの手段を使用して行うのと同じ方法でネットワーク インフラストラクチャやセキュリティ プラットフォームにアイデンティティを伝達できる機能がない点にあります。

図 8：IoT デバイスと IT デバイスのアイデンティティの課題



ISE のような IT セキュリティ プラットフォームが一貫した方法でセキュリティ ポリシーを適用するのに必要なコンテキスト情報を受け取ることができなければ、OT のネットワークの通信が中断し、OT のプロセスで障害が発生する可能性があります。

Industrial Network Director は、産業ネットワークの管理に特化したプラットフォームであり、アイデンティティとコンテキストを Cisco ISE に結び付けます。運用チームが自動化プロセスに関してネットワークとオートメーション デバイスを詳細に把握できるように設計されており、システムの可用性とパフォーマンスを向上させることで総合設備効率（OEE）を高めます。

図 9：Cisco Industrial Network Director

つ目次に戻る

安全なリモート アクセス

接続数を増やすと、ほぼ間違いなくデメリットを超えるメリットが得られるため、産業用機器や医療機器といった多くの機器のベンダーが、サポート契約にリモート サポートを含めようとするのは当然です。技術者を現場に派遣する必要がなければ、ベンダーはリモート サポートによって運用コストを削減できます。また、技術者が顧客との電話を続けながら作業を開始できるため、顧客のダウンタイムも短縮されます。

機能		ソリューション コンポーネント
	アイデンティティ	Cisco Identity Services Engine、エンタープライズ ディレクトリ サービス
	VPN	Cisco AnyConnect、Cisco ASA および Cisco Firepower Next-Generation Firewall（NGFW）
	マルウェア対策	エンドポイント向け Cisco AMP（Advanced Malware Protection）、ネットワーク向け Cisco AMP（Advanced Malware Protection）

１人の若手従業員と数人の熟練従業員しかいない場合、特に古いシステムやインフラストラクチャに対しては、適切な場所とタイミングで適切なリソースを提供するのは難しく、多くの場合にそうしたリソースを提供できません。企業では、状況に応じてリアルタイムで連携できる、さまざまな分野の多数の専門家が必要になる場合があります。また、そのような専門家が同じ場所に集まるのを待っている間に発生する費用を回避しなければならないこともあります。

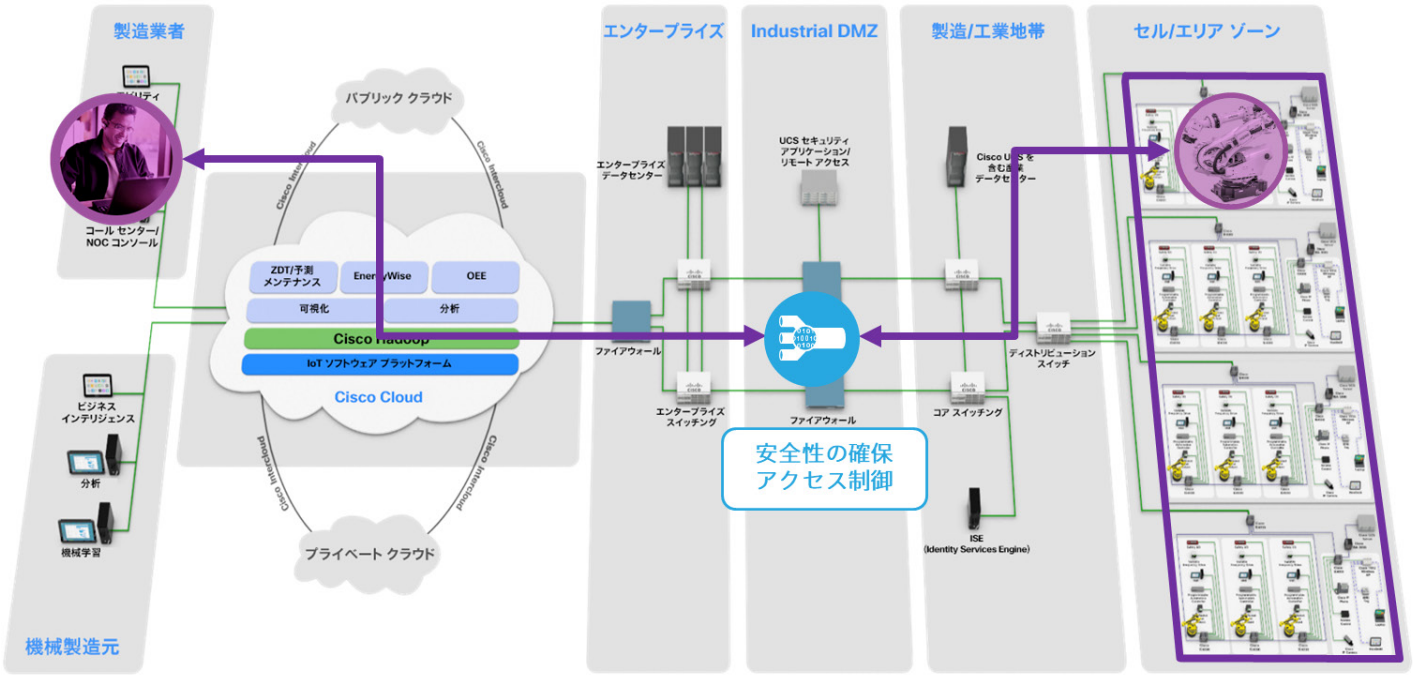
顧客にとってのデメリットには、以下のようなものがあります。

1. リモート アクセスを行うというのは、産業用制御ネットワークなどの機密性の高いネットワークにインターネットからアクセスできることを意味します。
2. 顧客が複数のベンダーの機器を利用していれば、それぞれのベンダーにアクセスを許可する必要があります。
3. 顧客は多くの場合、顧客の環境内で実際に通信しているデバイスを把握しておらず、さらには、ベンダーのネットワークが顧客のネットワークにセキュリティ上の脅威をもたらすかどうかさえ把握していません。

つ目次に戻る

IoT Threat Defense は、リモート側からネットワークへの安全な通信を実現し、セグメンテーション、可視性、および分析を導入することによって、リモート ユーザが脅威を取り込むことなく、許可されたシステムだけにアクセスできるようにします。

図 10：IoT Threat Defense が実現する安全な通信

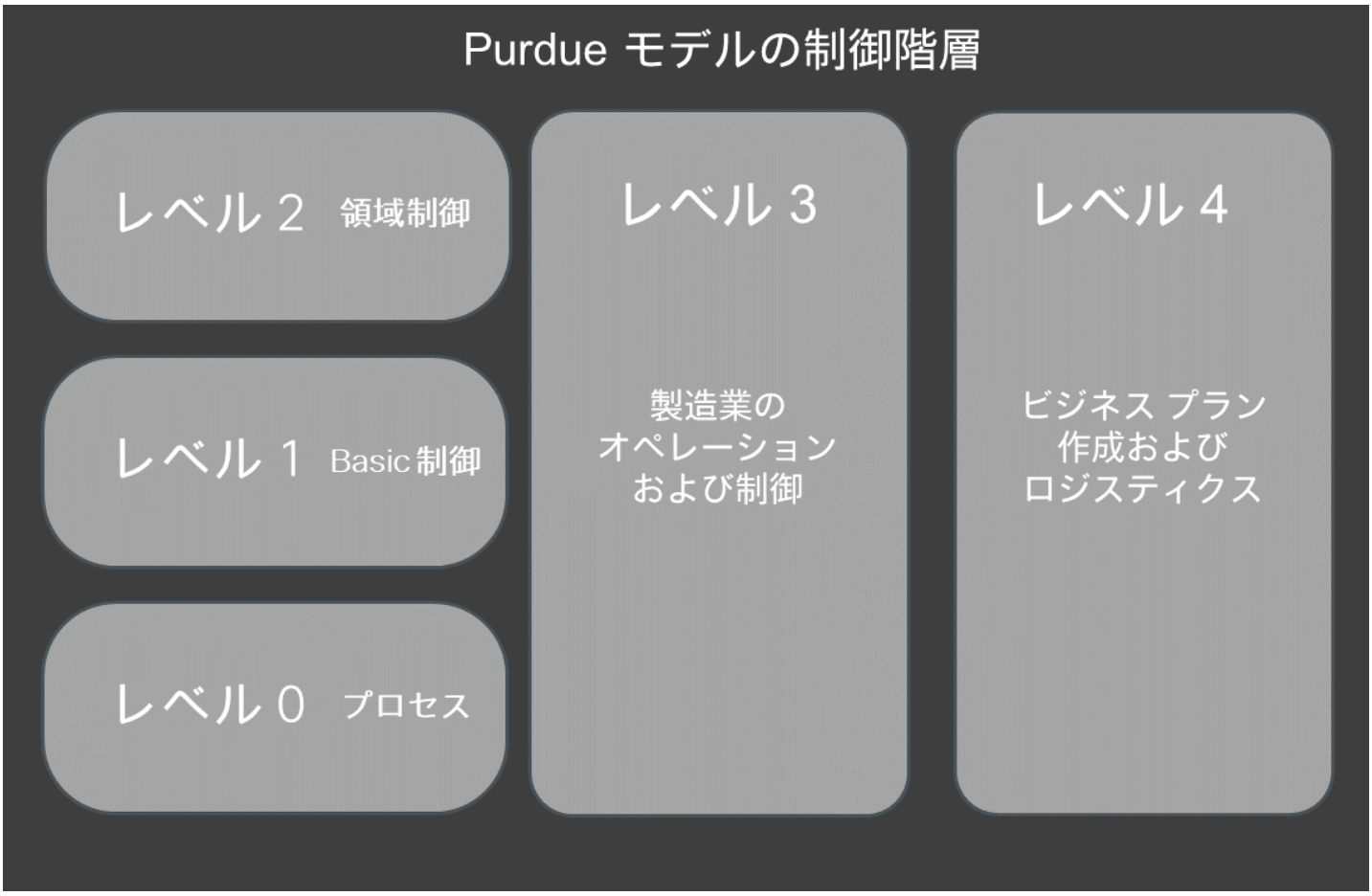


つ目次に戻る

制御階層の Purdue モデル

製造業の OT スタッフは、既存のインフラストラクチャを今日の IT システムに接続する必要があることを認識していました。このような IT と OT の統合は、IoT アーキテクチャの導入を進める大部分の業界が直面している一般的な課題であり、統合を行うには、OT と IT の両方に相互アクセスとシステム間の情報交換が可能な通信インターフェイスが必要です。このような複雑なシステムにおけるこれらのコンポーネント相互運用には、コンポーネントがプロセスで実行する機能に依存する、コンポーネント間の通信のフローを定義するフレームワークが必要です。現在多くの業界で使用されている有名なフレームワークは、図 11 に示す制御階層の Purdue モデルです。

図 11：制御階層の Purdue モデル



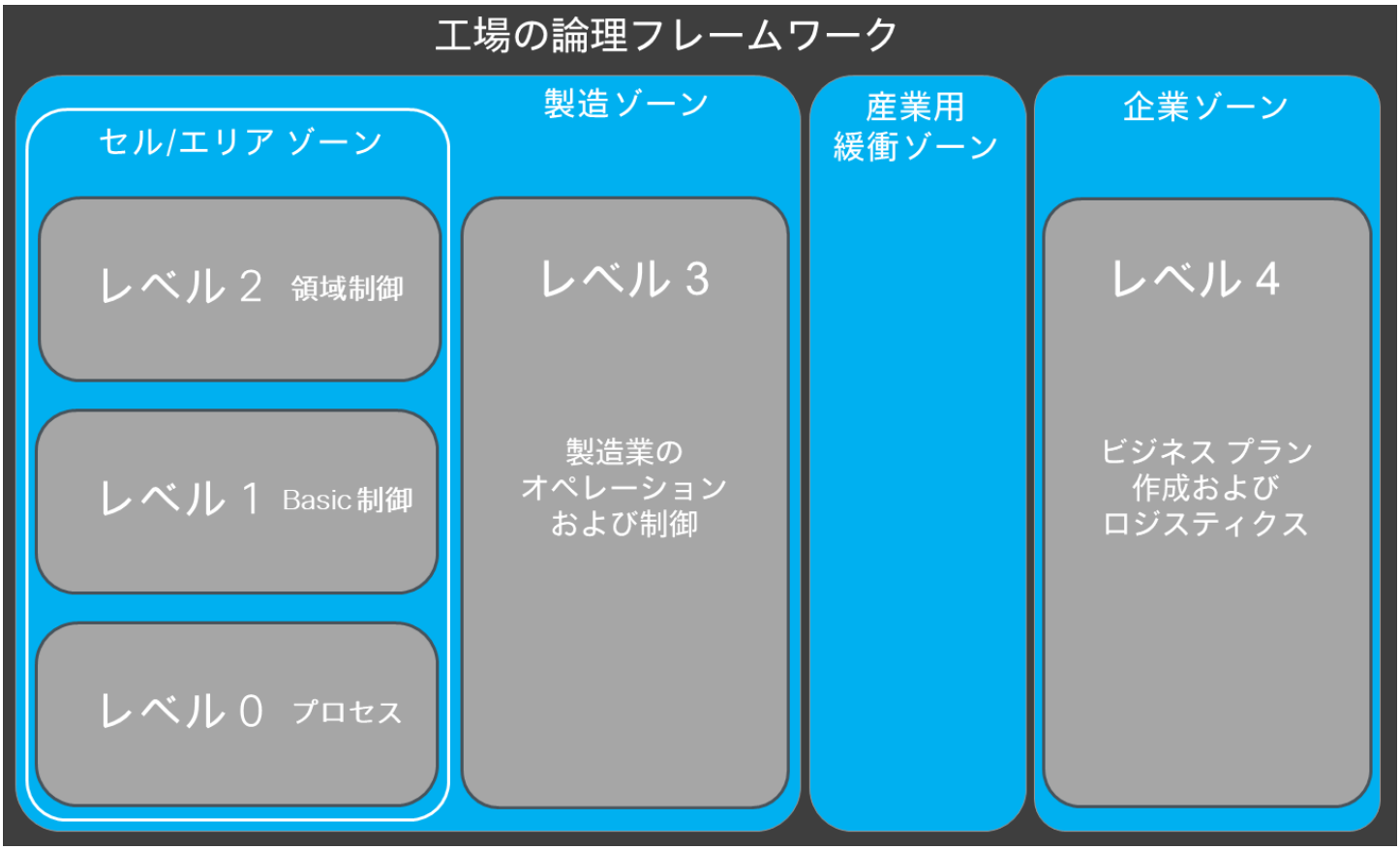
制御階層の Purdue モデル [2] は、デバイスや機器を階層機能にセグメント化する、製造業界で広く知られた一般的なモデルです。このモデルは、業界のその他多くのモデルや標準に組み込まれてきました。

[2] 参照 ISBN 1-55617-265-6

つ目次に戻る

International Society of Automation ISA-99 Committee for Manufacturing and Control Systems Security（IACS）は、この工場テクノロジーのセグメンテーションに基づいて、工場の論理フレームワークのレベルと論理フレームワーク ゾーンを明確化しました。

図 12：工場の論理フレームワーク



IACS 論理フレームワークの運用のレベルと主要ゾーンは、Purdue モデルと ISA-99 で明確化されました。これらのレベルとゾーンに加え、シスコと Rockwell Automation 社では、Converged Plantwide Ethernet（CPwE）アーキテクチャの一部として、企業ゾーンと製造ゾーン間に緩衝ゾーン（DMZ）を設けています。また、ISA-99、NIST 800-82、国土安全保障省の INL/EXT-06-11478 といった新しい IACS のセキュリティ標準にも、多層防御戦略の一環として DMZ が含まれています。DMZ の目的は、企業ゾーンと製造ゾーン間でデータやサービスを共有できるバッファ ゾーンを提供することにあります。DMZ は、可用性の維持、セキュリティ上の脆弱性への対処、および（サーベンスオクスリー法などの）法規制義務の遵守において重要な役割を果たします。さらに、DMZ によって組織内の制御のセグメンテーション（IT 組織と製造組織など）が可能になります。このようなセグメンテーションにより、さまざまなポリシーを適用したり組み込んだりできます。たとえば、製造組織は IT 組織とは異なるセキュリティ ポリシーとサービス品質（QoS）ポリシーを適用できます。DMZ では、ポリシーと組織の制御を分けることが可能です。

これらのレベルとゾーンは、IACS ネットワーク インフラストラクチャおよびサービスの設計の中心となり、シスコが提供する CPwE のシスコ検証済みデザイン（CVD）に使用される、基本的な論理フレームを形成します。

つ目次に戻る

工場のアーキテクチャ

CPwE では、IACS と IT 両方の情報と専門知識が統合されます。Cisco Enterprise Campus は、この環境のネットワーク アーキテクチャに最適なモデルです。Enterprise Campus ソリューションのアーキテクチャには、主要なネットワークの概念とモデルである、コア、アクセス、ディストリビューション、およびサービス レイヤが組み込まれています。IACS ネットワークは本質的に特殊なキャンパス ネットワークとみなすことができます。

CPwE のシスコ検証済みデザイン（CVD）を基本とする IoT Threat Defense ソリューションは、セグメンテーション、可視性、およびリモート アクセスの要素を追加することで改良しています。SAFE Campus Reference Architecture と IoT Threat Defense のビジネス フローを使用することにより、図 13 のエンドツーエンドのアーキテクチャに IT モデルと OT モデルの両方を含め、それらのフローを保護する機能を導入する方法を簡単に示すことができます。

図 13：SAFE 形式の CPwE のリファレンス アーキテクチャとビジネス フロー

つ目次に戻る

セル/エリア ゾーン

セル/エリア ゾーンは工場施設内の機能エリアで、多くの工場には複数のセル/エリア ゾーンがあります。自動車工場ではボディショップまたは部分組立プロセスが、食品および飲料製造施設ではバッチ混合エリアがこれに該当すると考えられます。プロセス スキッドで 1 台のコントローラとそれに関連するデバイスだけが最小限で使用される場合もあれば、組立てラインで複数のコントローラが使用される場合もあります。各工場施設では、さまざまな粒度でセル/エリア ゾーンの境界が個別に定義されます。このアーキテクチャの目的上、セル/エリア ゾーンは、製造プロセスの機能面のリアルタイム制御に関わる一連のデバイスやコントローラなどのセットを指します。機能プロセスを制御するために、これらはすべて互いにリアルタイムで通信を行います。

セル ゾーンには、エンドポイントとアクセス レイヤ機能が含まれます。それぞれのセル ゾーンは、TrustSec、VLAN、またはファイアウォールを使用してセグメント化されるべきで、さらに機密性の高い工場では、TrustSec や専用のファイアウォールによりセル内でもセグメンテーションが必要になる場合があります。デバイスは、適切なポリシー/セキュリティ グループに配置されるよう、ネットワークに接続したときにプロファイリングされます。セルへの、セルからの、セル間のトラフィックの可視化は、キャプチャと監視を行い、新たな脅威や問題を迅速に特定することが重要です。

製造ゾーン

製造ゾーンは、セル/エリア ゾーン（レベル 0 ～ 2）とサイトレベル（レベル 3）のオペレーションと制御で構成されます。製造現場の作業の監視と制御に欠かせないすべてのアプリケーション、デバイス、およびコントローラが製造ゾーンにあるため、このゾーンは重要です。工場でのスムーズな作業とアプリケーションやネットワークの機能を維持するため、このゾーンでは、レベル 4 と 5 の工場およびエンタープライズ業務からの明確かつ論理的なセグメンテーションと保護が必要とされます。

セル ゾーンは、キャンパス ネットワークで使用されているディストリビューション レイヤへの接続およびセグメンテーション方式のベスト プラクティスに従い、製造ゾーンで集約されます。作業における通信の大部分はこのゾーンから発生するうえ、たくさんの古い脆弱なオペレーティング システムが数多く含まれているため、ここでも TrustSec によるセグメンテーションと NetFlow による可視性が同じように重要となります。

Industrial DMZ

この緩衝ゾーンは、製造ゾーンと企業ゾーン間でサービスやデータを共有できるバッファ ゾーンを提供します。さらに、DMZ では組織の制御を簡単にセグメント化できます。シスコでは、トラフィックが直接通過しないように DMZ を設計することを推奨します。すべてのトラフィックは DMZ を起点とし、DMZ で終端させる必要があります。またこのチョークポイントは、工場を出入りするすべてのトラフィックのディープ パケット インスペクションによって可視性を得るのに最適な場所を提供します。

企業ゾーン

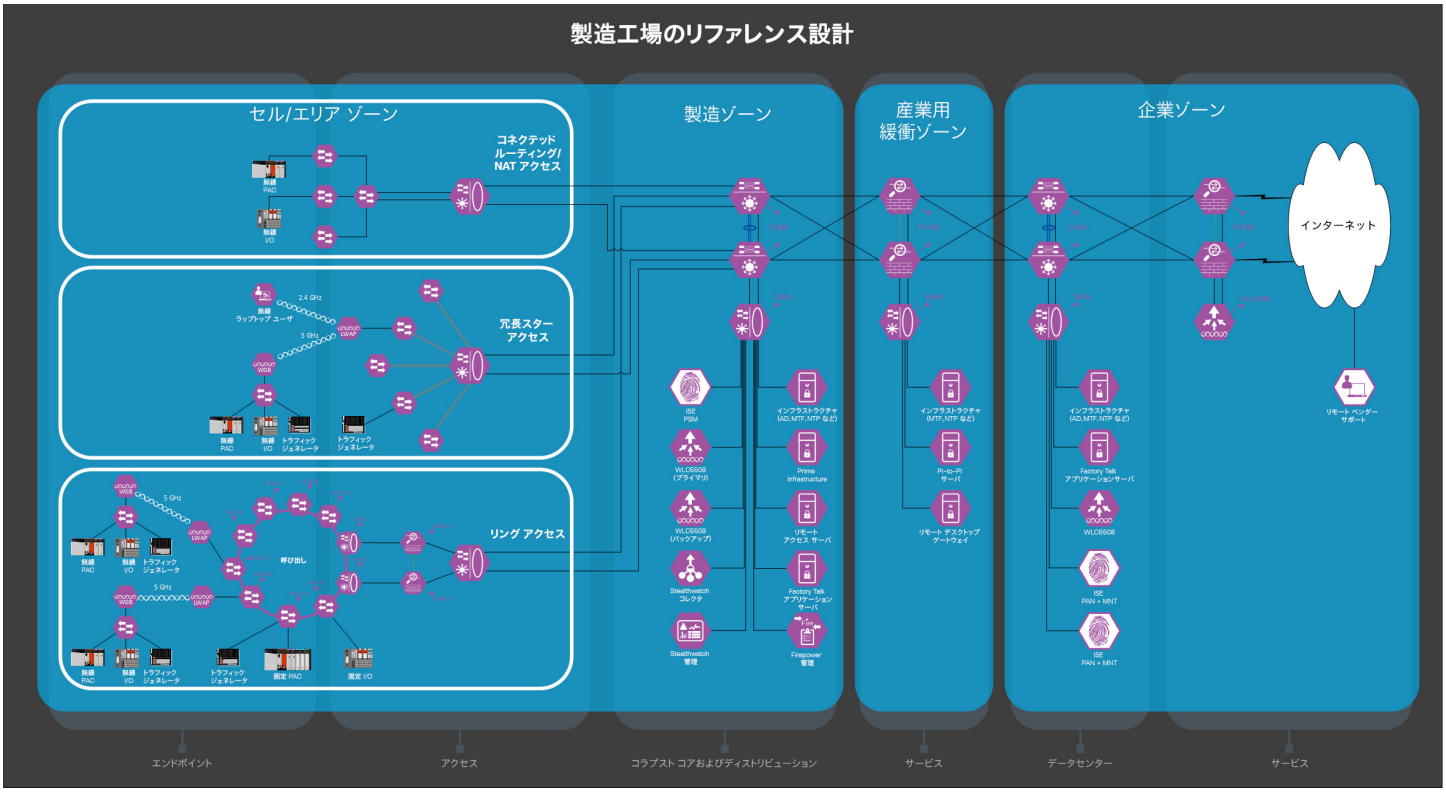
企業ゾーンは、企業ネットワークで提供されるサービスへの標準的なアクセスを必要とする機能とシステムがある場所です。このレベルは、企業ネットワークの拡張部分とみなされます。ここでは基本的なビジネス管理タスクが実行され、それらのタスクでは標準的な IT サービスが使用されます。これらの機能とシステムには、企業ネットワーク サービスへの有線および無線アクセスが含まれています。

また、企業ゾーンは集中 IT システムおよび機能が存在する場所でもあります。エンタープライズ リソース マネージメント（ERM）、Business-to-Business、および Business-to-Customer サービスは通常、このレベルに存在します。多くの場合、外部パートナーまたはゲスト アクセス システムはここに存在しますが、企業レベルでは実現するのが難しい柔軟性を得るために、下位レベル（レベル 3 など）のフレームワークに置かれることも珍しくありません。

工場の設計

各機能がどこに実装されるのかを把握すれば、アーキテクチャから設計への移行が大幅に簡素化され、機能マッピングで必要な機能を備えた適切なハードウェアを選択するだけで済みます。ここでは、高可用性、復元力、拡張性などの他の要素も考慮されます。図 14 に製造工場で使用されるリファレンス設計を示します。

図 14：製造工場のリファレンス設計



付録には、さらに詳細なラボ図（図 36 と図 37）があります。

CPwE の詳細については、以下を参照してください。

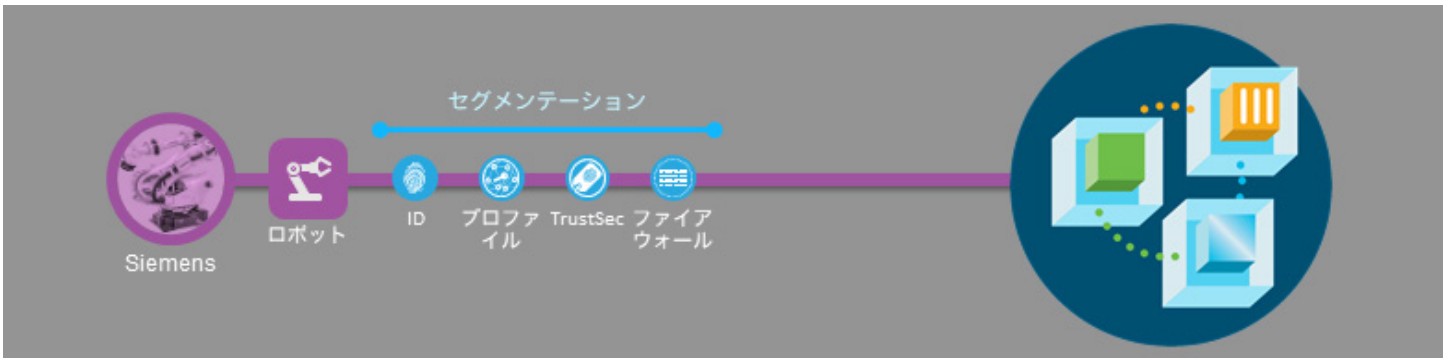
https://www.cisco.com/c/en/us/solutions/enterprise/design-zone-manufacturing/design-guide-listing.html

つ目次に戻る

導入

以下の各製品のセクションでは、企業の IoT インフラストラクチャを最大限に保護するために、通常のインストール後にどのようなカスタマイズを行ったのかを説明します。すべての製品とバージョンの一覧表は付録にあります。

このソリューションでは、全社レベルでの NTP との時刻同期が必要です。また、pxGrid 証明書には CA サーバが推奨されます。



Cisco Identity Services Engine（ISE）

企業の保護は、ユーザとデバイスがネットワーク インフラストラクチャに接続するときの認証から始まります。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。ネットワークから収集したコンテキスト情報は、ユーザ、デバイス、およびその他の対象となる要素に対する可視性を提供します。デバイスにアイデンティティをうまく結び付けるこのようなコンテキストは、ポリシー適用の条件として使用されます。

このガイドでは、IoT デバイス（および広義にはユーザ）を接続するための ISE の設定方法に重点を置いています。ISE の展開方法と別の設定については、以下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

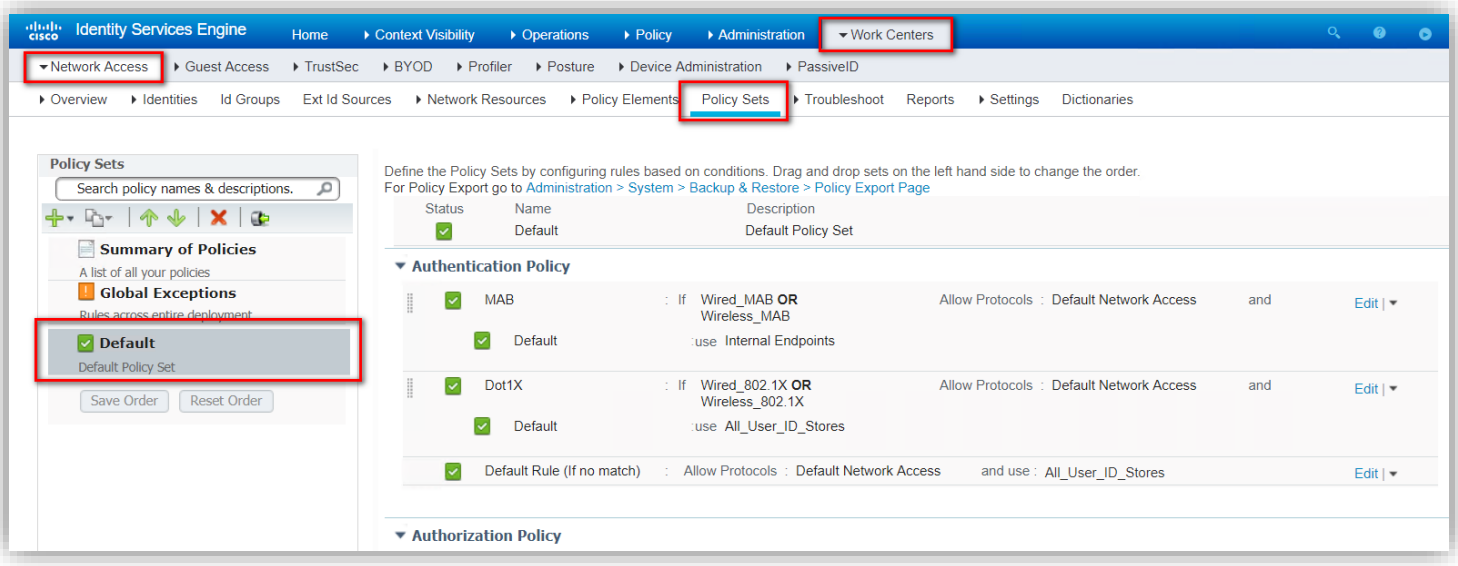
また、https://communities.cisco.com/community/technology/security/pa/ise もご覧ください。

ネットワーク AAA の設定

製造環境では、多くの制御システムで確定的なタイミングが要件となっているため、IoT デバイスの大部分は有線ネットワークで接続されています。ただし、これらのデバイスは、多くの場合に 802.1x（Dot1x）をはじめとする従来のネットワーク認証標準の実装や設定をサポートしていません。そのため、デバイスの製造元がハードウェアに割り当てた MAC アドレスを認証に利用する、MAC 認証バイパス（MAB）が使用されます。

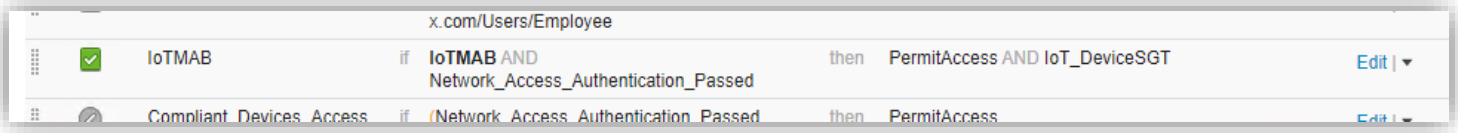
つ目次に戻る

ISE は、認証、認可、およびアカウンティング（AAA）サーバです。つまり、ユーザとデバイスがネットワークに接続するための認証と認可を行う必要があります。ISE では、MAB の認証ポリシーがデフォルトで有効になっています。これらのポリシーを表示して編集するには、[ワークセンター（Work Centers）] > [ネットワークアクセス（Network Access）] > [ポリシーセット（Policy Sets）] に移動します。以下のスクリーンショットでは、デフォルトのポリシーセットが使用されています。



デフォルトの認証ポリシーに示されているように、ISE は最初にデバイスの MAC アドレスを確認し、認証フェーズを通過させるために既知の製造元の MAC アドレスと一致させようとします。これらの内部エンドポイントは、[管理（Administration）] > [ID の管理（Identity Management）] > [グループ（Groups）] メニューで確認できます。

次のステップでは、ユーザとデバイスを認可します。以下の画面のケースでは、エンドポイントをプロファイリングしてエンドポイント グループ（IoTMAB や Siemens Device など）に追加しています。その方法については後から説明しますが、ここではデバイスが IoT デバイスであると特定され、エンドポイント グループに追加されると考えてください。認可ルールにコンテキストが条件として含まれていることを確認できます。これについては、デバイスが IoTMAB エンドポイント グループに含まれているかどうかをチェックすることで確認できますが、これはネットワーク認証が成功した際に実施可能です。エンドポイント グループに含まれている場合、そのデバイスは対応するセキュリティ グループ タグ（SGT）で分類され、個別またはグループ用の資産として、16 ビットの番号が作成されています。



新しい IoT デバイスは、次の 2 つの方法で特定できます。

1. デバイスの MAC アドレスをエンドポイント グループに手動で追加するか、CSV を使用してインポートする。
2. ISE のプロファイリング機能を使用する。

つ目次に戻る

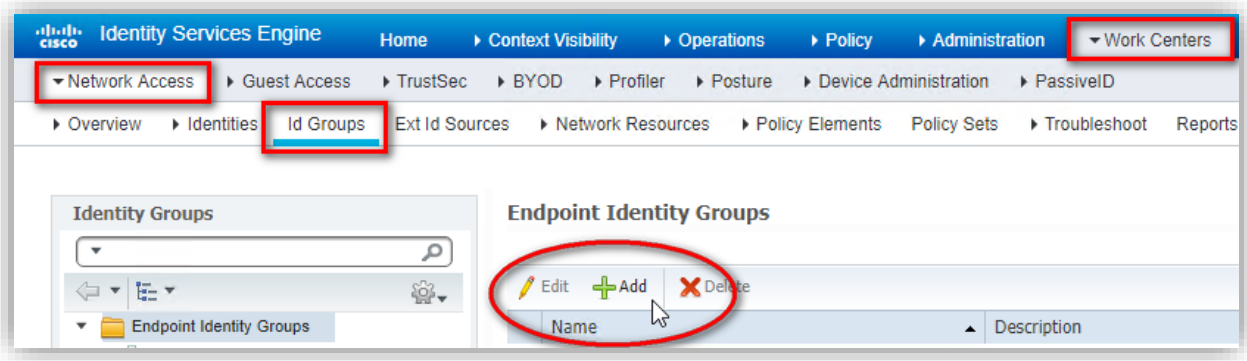
デバイスをエンドポイント グループに追加すると、デバイスは既知のデバイスになります。上記のスクリーンショットに示すように、これらのデバイスにはセキュリティ グループ タグを割り当てることができます。不明なデバイスはプロファイリングでき、ISE ではそれらのデバイスをコントローラ、カメラ、プリンタ、およびその他のデバイスとして検出することが可能です。デバイスが不明で最初に正しくプロファイリングされない場合は、それらのデバイスのネットワーク アクセスを制限する認可ポリシーを追加できます。IoTMAB の例に示されているように、プロファイリングが完了すると、デバイスがその役割に合った別のセグメントに自動的に追加され、認可を行うことができます。

注：

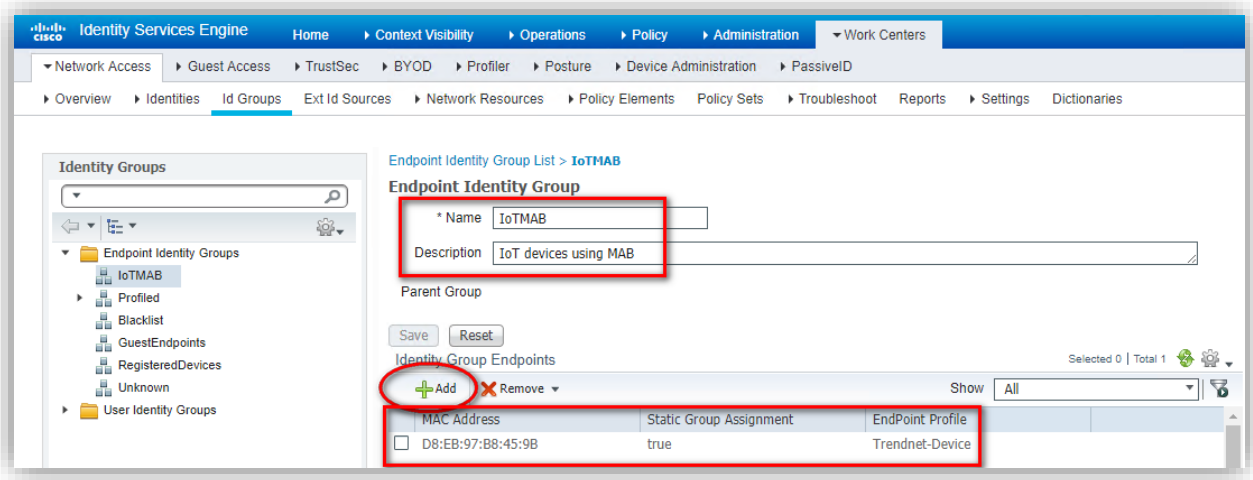
プロファイリングの詳細については、次の『*ISE プロファイリング設計ガイド*』を参照してください。https://communities.cisco.com/docs/DOC-68156

MAB を必要とする IoT デバイスについては、特定のエンドポイント アイデンティティ グループに追加された IoT デバイスのアクセスを許可する認可ポリシーを追加します。

ステップ 1：IoTMAB というエンドポイント アイデンティティ グループを作成し、必要に応じてデバイスの MAC アドレスを追加します。[ワークセンター（Work Centers）] > [ネットワークアクセス（Network Access）] > [ID グループ（Id Groups）] の順に選択し、[追加（Add）] をクリックします。



ステップ 2：グループの名前と説明を入力します。[保存（Save）] をクリックします。[追加（Add）] をクリックし、表示されているエンドポイントのリストからデバイスの MAC アドレスを選択します。



つ目次に戻る

この使用例では、MAC アドレスに基づいて新しいエンドポイント グループを作成し、認可ポリシーでそのエンドポイント グループを使用しています。このエンドポイント グループが自動的にエンドポイント プロファイル（Trendnet-Device）に関連付けられていることがわかります。

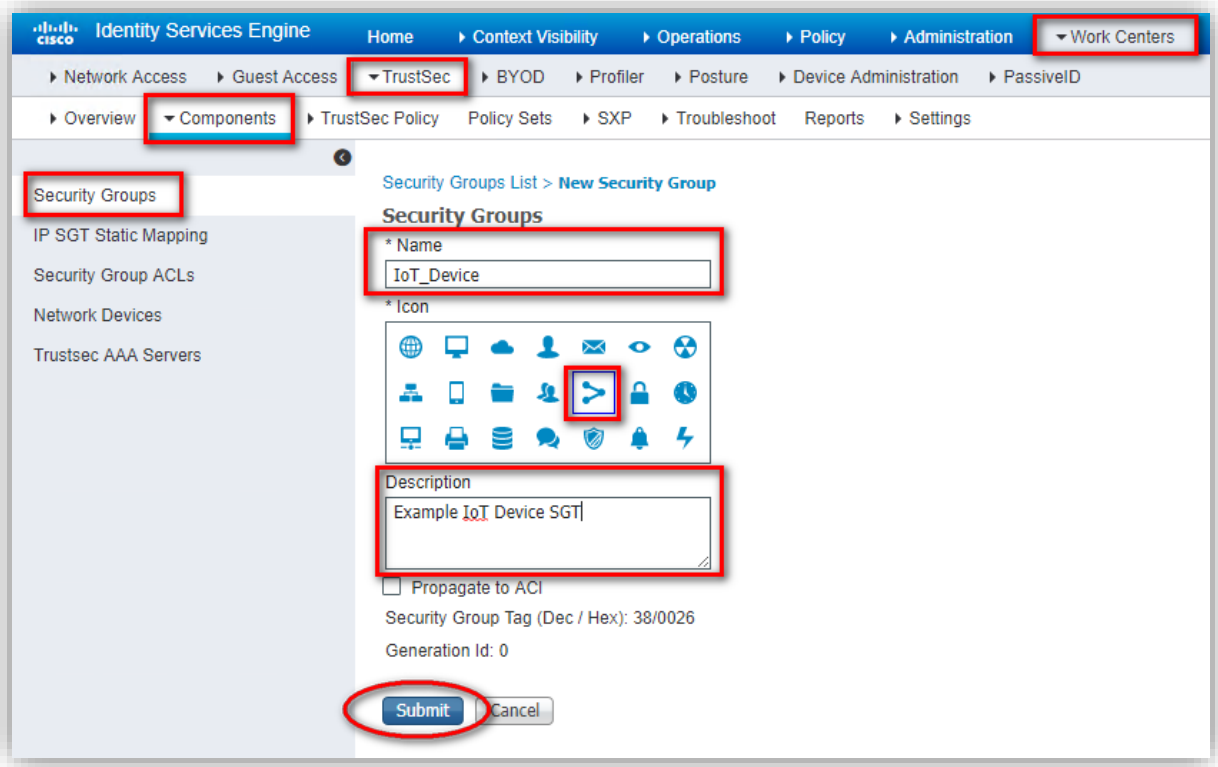
ISE では、MAC アドレスの OUI 情報を使用してプロファイルをデバイスに一致させます。また、これらの IoT デバイスから収集した情報を使用してデバイスをプロファイルに一致させます。今回のケースでは、エンドポイント グループに基づくデバイスのホワイトリストを使用しているため、デバイスを特定して認可できます。

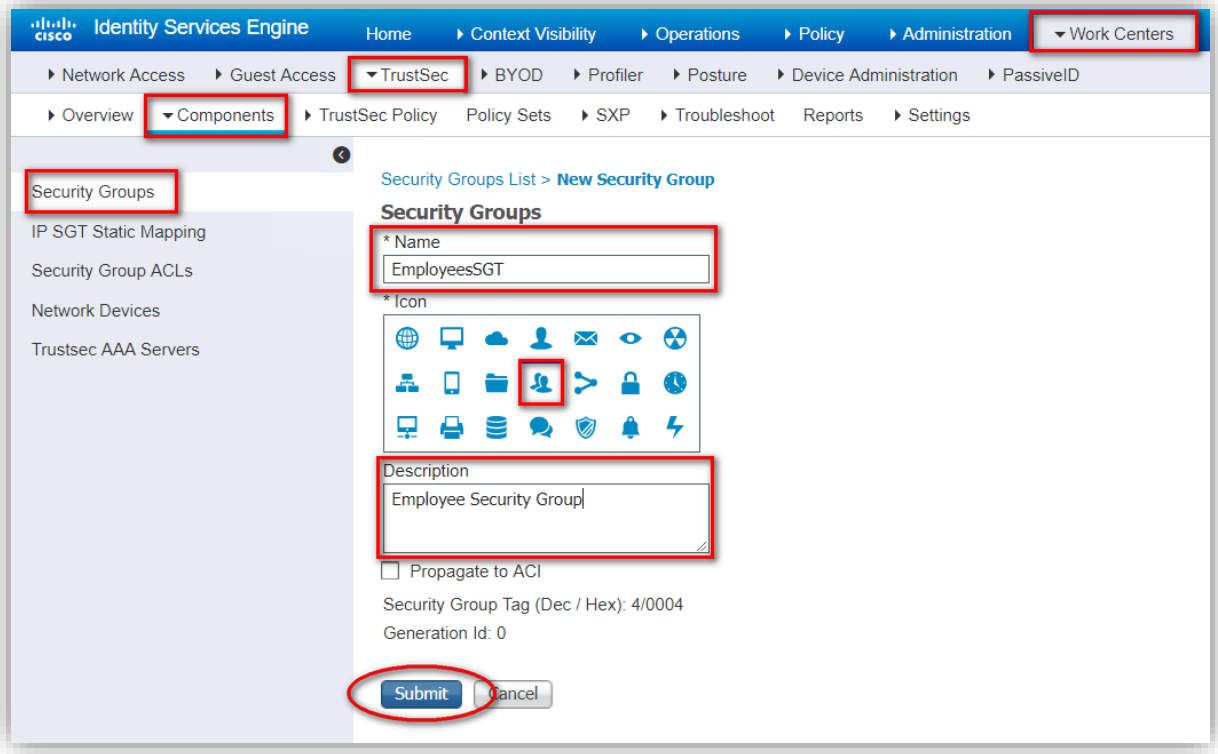
デバイスを特定する別のアプローチとしては、ISE のプロファイラ サービスを使用します。既知のデバイスのプロファイルは、Cisco Cloud からフィード経由で継続的に追加されます。この機能を使用するには、ISE でフィード サービスを有効にする必要があります。[ワークセンター（Work Centers）] > [プロファイラ（Profiler）] > [フィードサービス（Feed Service）] に移動してフィード サービスを有効にします。

プロファイラ サービスは本質的により動的であるため、デバイスの MAC アドレスをホワイトリストに登録する必要はありません。より正確に言うと、ISE はデバイスを分類して適切なエンドポイント プロファイルに追加します。これらのエンドポイント プロファイルは、ベンダーやデバイス タイプなどに基づいて分類され、それらを使用して認可ポリシーを作成するときに認可ポリシーの条件に従って公開されます。

詳細については、『ISE プロファイリング設計ガイド』（https://communities.cisco.com/docs/DOC-68156）を参照してください。

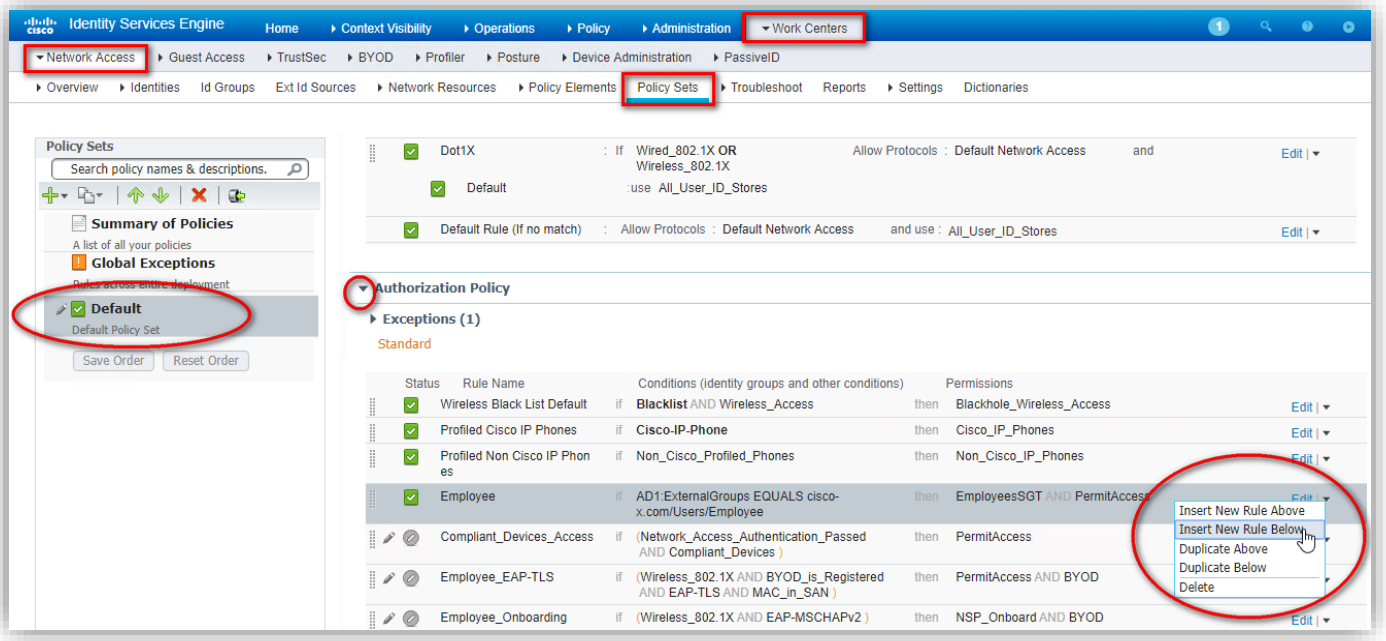
ステップ 3：IoT デバイス、ユーザ、およびシステムのセキュリティ グループを作成します。[ワークセンター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [セキュリティグループ（Security Groups）] の順に選択します。[追加（Add）] をクリックして新しいセキュリティ グループを追加します。新しいセキュリティ グループの名前、アイコン、および説明（任意）を入力します。[送信（Submit）] をクリックします。



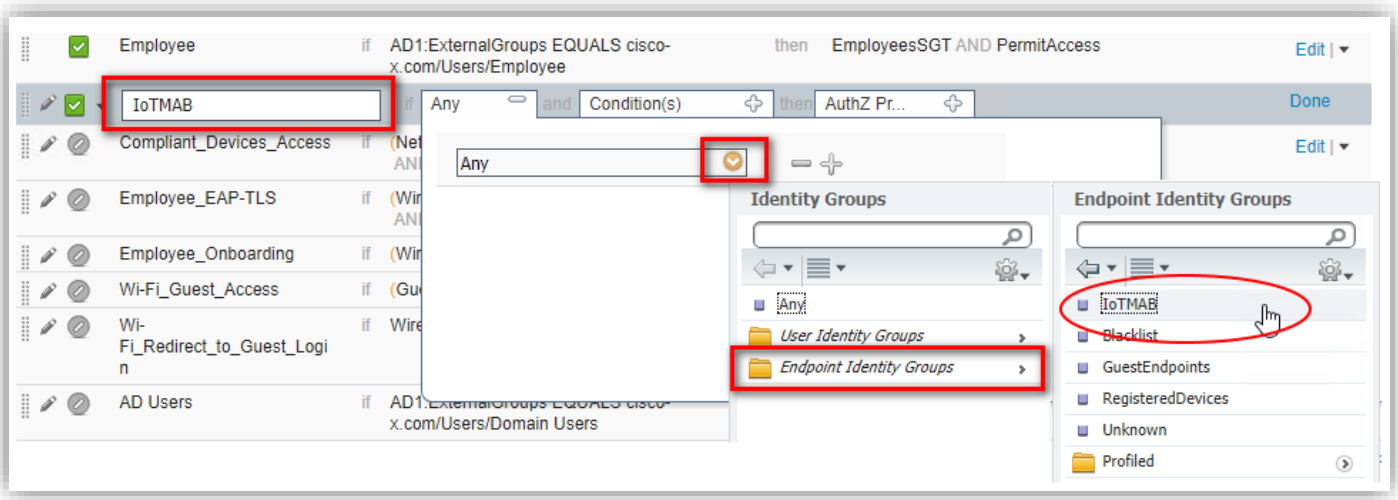


つ目次に戻る

ステップ 4：IoTMAB エンドポイント グループを一致させ、権限とセキュリティ グループ タグを割り当てる認可ルールを作成します。[ワークセンター（Work Centers）] > [ネットワークアクセス（Network Access）] > [ポリシーセット（Policy Sets）] の順に選択します。左側にあるポリシー セットの [デフォルト（Default）] を選択します。認可ポリシーを展開し、右側にある矢印をクリックして最後のアクティブ ルールの下に新しいルールを挿入します。

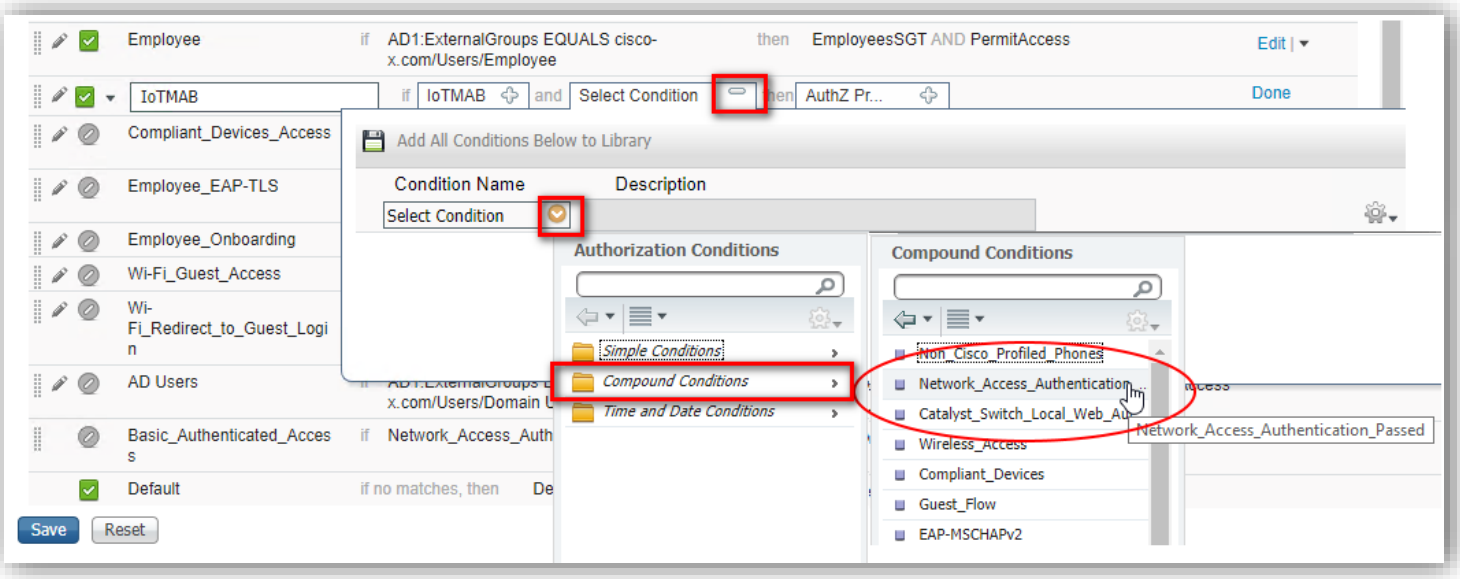


ステップ 5：ルールに名前を付けてエンドポイント アイデンティティ グループを選択します。

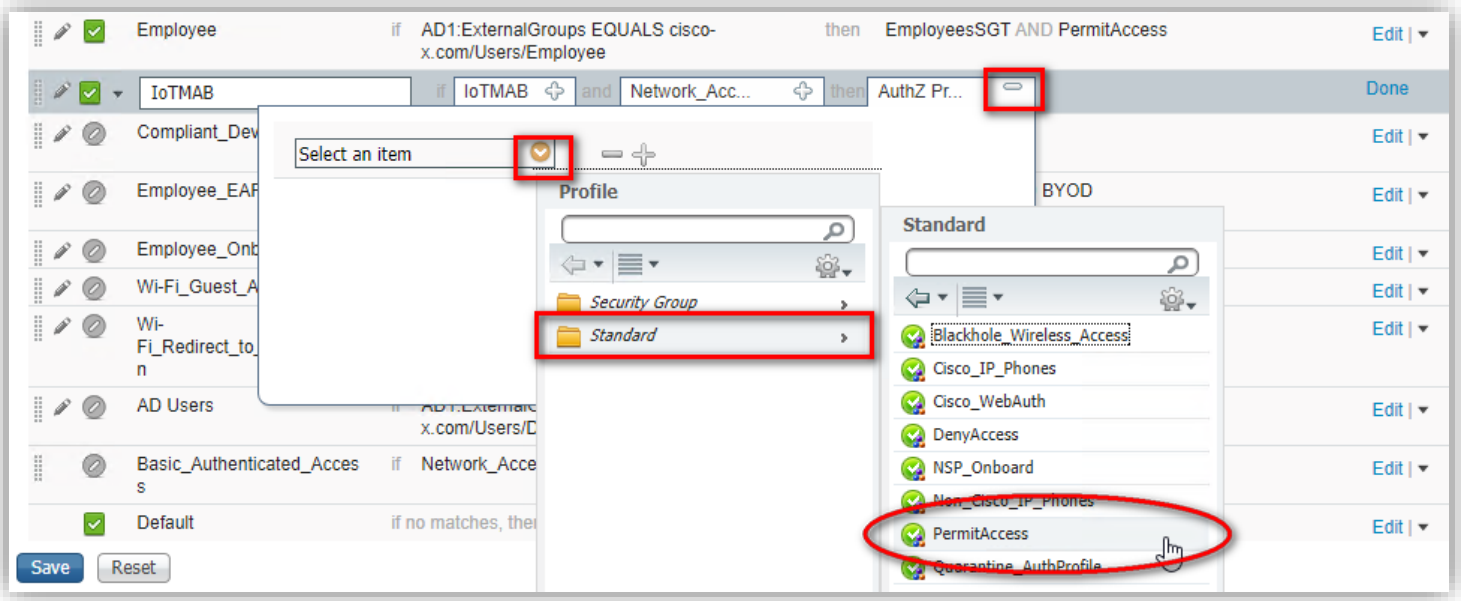


つ目次に戻る

ステップ 6：ライブラリより Compound Conditions のうち Network_Access_Authentication_Passed を選択します。

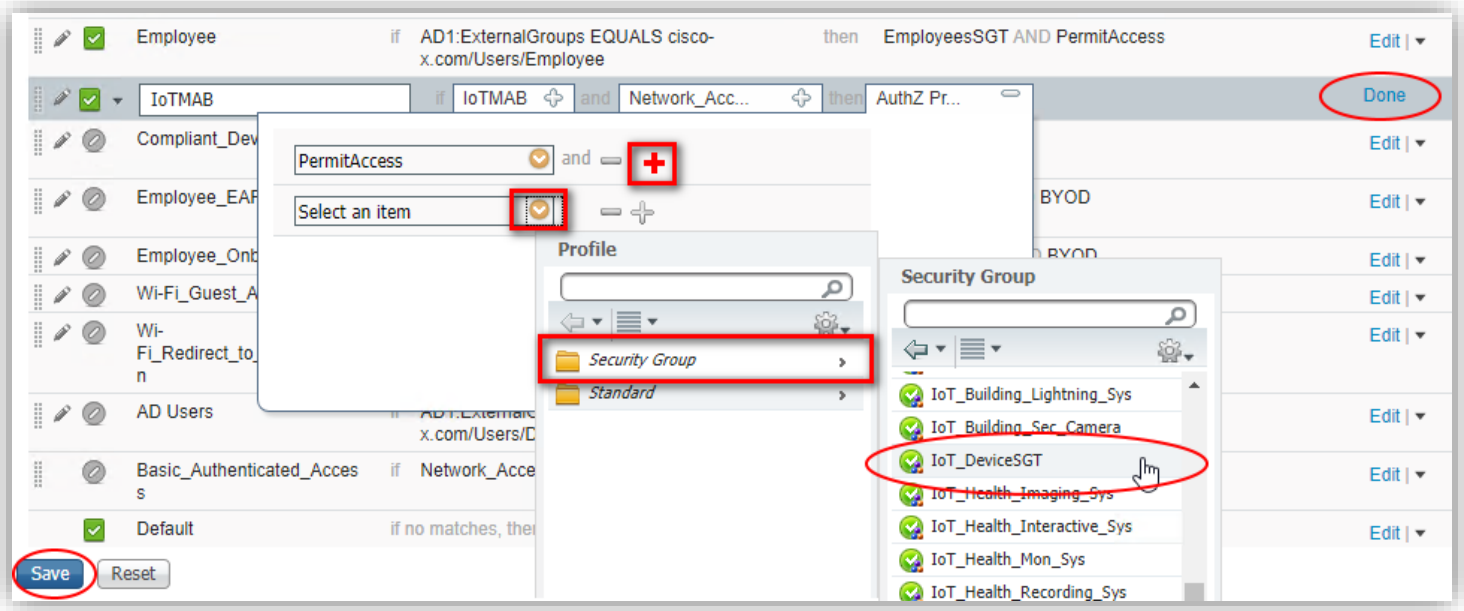


ステップ 7：標準的な権限を割り当ててアクセスを許可します。



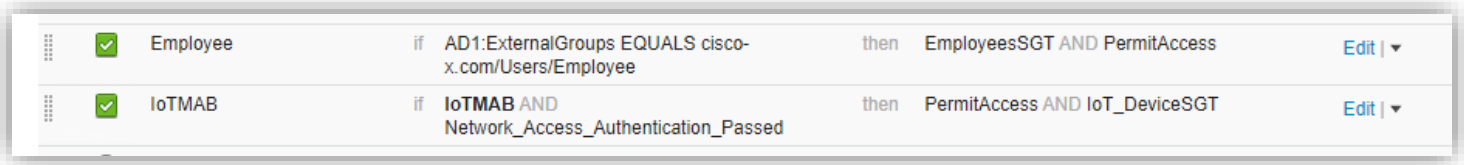
つ目次に戻る

ステップ 8：[+] をクリックし、2 つ目の権限としてセキュリティ グループ タグを割り当てます。編集を終了するには、[完了（Done）] と [保存（Save）] をクリックします。



ステップ 4 ～ 8 を繰り返し、IoT デバイスへのアクセスを必要とする、特定のユーザ アイデンティティ グループに含まれる dot1x 認証ユーザの認可ポリシーを追加します。ISE は、Active Directory、LDAP、ODBC などの内部および外部アイデンティティ ストアによるユーザの検証をサポートしています。

この例の dot1x 認証ユーザ グループは、Active Directory で検証されています。アイデンティティを指定したら、適切な SGT とアクセス ポリシーを割り当てます。

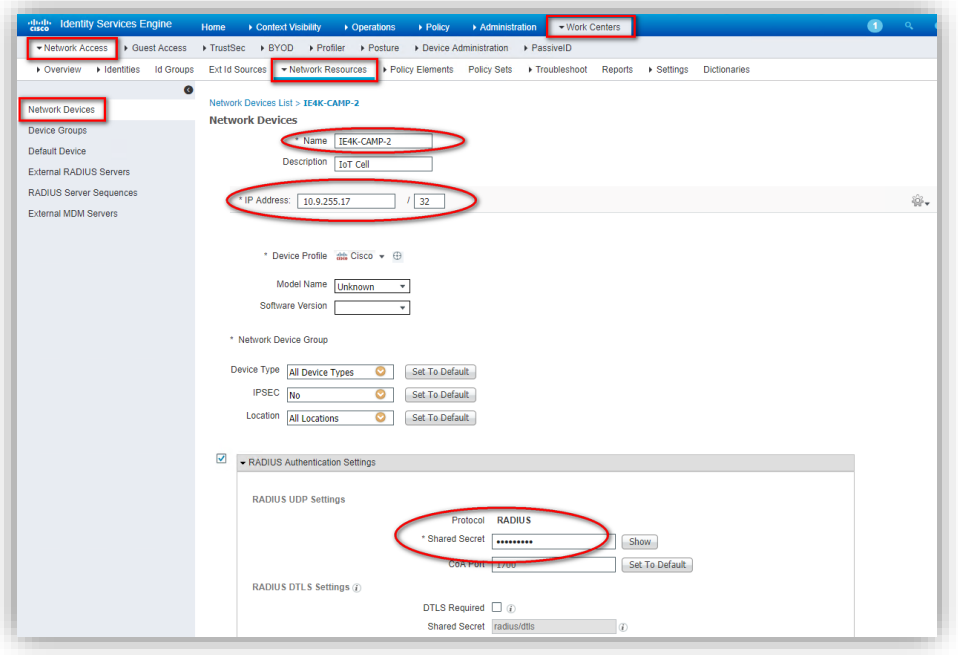


注：

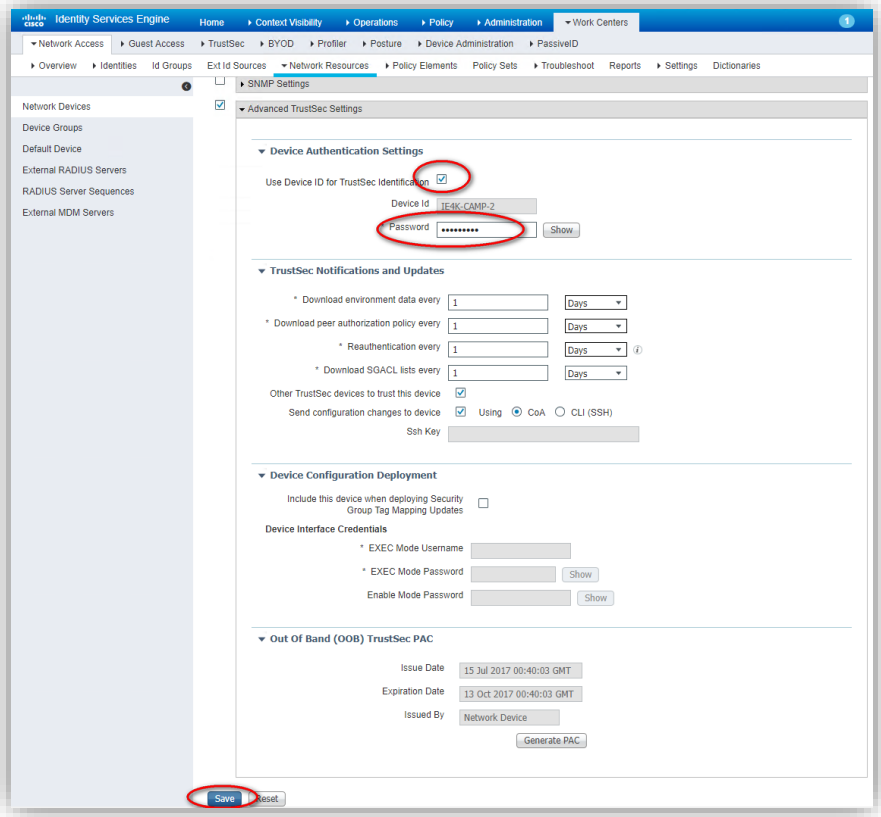
外部アイデンティティ ストアを追加して認証/認可ポリシーで使用する方法の詳細については、以下を参照してください。

https://www.cisco.com/c/en/us/td/docs/security/ise/2-2/ise_active_directory_integration/b_ISE_AD_integration_2x.html

ステップ 9：デバイスとユーザを認証するスイッチ、ファイアウォール、およびルータを ISE に追加します。[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（ネットワーク デバイスの設定で使用するパスワード）を設定します。



ステップ 10：スクロール ダウンして TrustSec デバイス ID でデバイス名を使用するように設定します。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。



つ目次に戻る

AAA スイッチの設定

各スイッチは、IoT デバイス、ユーザ、およびその他のシステムを認可する 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。

以下の設定では、同じような広範なデバイスで簡単に一貫した方法で処理が行えるよう、コマンド ライン インターフェイス（CLI）を使用します。

RADIUS 認証、許可、およびアカウンティングの設定

ステップ 1：コンフィギュレーション モードを開始します。送信元の認証要求に使用される 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。AAA をイネーブルにします。

```
ip radius source-interface Loopback0

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、認可、および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
```

つ目次に戻る

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、無効化が可能になります。

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

ステップ 7：ポートベースの認証をグローバルに有効にします。

```
dot1x system-auth-control
```

ステップ 8：デバイス トラッキングをグローバルに有効にします。これにより、RADIUS の要求にデバイスの IP アドレスを含めて TrustSec の IP-to-SGT マッピングを有効化します。

```
ip device tracking
```

ステップ 8b：新しいスイッチ ソフトウェア バージョンでは ip device tracking コマンドが廃止され、機能が device-tracking に置き換えられています。トラッキングを有効にし、後でスイッチ インターフェイスに適用されるポリシーを作成します。

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

注：

IPDT のベスト プラクティスとワークアラウンドの詳細については、以下を参照してください。
https://www.cisco.com/c/ja_jp/support/docs/ip/address-resolution-protocol-arp/118630-technote-ipdt-00.html

ステップ 8c：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
```

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。dot1x は、サプリカント ソフトウェアを使用するユーザとモバイル デバイス/ワークステーションの認証を安全に行える方法です。このソフトウェアは、デバイスから ISE へのセキュアな通信セッションを開始します。MAB は、動作中のコントローラ、カメラ、プリンタ、およびその他のレガシー IoT デバイスといった、サプリカントを実装していないデバイスで使用されます。導入に際しては多くの場合、検証のためにデバイスを切断したり、従業員やベンダーのシステムを接続したりできるのが望ましいと言えます。この機能をサポートする場合、MAB と dot1x の両方を有効することができます。MAB メソッドと dot1x メソッドを共存させて期待どおりに機能させるには、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、順序と優先順位を正しく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

ステップ 9：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 range GigabitEthernet1/0/1-24
 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
```

注：

port-control auto は適用をアクティブ化するコマンドで、検証では追加することも削除することもできます。また、モニタ モードを有効にする **authentication open** を使用して、稼働中の業務を中断することなく実装をテストすることが可能です。

Cisco 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。まず、他の資産との通信を許可する資産を決定するポリシーを定義します。これらの資産は、データ トラフィックの送信元と宛先です。資産は、分類方法に基づいてグループか単一のエンティティになります。これらの資産には、カテゴリに分類するための SGT が付与されます。

これらのセキュリティ グループのカテゴリを使用するポリシーは、ISE とファイアウォール ポリシー マネージャ（Firepower Management Center、ASA Security Device Manager、Cisco Security Manager など）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（産業用イーサネット スイッチを使用する環境など）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。インライン タギングで各パケットが変更され、適切な SGT が追加されます。次の接続デバイスが受け取ったタグ付きパケットを信頼している限り、そのデバイスではポリシーを決定するためにこの情報が使用されます。スイッチおよびファイアウォール インターフェイスで Trustsec によるアクセス制御を有効にします。

複数の製品間でのセキュリティ情報が共有されるため、IT セキュリティ チームは時間のかかる調査を行うことなく、迅速に問題を解決できます。脅威が検出されると、本書で説明するすべてのテクノロジーが連携して迅速に脅威を封じ込めます。ISE には、手動か自動で感染したエンドポイントを封じ込めるよう指示が出されます。このような封じ込めでは、デバイスが観察のためにサンドボックスに移動されたり、修理のために修復ドメインに移動されたり、完全に削除されたりすることがあります。ISE はその後、エンドポイントのアクセス ポリシーを自動的により制限の厳しいものに更新し、ネットワークから効果的にエンドポイントを隔離します。これでデバイスを修復するか、デバイスからネットワークへのアクセスを完全にブロックできます。

Cisco Platform Exchange Grid（pxGrid）は、シスコおよびシスコ以外の製品で ISE からコンテキスト情報を収集し、ISE に具体的な指示（デバイスの隔離など）を送ることができる安全なチャネルを提供します。脅威を封じ込めるには、ISE で pxGrid サービスを有効にし、ISE と Firepower 間、および ISE と Stealthwatch 間で通信を行えるようにすることが不可欠です。

pxGrid のインストール手順については、以下のガイドを参照してください。

- Rapid Threat Containment 設計ガイド：https://communities.cisco.com/docs/DOC-68293
- pxGrid で Firepower と ISE を統合する方法：https://communities.cisco.com/docs/DOC-70354

最新の TrustSec プラットフォームの機能マトリックスについては、以下を参照してください。

https://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/solution-overview-listing.html

Identity Services Engine（ISE）：Cisco TrustSec ポリシー マトリックス

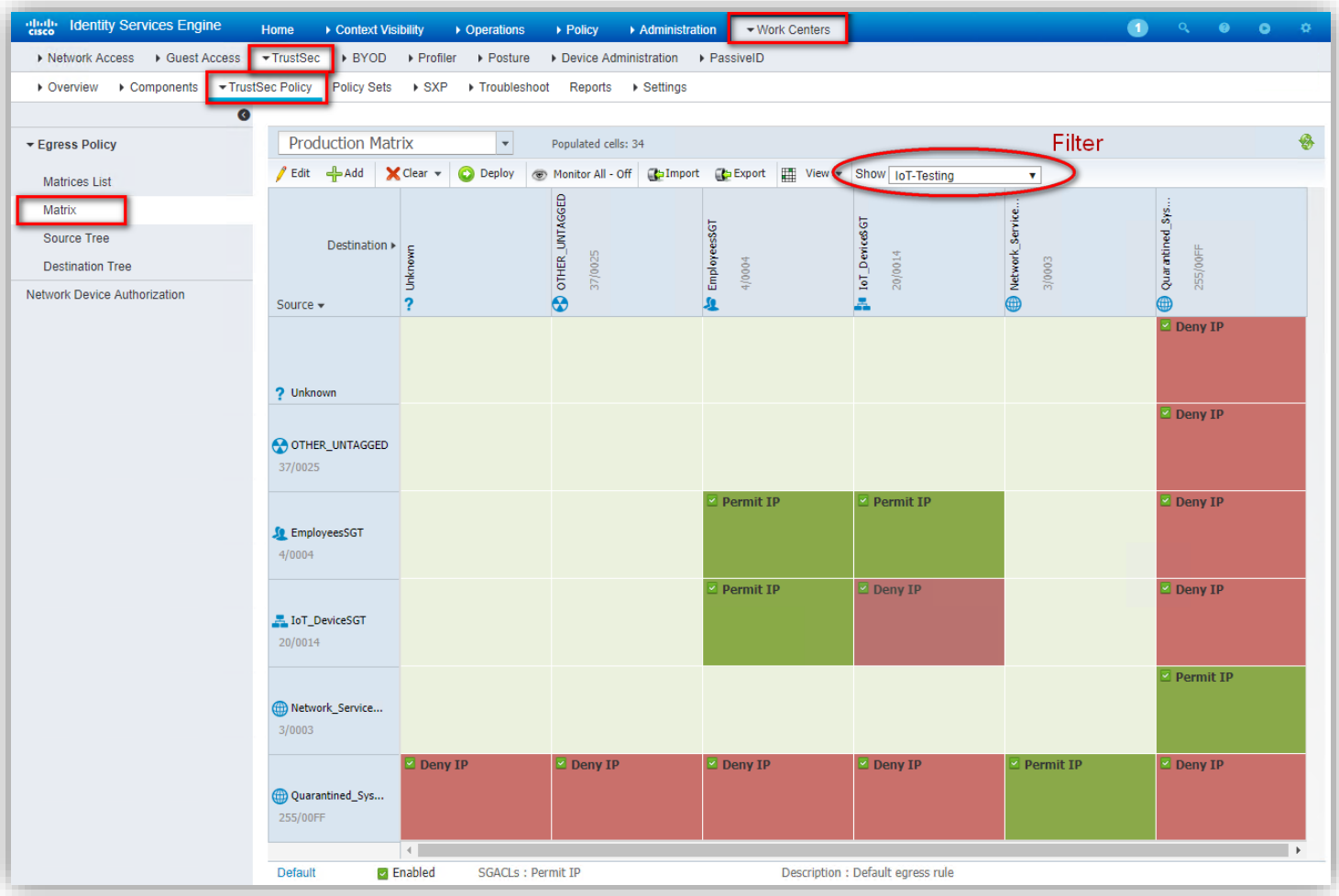
ISE ポリシー マトリックスによって制御され、スイッチによって実行される通信は、一方向のステートフルではない通信です。したがって、適切な対称性と期待される機能を実現するために、要求と応答の両方を考慮する必要があります。アクセス スイッチのポートに宛先デバイスが接続されている場合や、ポートにセキュリティ グループが割り当てられている場合に、パケット送信時にアクセス制御が実施されます。

ISE と TrustSec は、同じスイッチ上、セル内、またはセル間の IoT デバイスの間でスイッチ レベルのセキュリティを実装するのに理想的なテクノロジーであり、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。

つ目次に戻る

42

TrustSec 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。



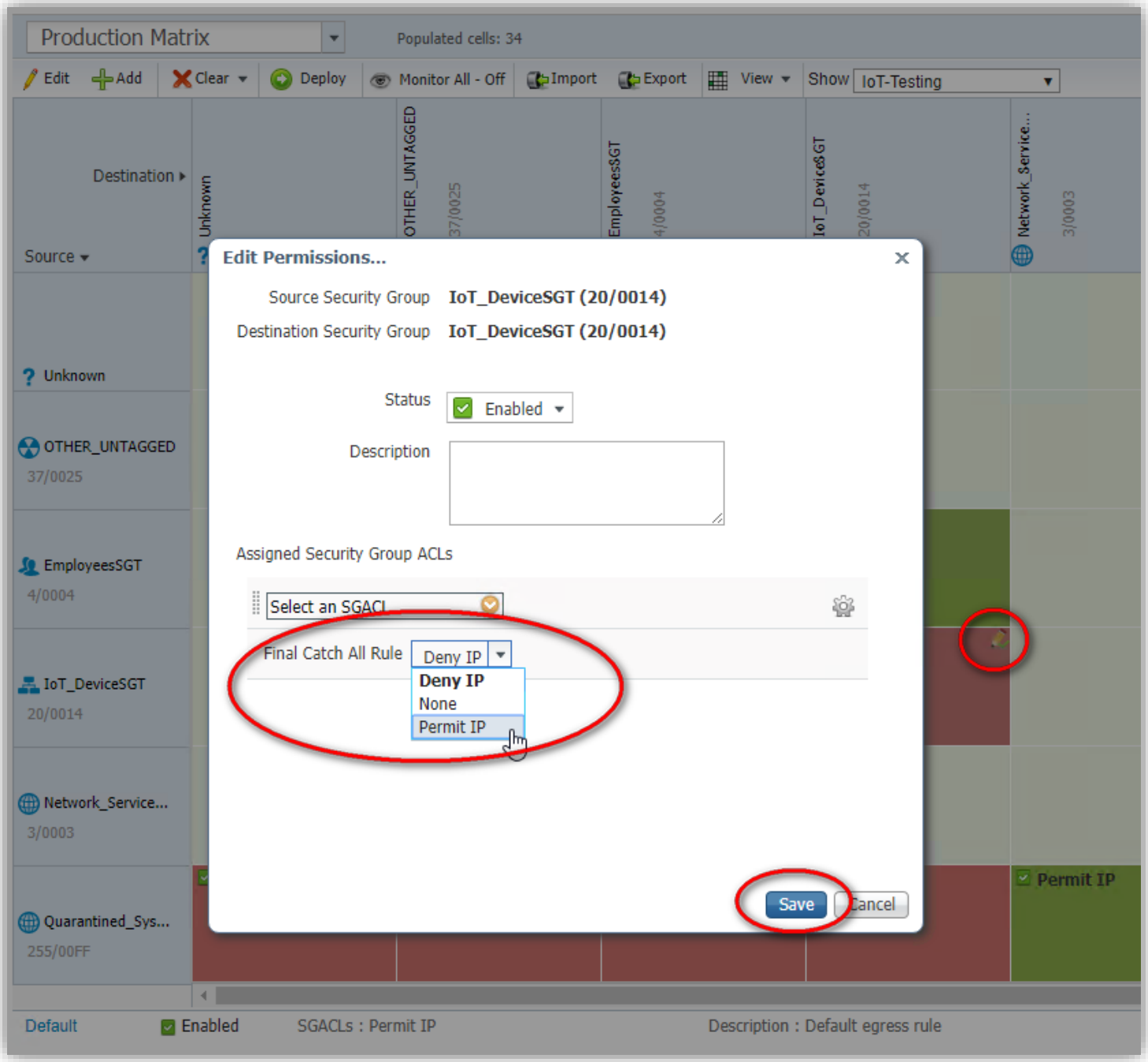
この例では、作業担当の従業員は IoT デバイスと通信できますが、IoT デバイスは相互に通信できません。

注：

必要に応じてマトリックスをフィルタリングし、使用する必要があるグループだけを表示できます。

つ目次に戻る

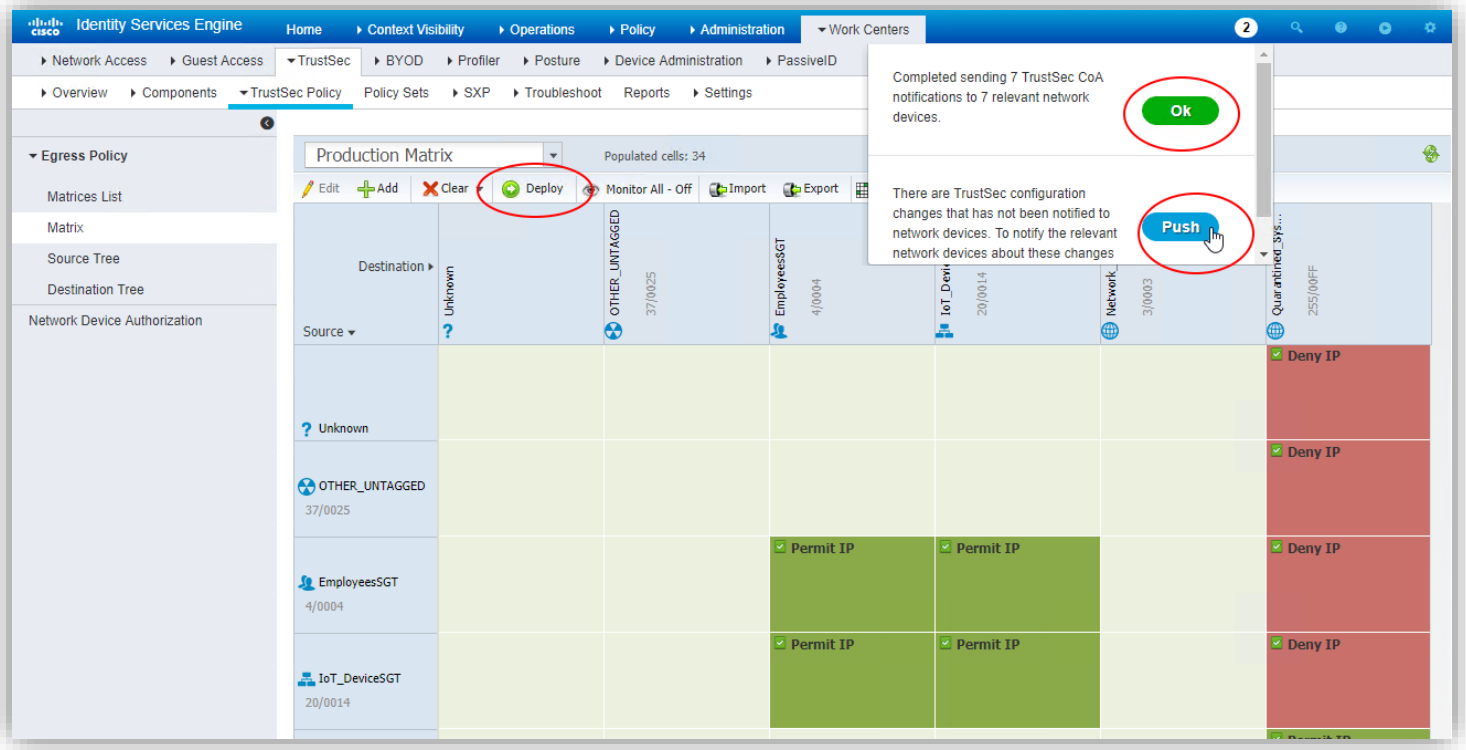
ステップ 1：IoT デバイス間の通信を許可するようにポリシーを編集します。セルをクリックし、セルの右上の鉛筆アイコンをクリックしてセキュリティ グループ アクセス コントロール リスト（SGACL）を選択するか、[最終的な catch-all ルール（Final Catch All Rule）] を変更します。セキュリティ グループ ACL により、特定のポートとプロトコルをきめ細かく開いたりブロックしたりできますが、この例では [最終的な catch-all ルール（Final Catch All Rule）] を [IP を許可（Permit IP）] に変更してすべての IP 通信を許可します。[保存（Save）] をクリックします。



つ目次に戻る

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。

また、TrustSec ポリシー マトリックスでは、最初に一連のデバイスに設定をステージングし、実稼働環境のデバイスに展開する前に変更の影響を確認することもできます。



例に関する注意：

TrustSec 適用が有効になっていないスイッチに宛先デバイスが接続されている場合、通信をブロックするようにポリシーが設定されていても、パス内の他のスイッチすべてに TrustSec 適用が設定されていても、通信はブロックされません。TrustSec が有効になっている出力スイッチ ポート（デバイスが接続されているスイッチ）だけで適用が実行されます。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。

つ目次に戻る

45
Security Group Tag Exchange Protocol

3 つのビジネス使用例におけるセグメンテーションの最後の部分では、通過する各ネットワーク デバイス全体のフローを特定するのに必要な情報を共有します。この情報は、タグ（SGT）でわかるセキュリティ グループと ISE への認証に使用されるアイデンティティにコンテキストに従ってリンクされたデバイスの IP アドレスで構成されます。

Security Group Tag（SGT）Exchange Protocol（SXP）は、これらのネットワーク デバイスに SGT を伝播するために使用されます。SXP は、SGT を認識可能なネットワーク 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、ISE で行ったように静的または動的に割り当てられ、ネットワーク ポリシーで使用されます。

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も設定できます。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。

アーキテクチャのセクションで説明したように、SXP はハブアンドスポーク方式で設定され、すべてのネットワーク デバイスが SXP のために ISE サーバとピアリングされています。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。

SXP を許可するための Cisco ASA におけるポリシーの例外設定

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、および MD5-AUTHENTICATION TCP オプションを有効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。

次のコマンド セットは、CLI を使用した 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 OR 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
```

つ目次に戻る

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]

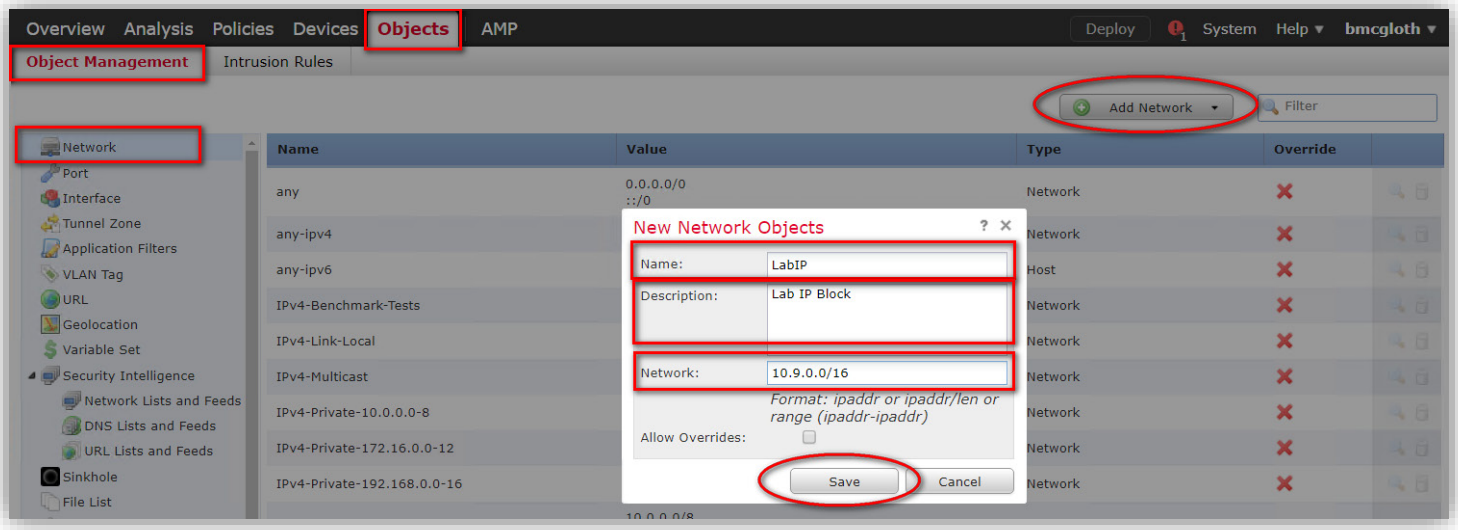
SXP を許可するための FTD におけるポリシーの例外設定

FTD では、以下の大まかな手順でファイアウォールに対する FlexConfig の修正を作成して SXP プロトコルを許可する方法を概説します。

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

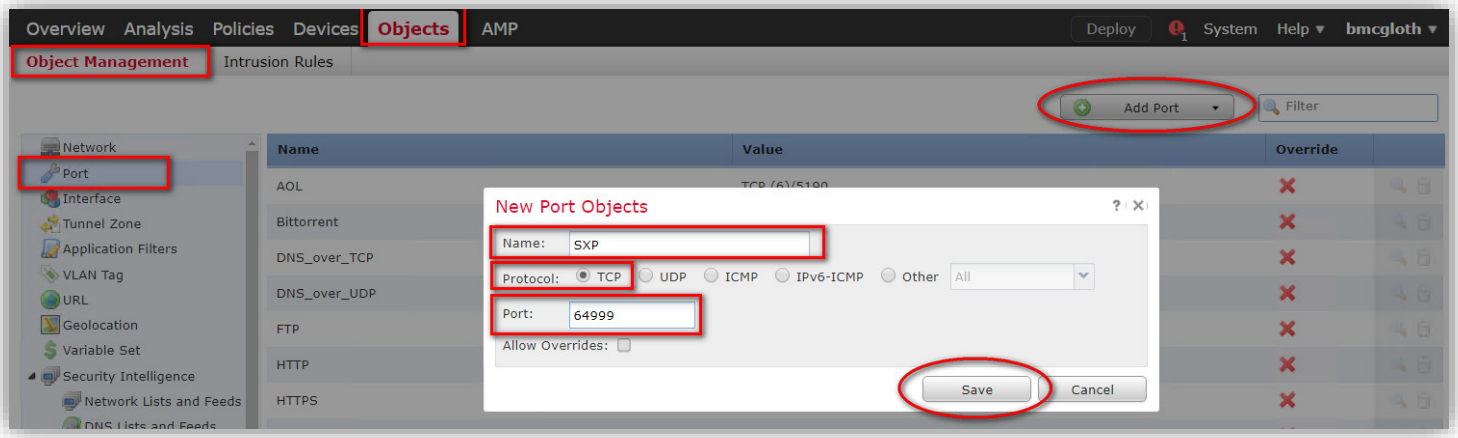
以下に概説した手順の詳細を示します。まず、すべての適切なスイッチの IP および ISE にポート 64999 を許可する拡張アクセス リストのオブジェクトを追加します。この例では、ラボ IP ブロック用のネットワーク オブジェクトを作成しました。

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）] の [オブジェクトの追加（Add Object）] 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。

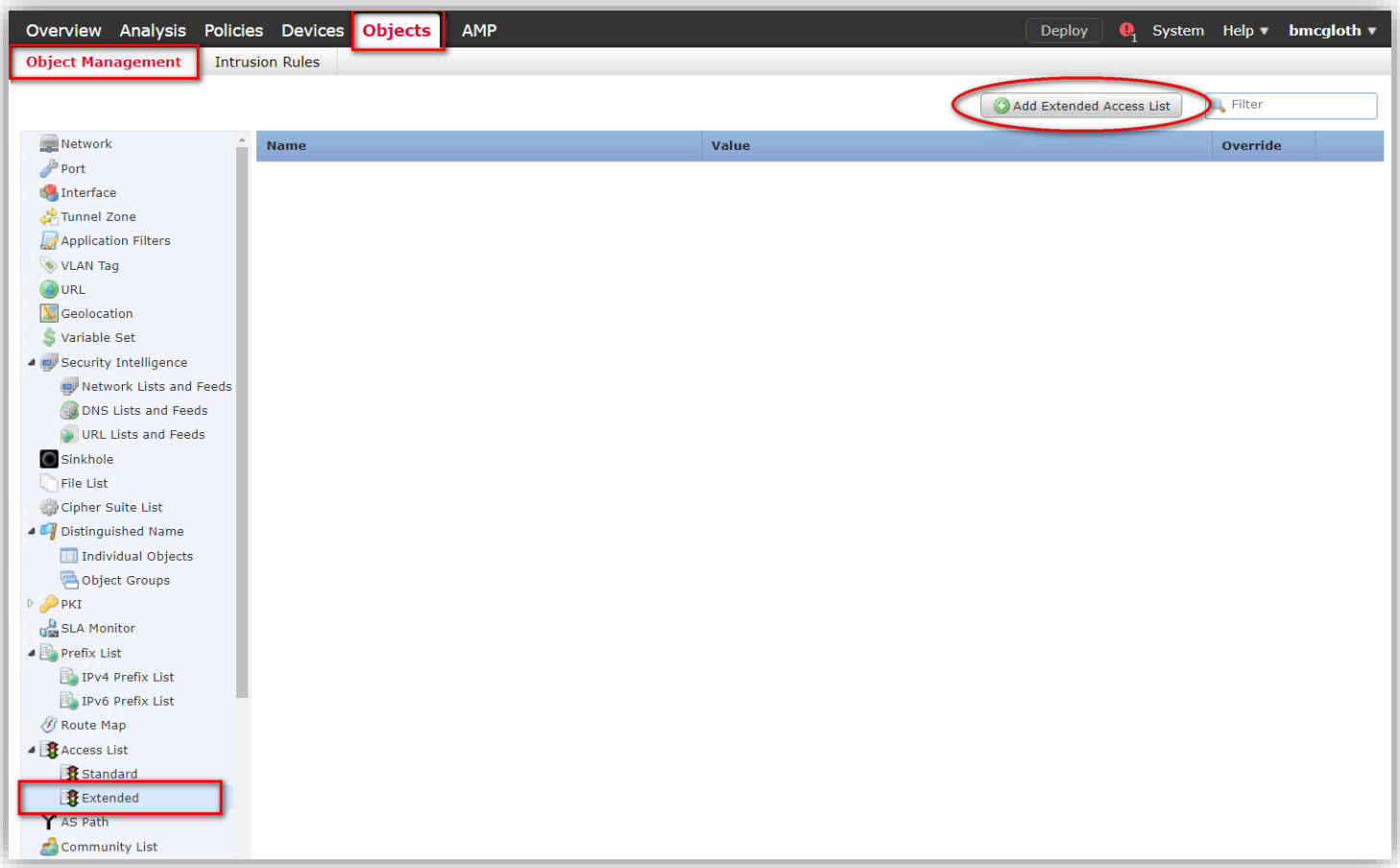


つ目次に戻る

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）] の [オブジェクトの追加（Add Object）] ボタンをクリックします。[名前（Name）] に「SXP」 と入力して [TCP] を選択し、[ポート（Port）] に「64999」 と入力します。[保存（Save）] をクリックします。

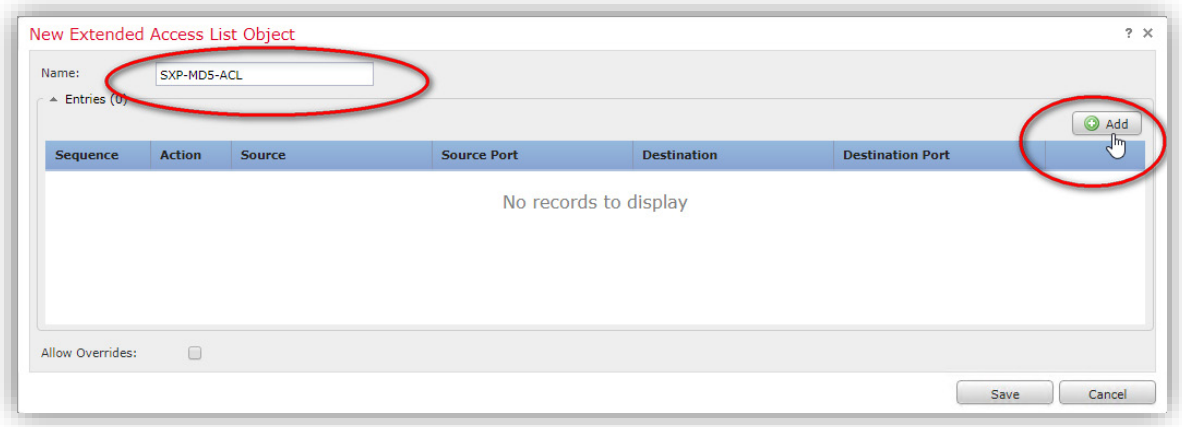


ステップ 3：[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [アクセスリスト（Access List）] > [拡張（Extended）] に移動します。右上の [拡張アクセスリストの追加（Add Extended Access List）] ボタンをクリックします。

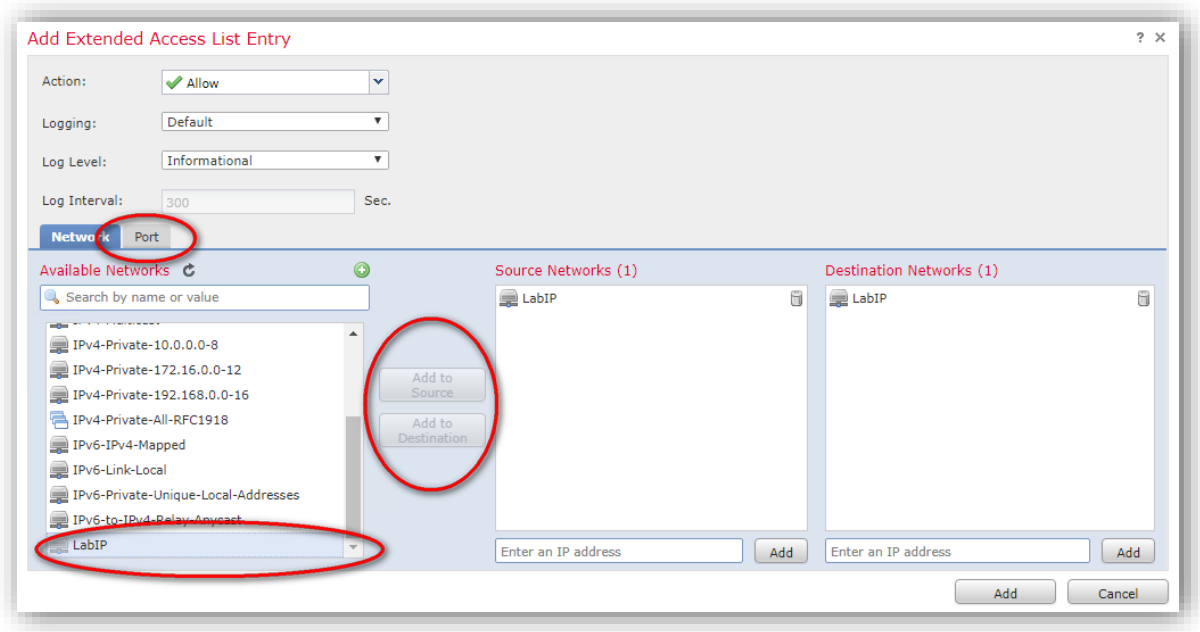


つ目次に戻る

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。

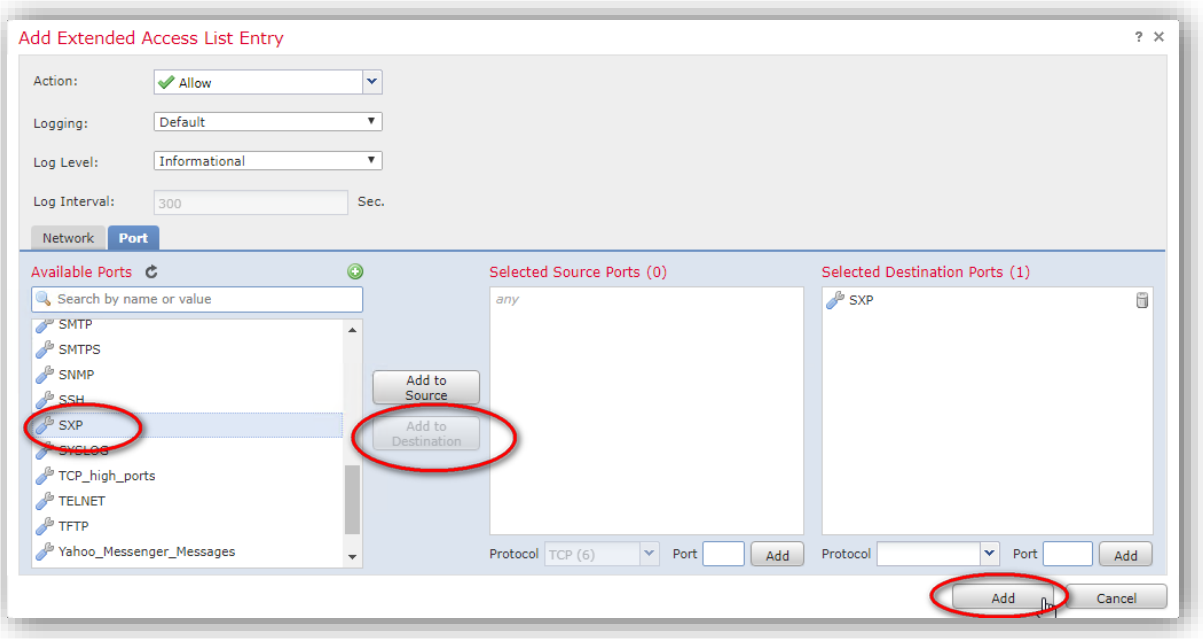


ステップ 5：前のステップで作成した適切なネットワーク オブジェクトを選択し、お使いの環境に適切な送信元および宛先ネットワークにそのオブジェクトを追加します。[ポート（Port）] タブをクリックします。



つ目次に戻る

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。



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、および class-map を貼り付けます。

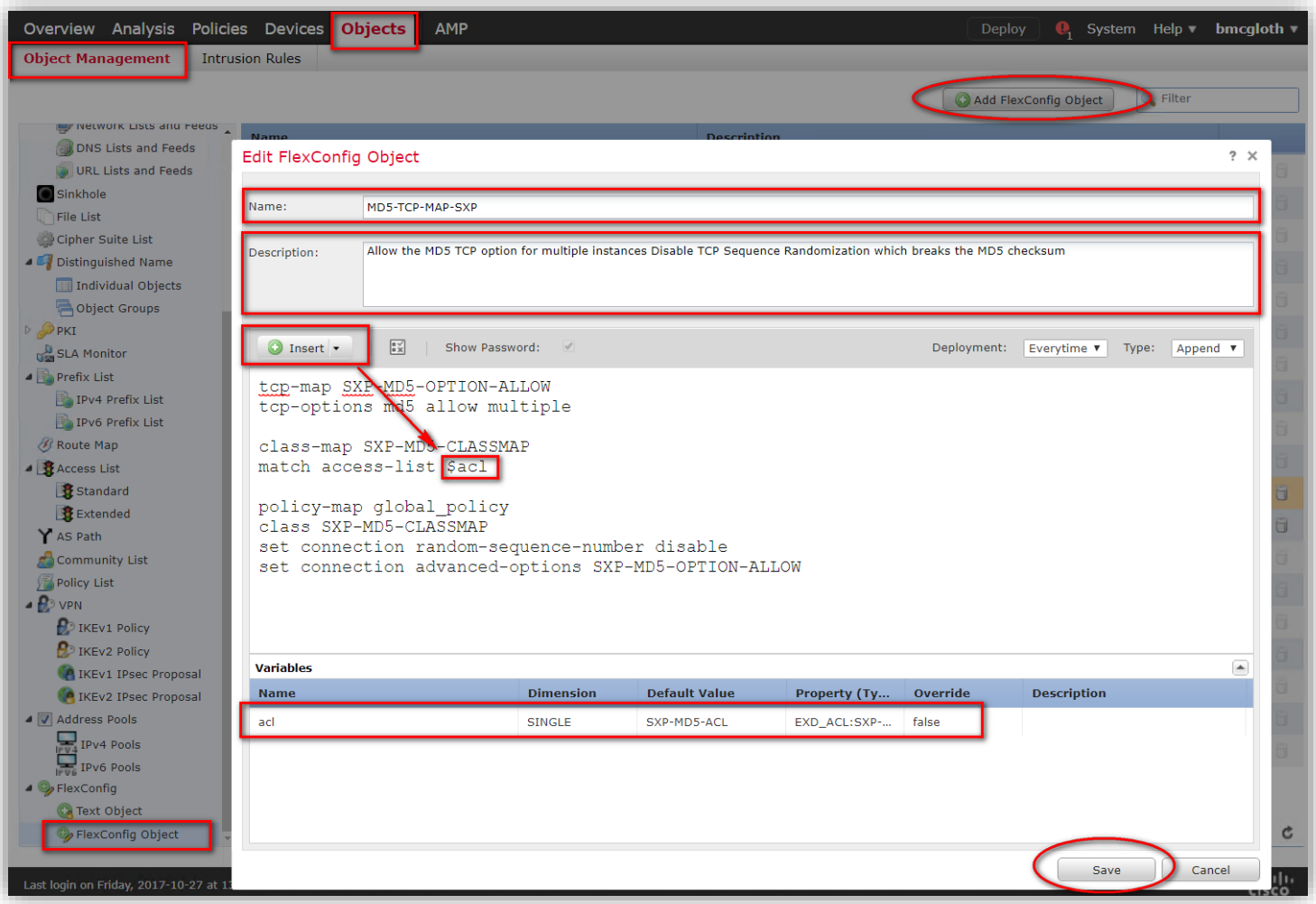
```
tcp-map SXP-MD5-OPTION-ALLOW
  tcp-options md5 allow multiple

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。

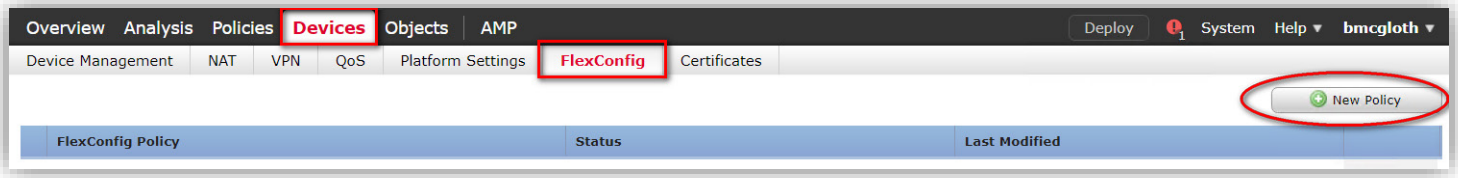
```
policy-map global_policy
  class SXP-MD5-CLASSMAP
   set connection random-sequence-number disable
   set connection advanced-options SXP-MD5-OPTION-ALLOW
```

つ目次に戻る

[保存（Save）] をクリックします。

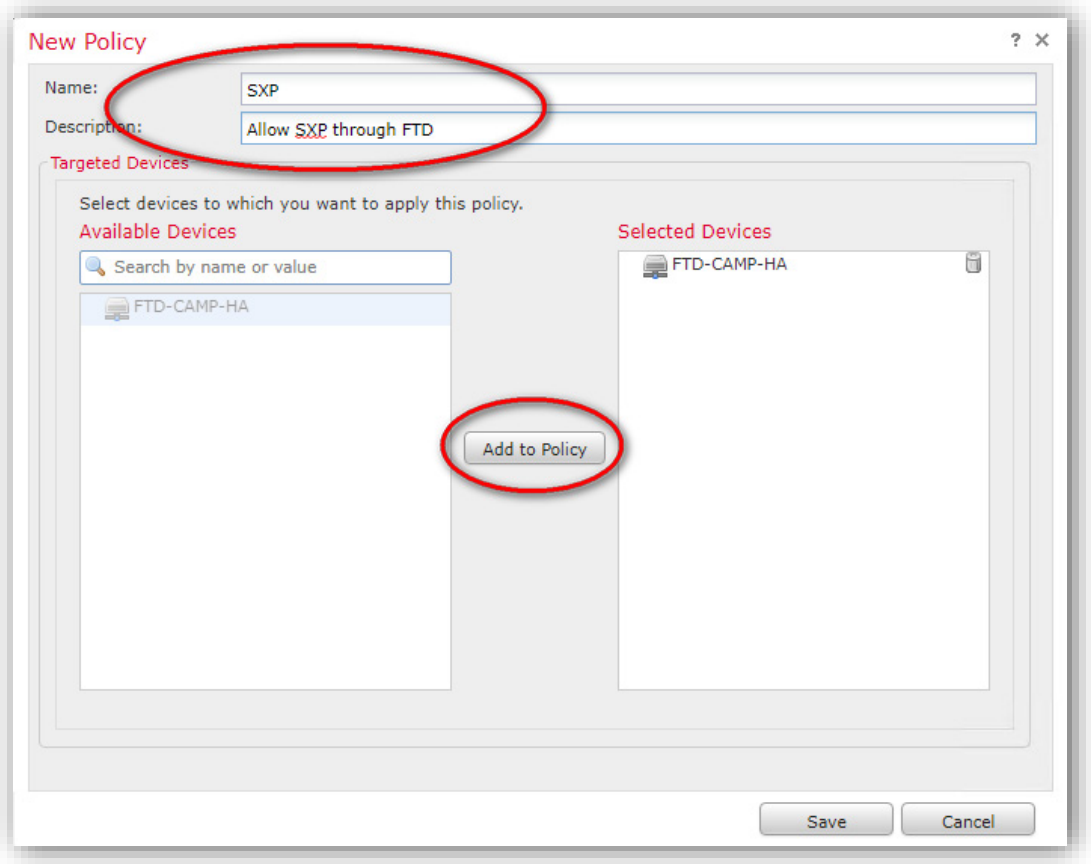


ステップ 8：ネットワーク内のデバイス用に新しい FlexConfig ポリシーを作成します。[デバイス（Devices）] > [FlexConfig] に移動します。右上の [新しいポリシー（New Policy）] ボタンをクリックします。



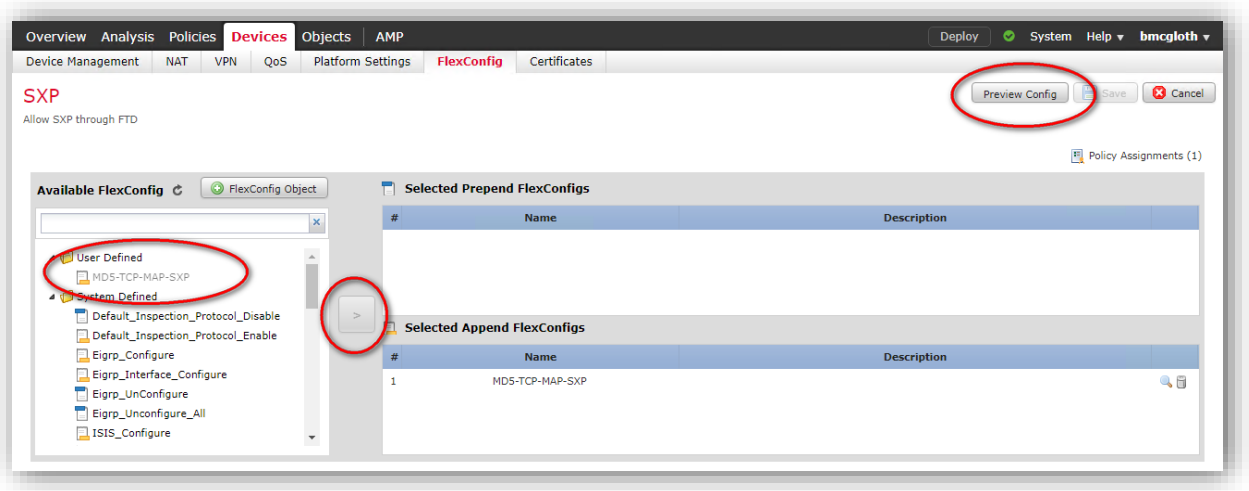
つ目次に戻る

ステップ 9：[名前（Name）] と [説明（Description）]（任意）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。



つ目次に戻る

ステップ 10：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。



ステップ 11：[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。

これでファイアウォールを通過する SXP が適切に接続されて機能するようになります。すでにピアが設定されている場合は、ISE にて SXP 接続テーブルをチェックすることで接続を確認できます。

FlexConfig の詳細については、以下を参照してください。

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

つ目次に戻る

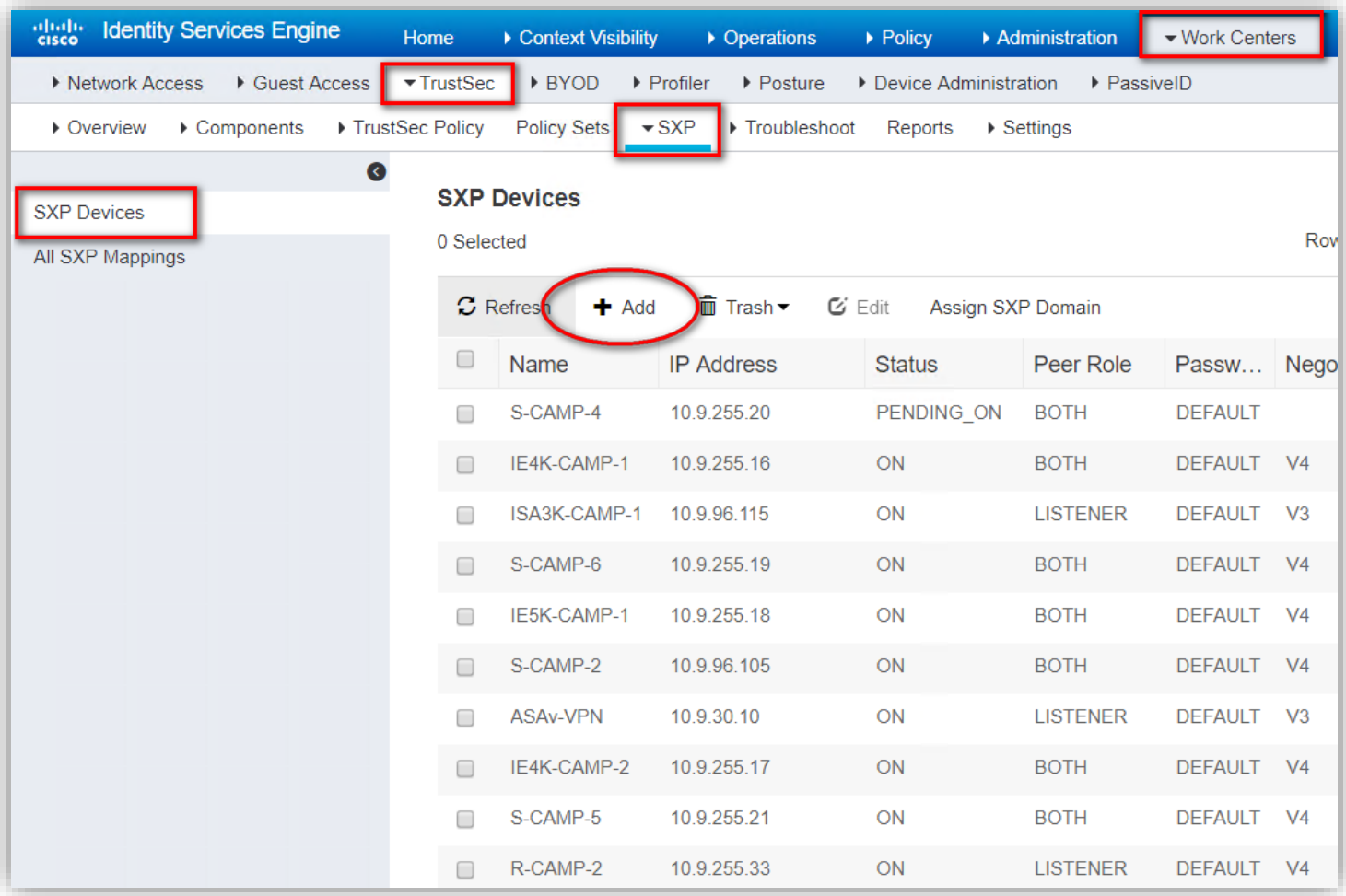
Identity Services Engine（ISE）での SXP デバイス ピアの設定

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。

この設計では、ISE PSN と各スイッチ/ファイアウォール間をハブアンドスポーク型で SXP を実装するベスト プラクティス モデルを使用します。デバイス間の SXP の関係を設定する別の方法では、展開中に設定ミスが発生しやすく、ループが起きる可能性があります。

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。



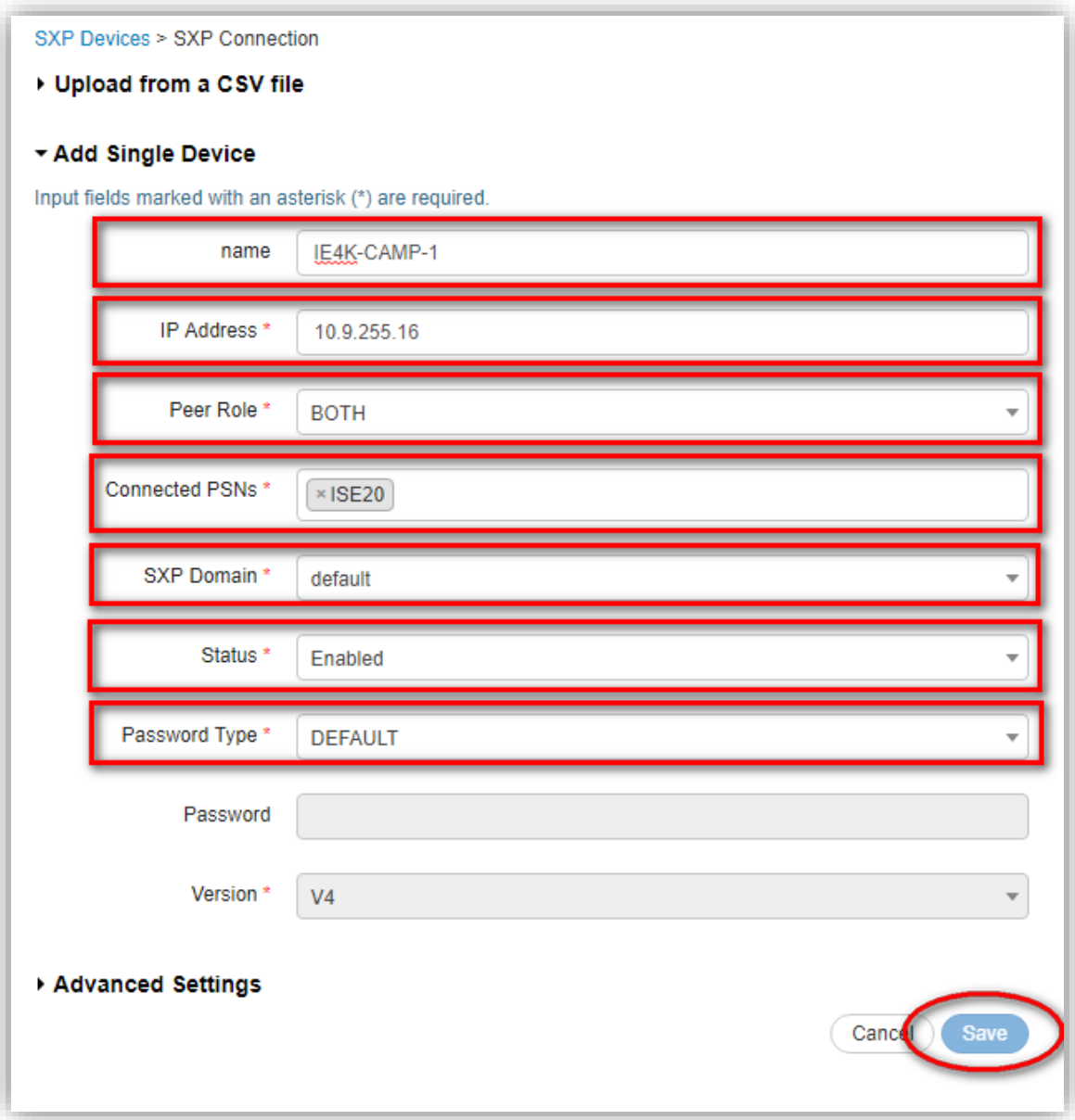
つ目次に戻る

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* と表示されます。BOTH をサポートしていないスイッチのピア ロールは、LISTENER に設定する必要があります。

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）]、[接続 PSN（Connected PSNs）]、および [パスワード（Password）] を入力します。[保存（Save）] をクリックします。



つ目次に戻る

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。

デバイスが [ピアロール（Peer Role）] の [BOTH] をサポートしていない場合は、ISE でデバイスの [ピアロール（Peer Role）] を [LISTENER] に設定します。

ネットワークの各 SXP スイッチ、ルータ、およびファイアウォールでこれらの手順を繰り返します。

ネットワーク デバイスでの Cisco TrustSec と 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）間の 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 で認証を行って PAC ファイルを作成するときに使用する、このスイッチの Cisco TrustSec デバイス ID および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。

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

注：

*スイッチの ID とパスワード*は、ISE TrustSec で設定したものと同じになるようにしてください。

ステップ 2：ピアの接続を設定する前に、コンフィギュレーション モードで Cisco TrustSec SXP を有効にします。

```
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 送信元アドレスが指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。

つ目次に戻る

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 モードの BOTH をサポートしていない場合は、以下に示すようにピアを SPEAKER に設定します。これは、ハブアンドスポーク設計と前述の ISE 側における SXP の設定方法に一致します。

```
cts sxp connection peer ISEPSN password default mode peer both or
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
```

これにより、SXP のステータスと接続の詳細情報が表示されます。

```
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 のテスト コマンド

- show cts environment-data
- show cts pac
- show cts sxp sgt-map brief

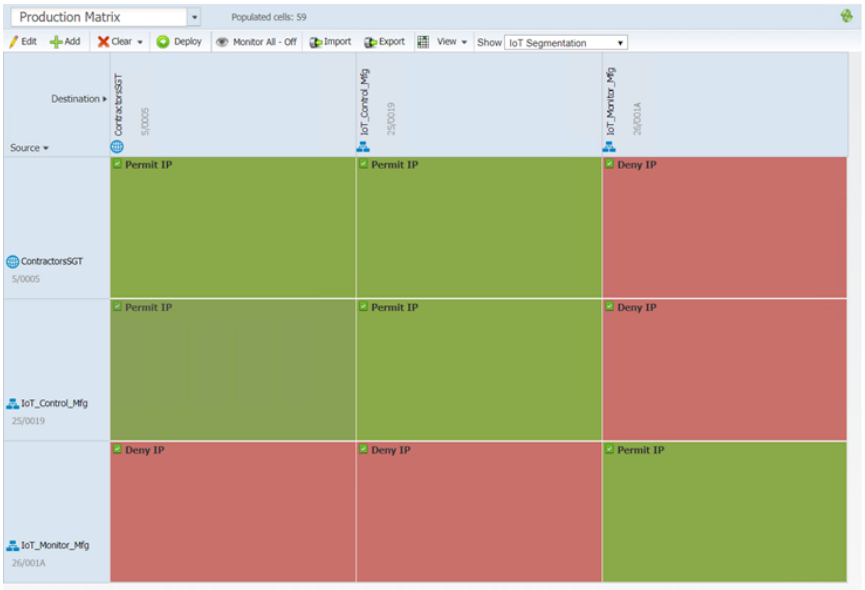
つ目次に戻る

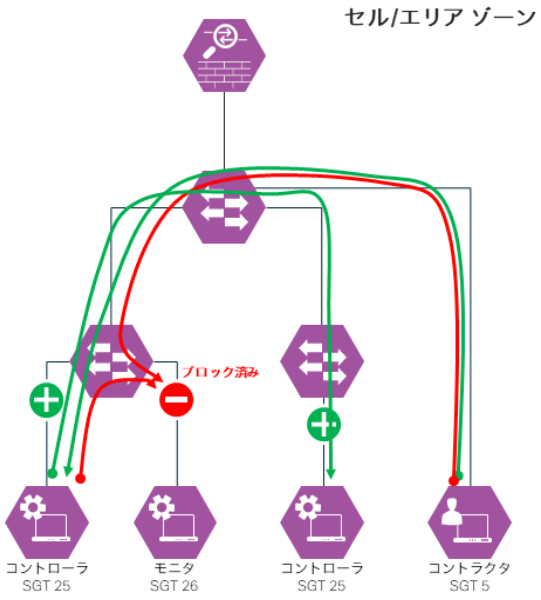
57

Cisco TrustSec によるアクセス制御の有効化

工場内では、Purdue モデルのレイヤ 1 および 2 のセル内とセル間にある IoT システムを保護するためにセグメンテーションに TrustSec を使用することが、静的 VLAN のメソッドに代わるコスト効率と拡張性に優れた手段となります。たとえば、すべてのデバイスが同じ VLAN 上にあり、同じサブネットで静的 IP アドレッシングを使用する単一のセルのフラット ネットワークは、TrustSec のセキュリティ グループ タグと図 15 に示す ISE で提供されるポリシーを使用して完全にセグメント化できます。

図 15：アクセス制御のための TrustSec ポリシー





以下の設定により、スイッチにアクセス制御の機能を追加します。

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 認可を使用するようにスイッチを設定します（ISE グループは、このガイドの前述のセクションで作成済みです）。

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

ステップ 2：cts 認可に 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
```

ら目次に戻る

ステップ 4：グローバルおよび VLAN ごとにロールベースのアクセス制御を有効にします。

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

産業用イーサネット スイッチの IE4K および IE5K の TrustSec によるアクセス制御は、直接接続デバイスと受信時に信頼された STG 情報を含むパケットに対してのみ機能します。その理由は、SXP で学習したマッピングをこれらのプラットフォームでのアクセス制御に使用できないためです。工場のセル内およびセル間の通信をセグメント化するには、インライン タギングをサポートするようにスイッチを設定し、要望どおりにアクセス制御を機能させる必要があります。アップストリームまたはダウンストリームの隣接スイッチやファイアウォールからこれらのスイッチに送信されるパケットにタグを付けることにより、包括的なアクセス制御を実現できます。インライン タギングを有効にするには、まず IP ルーティングを有効にする必要があります。

ステップ 5 ～ 10 では、産業用イーサネット スイッチと Cisco Catalyst スイッチでインライン タギングを有効にする方法を説明します。

ステップ 5：スイッチでグローバルにルーティングを有効にします（LAN Base 以外のソフトウェアが必要）

```
IE4K-CAMP-2(config)#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 タギングを有効にする前に、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はコンフィギュレーション 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
```

つ目次に戻る

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 タギングを有効にします。学習した SGT の伝播を有効にし（デフォルト）、不明なトラフィックに定義済みの SGT を手動でタグ付けして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
```

このケースの「trusted」は、インターフェイス上の入力トラフィックで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 によるアクセス制御は、IoT デバイスが接続されたスイッチの出力ポートで行われるため、スイッチ間およびアップリンクのトランク ポートのインターフェイスではアクセス制御を無効にする必要があります。下記に、ロールベースのアクセス制御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
```

60

TrustSec のトラブルシューティング コマンド

- show cts interface brief
- show cts sxp sgt-map brief
- show cts role-based counters
- show 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

その他のヘルプについては、TrustSec トラブルシューティング ガイドを参照してください。

https://communities.cisco.com/docs/DOC-69479

つ目次に戻る

61

Cisco TrustSec Cisco Firepower Next-Generation Firewall（NGFW）ポリシー

Firepower のポリシーは、Industrial DMZ へのフローと Industrial DMZ からのフロー、およびセル/エリア ゾーン間のフローを制御します。Purdue レベル 3 以上（企業ゾーンと Industrial DMZ）では、Firepower 2100 および 4100 シリーズがビジネスのすべての部分にわたる多層防御を提供します。このような過酷な産業環境で ISA 3000 や ASA 5506H などのデバイスを使用する場合は、Purdue レベル 3 以下（セルの境界セキュリティ）が最適です。

Firepower Management Center は、Rapid Threat Containment 設計ガイドに従ってインストールと設定を行います。このガイドには、インストールから ISE に戻る pxGrid 接続の確立までの手順が記載されています。ラボのインストールとテストに関しては、自己署名証明書の代わりに認証局をインストールして使用しました。

Rapid Threat Containment のガイドについては http://cisco.com/go/rtc を、その他の Firepower と ISE のガイドについては https://communities.cisco.com/docs/DOC-68292 を参照してください。

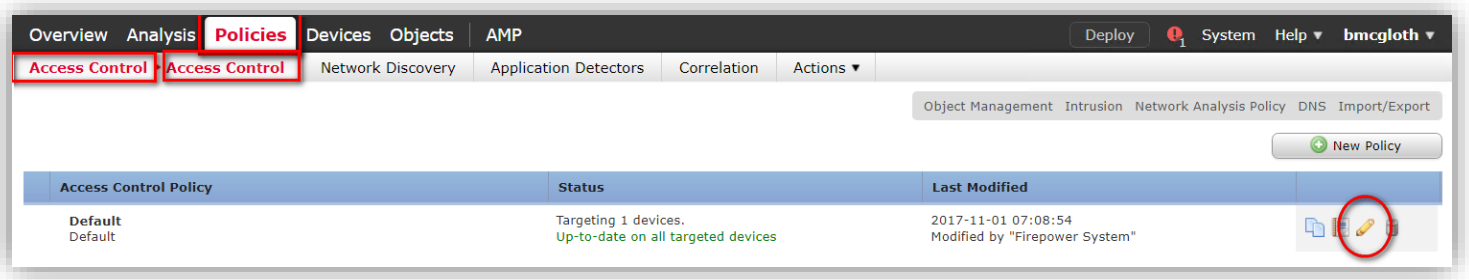
このサンプルのポリシーでは、従業員は企業ポリシーでブロックされているカテゴリ（ギャンブル、ピアツーピア、マルウェア、ハッキング）を除き、すべてのインターネット URL にアクセスできます。システムが隔離された状態になると、企業サポート サイト「cleanme.cisco-x.com」への接続を除く、すべてのアウトバウンド Web 接続がブロックされます。

pxGrid により、トラフィックの送信元として SGT を使用し、ネットワークやデバイスの IP アドレスを指定する必要をなくしてポリシーを大幅に簡素化できます。

ここで、IoT 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。

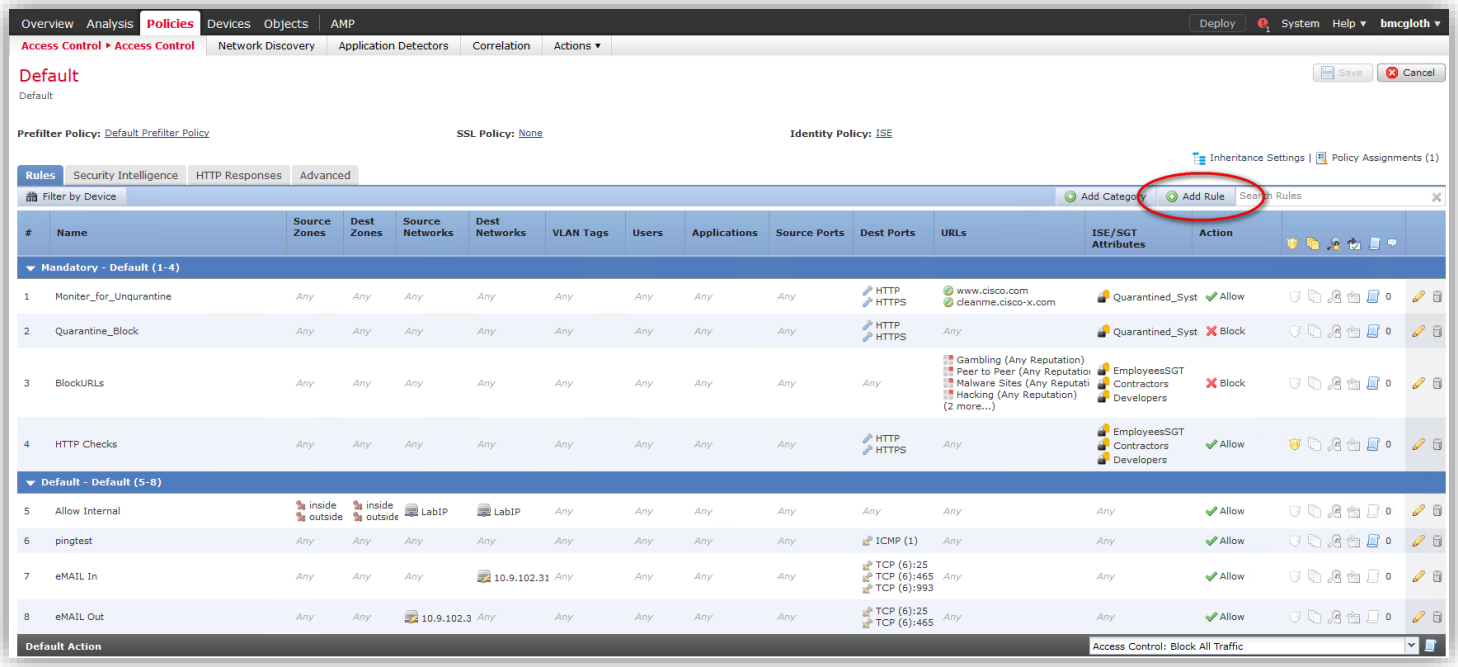
Firepower Management Center では、[ポリシー（Policies）] > [アクセスコントロール（Access Control）] > [アクセスコントロールポリシー（Access Control Policy）] > [デフォルト（Default）] を選択して次世代ファイアウォールおよび次世代 IPS のポリシーを設定します。

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。

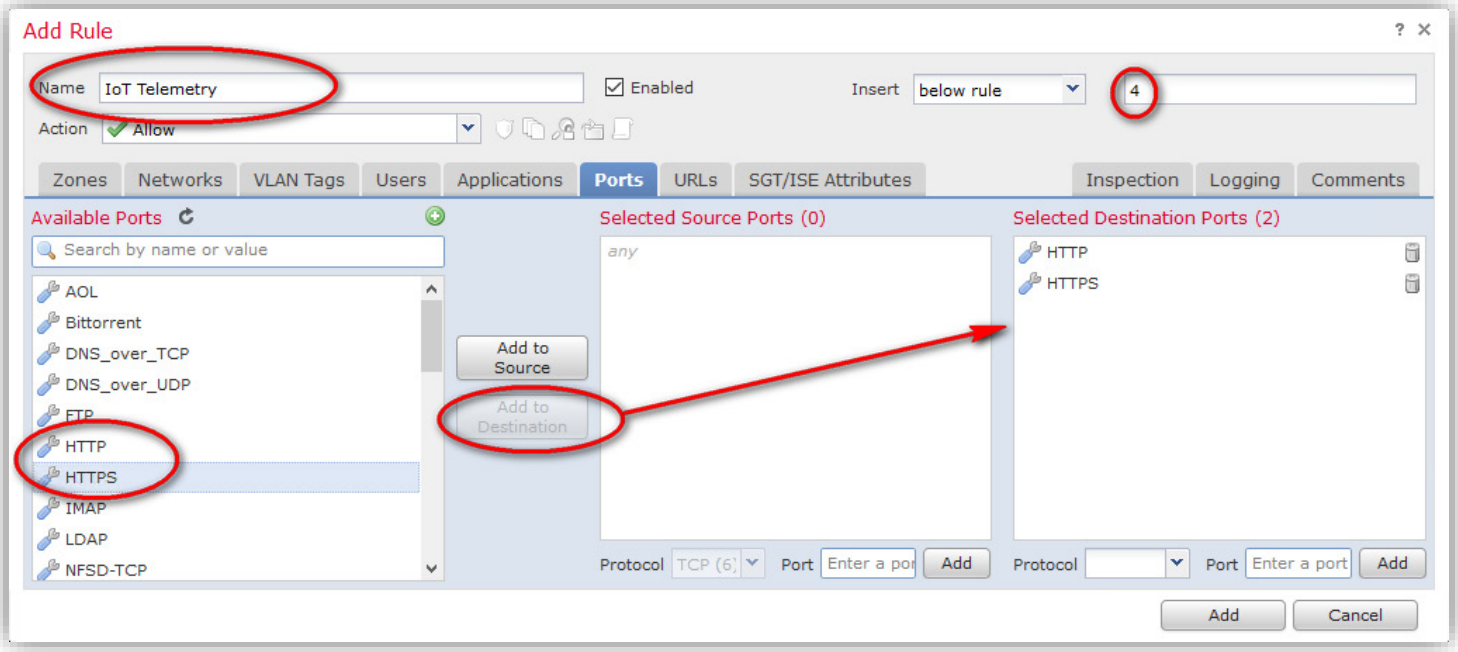


つ目次に戻る

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。

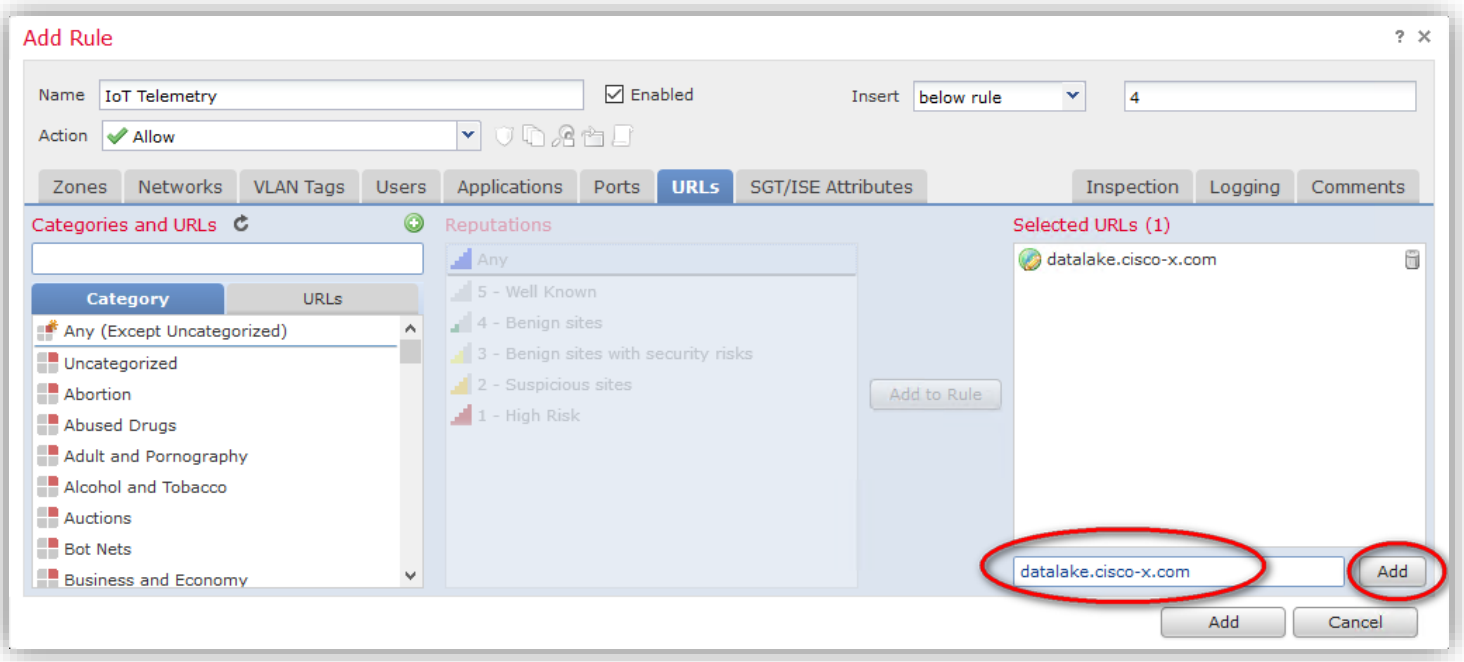


ステップ 3：わかりやすい名前を入力し、ルールを挿入する場所と宛先ポートを指定します。

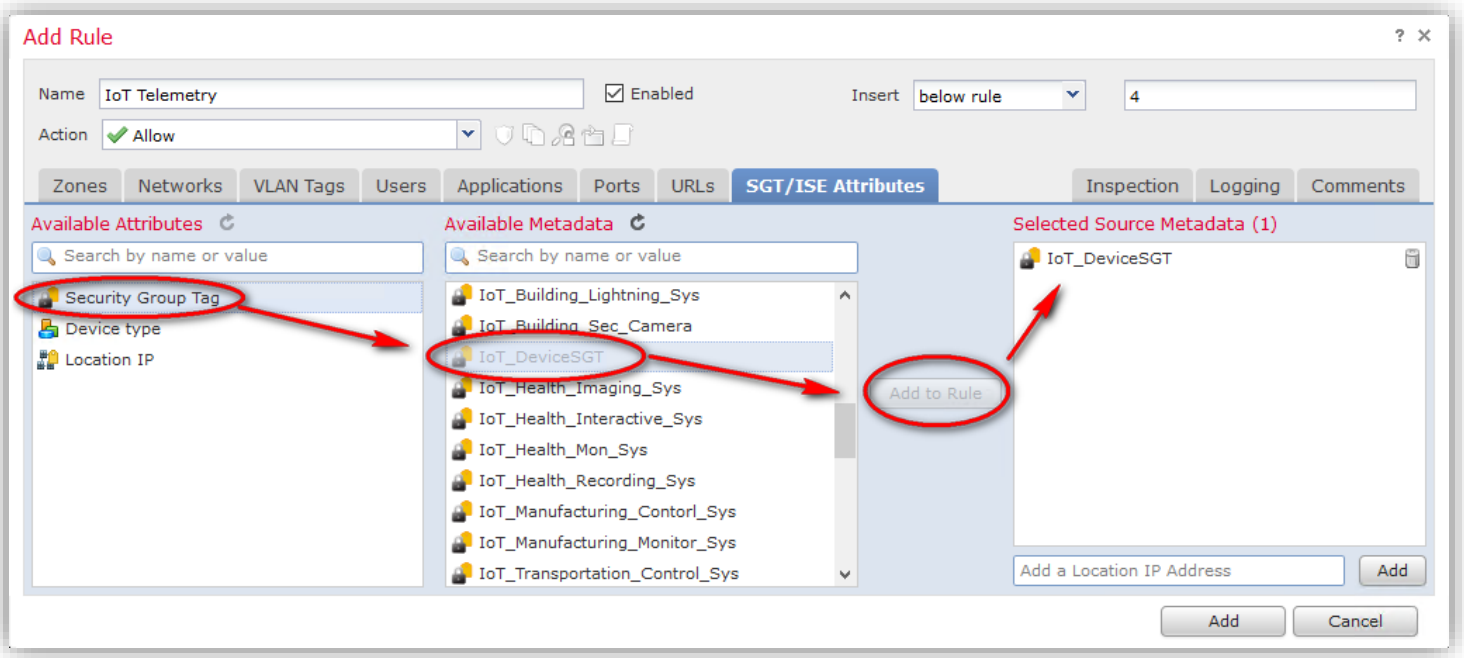


つ目次に戻る

ステップ 4：URL を入力し、ボックスの横にある [追加（Add）] をクリックします。



ステップ 5：テレメトリを送信する必要があるデバイスの SGT グループを選択します。

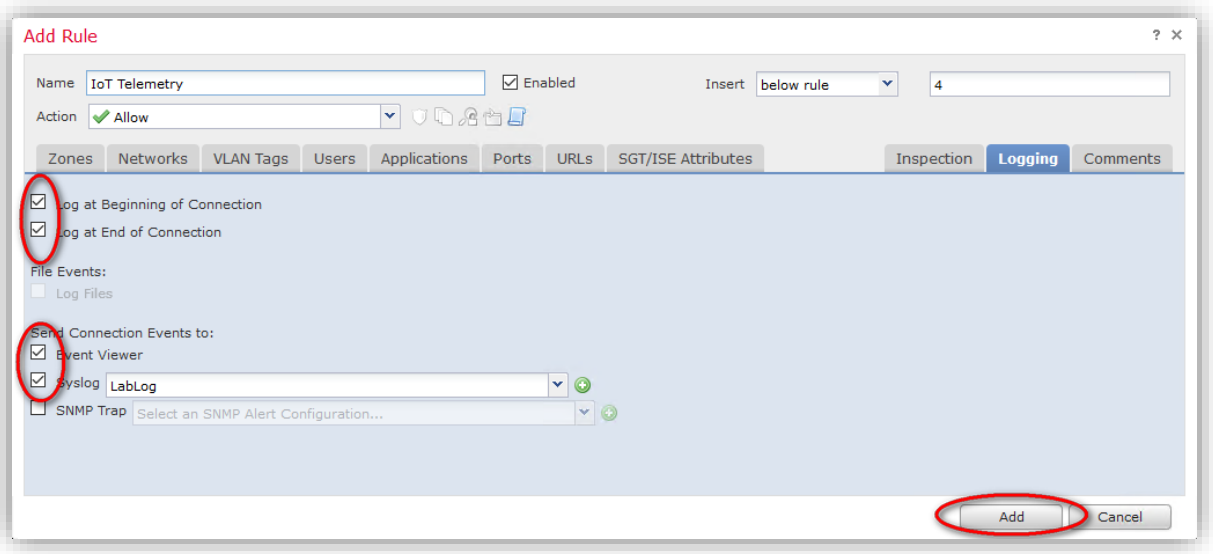


上記のセキュリティ グループ タグ リストにある使用可能なメタデータは、pxGrid を通じて ISE から取得されます。pxGrid のインストール手順については、以下のガイドを参照してください。

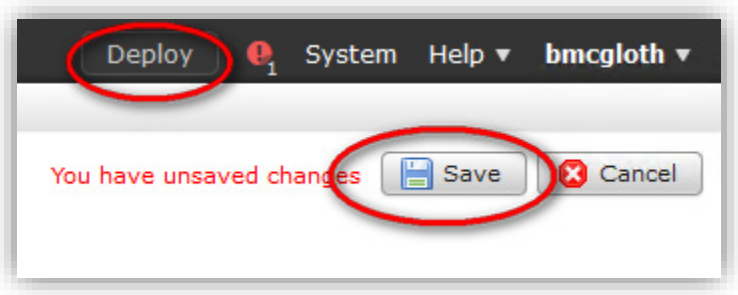
- Rapid Threat Containment 設計ガイド：https://communities.cisco.com/docs/DOC-68293
- pxGrid で Firepower と ISE を統合する方法：https://communities.cisco.com/docs/DOC-70354

つ目次に戻る

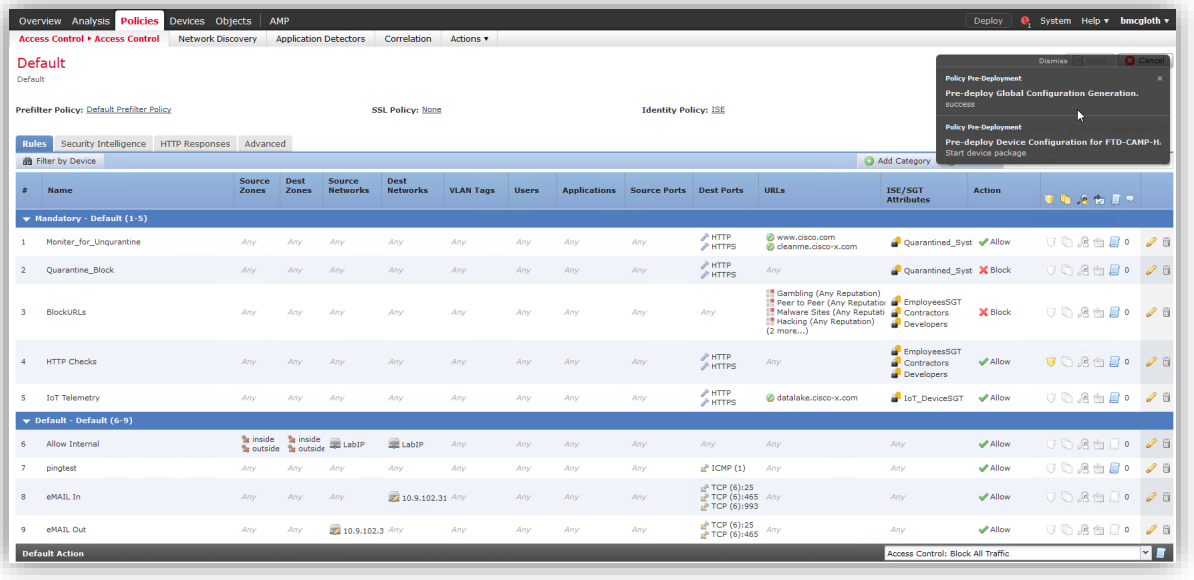
ステップ 6：ロギングを有効にし、設定が完了したら [追加（Add）] をクリックします。



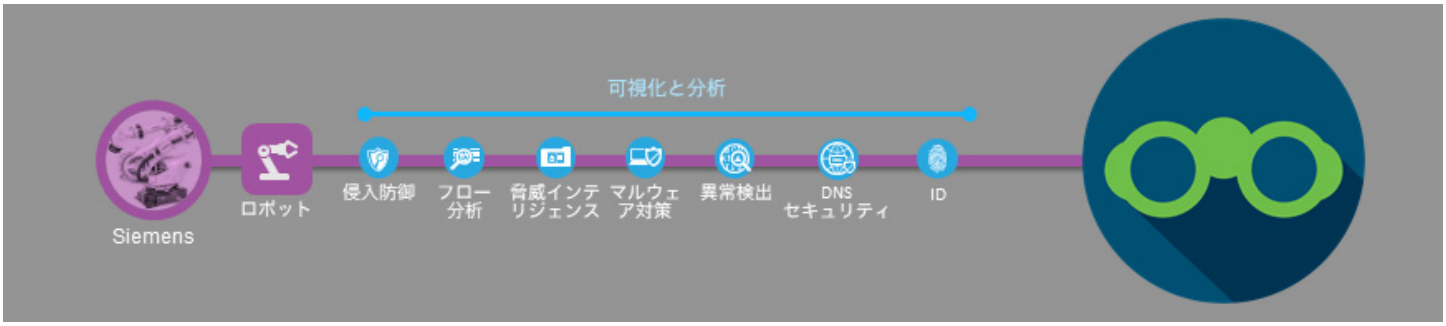
ステップ 7：すべてのルールが追加されたら、[保存（Save）] と [展開（Deploy）] をクリックしてルールを実装します。



ステップ 8：これで展開は完了です。



つ目次に戻る

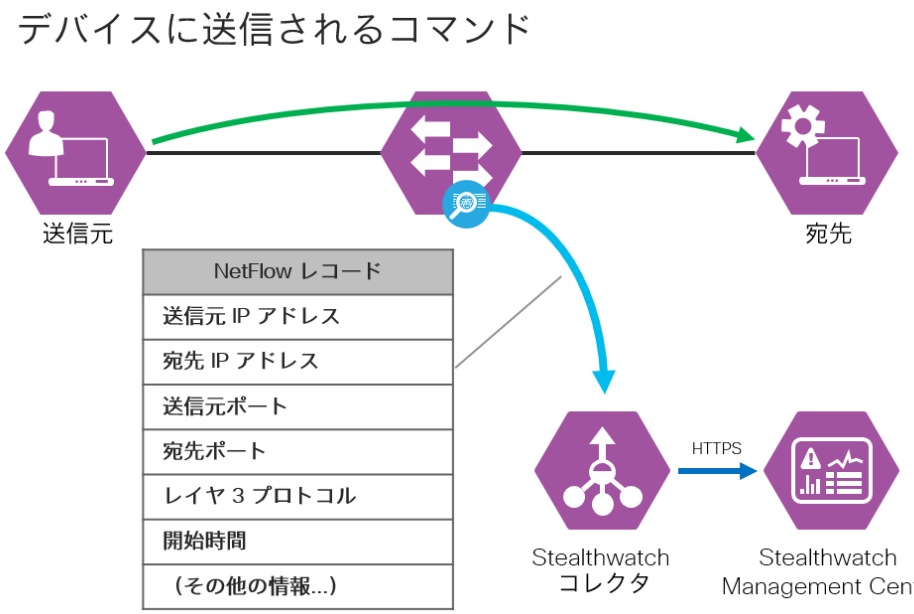


Cisco Stealthwatch

Cisco Stealthwatch はネットワークをセンサー（NaaS）に変え、スイッチ上の NetFlow と sFlow、ルータ、およびファイアウォール上の IPFIX を活用することにより、ネットワークで優れた可視性を提供します。pxGrid を ISE に統合することにより、攻撃者を隔離して脆弱な IoT デバイスを保護できます。

NetFlow は、図 16 に示すようにネットワーク上の「通信」について説明するメタデータで構成されます。ここには、ネットワーク通信、通信が行われたタイミングに関する情報、通信の所要時間、および使用されたプロトコルに関する重要なテレメトリの詳細が含まれています。NetFlow は、ネットワークを通過するフローを可視化するとともに、高度なネットワーク異常およびセキュリティ検出機能を提供します。

図 16：NetFlow レコード



Stealthwatch は、ネットワークにおける各デバイスの動作、すべてのネットワーク接続、インターフェイスの使用率、および全体的なネットワーク パフォーマンスに関するリアルタイムの情報を提供します。また、IoT のピアツーピア マルウェアをはじめとする、さまざまなレベルのマシン間通信を可視化できます。悪意のある P2P トラフィックは、コマンド アンド コントロール サーバに関連付けられた既知の IP アドレスとホストのリストに依存する従来のアプローチで検出してブロックするのが困難です。多層防御のセキュリティが必要ですが、さまざまな情報ポイントと情報ベクトルを組み合わせることで示される情報を分析して理解できれば、運用に関する意思決定を行うための他にはない可視性も得られます。

つ目次に戻る

たとえば、DoS 攻撃はデバイスのリソースを使い尽くそうとします。これらの標的となるリソースは、ネットワーク帯域幅の場合もあれば、処理能力やオペレーティング システムのデータ構造の場合もあります。DDoS 攻撃を開始するにあたり、悪意のある攻撃者はまず、ユーザに対するサービス拒否のため必要な量のトラフィックを生成するネットワークを構築します。

攻撃者は、こうした攻撃ネットワークを構築するためにネットワーク上の脆弱な IoT デバイスを見つけ出します。脆弱なホストは通常、ウイルス対策ソフトウェアを実行していないか、古いソフトウェアを実行しているか、適切にパッチが適用されていません。そのため、脆弱なホストは、脆弱性を利用してそれらのホストにアクセスする攻撃者に悪用されてしまいます。次のステップとして、侵入者は攻撃ネットワークの侵害を受けたホストに攻撃ツールをインストールします。このような攻撃ツールを実行しているホストはゾンビと呼ばれ、攻撃者の制御下であらゆる攻撃を仕掛けることができます。多くのゾンビは、一体となっていわゆる軍隊を形成します。WAN の帯域飽和、ホスト数の増加、および UDP パケットの増加はいずれも、侵害を受けた組織に共通して見られる特徴です。

Stealthwatch は、DNS サーバやアプリケーション サーバを標的とし、DNS に依存する他のシステムで障害を発生させて事業運営を中断させる攻撃トラフィックを検出します。Stealthwatch では受け取ったコンテキストおよびフロー情報に基づく 94 を超える分析アルゴリズムを使用して脅威を検出し、修復することが可能です。これらのアルゴリズムは異常検出に使用されます。イベントはアラーム カテゴリにフィードされ生成できます。一部のセキュリティ イベントは、それ自体でアラームを生成することが可能です。アラームにより、アラーム テーブルでの通知や SIEM に対する syslog メッセージの生成といった関連する対応を行うことができます。

Cisco Stealthwatch は Network as a Sensor のシスコ検証済みデザイン（CVD）ガイドを使用して開発され、pxGrid は CA ベースの証明書を使用して ISE と通信できるように設定されました。

Cisco Network as a Sensor の設計ガイドについては、以下を参照してください。

https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Feb2017/CVD-NaaS-Stealthwatch-SLN-Threat-Visibility-Defense-Dep-Feb17.pdf

Stealthwatch のインストール ガイドについては、以下を参照してください。

https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/management_console/virtual/installation/guide/SW_6_9_0_SMC_VE_and_Flow_Collector_VE_Installation_and_Configuration_DV_1_4.pdf

67

ネットワーク デバイスにおける NetFlow エクスポートの有効化

このガイドでは、CPwE デザインガイドで利用される IoT ネットワーク アクセス デバイスと Cisco Catalyst 3650/3850 で NetFlow を有効にする方法、および Industrial Ethernet 4000/5000 スイッチで NetFlow Lite を有効にする方法について説明します。ISA 3000（ASA シリーズ）では、NetFlow ではなく Network Secure Event Logging（NSEL）を使用します。

他のデバイスで NetFlow を有効にする方法については、NetFlow の設定に関する Stealthwatch の Wiki ページ（https://www.cisco.com/c/ja_jp/products/security/stealthwatch/index.html）を参照してください。

ネットワーク スイッチの NetFlow

スイッチやルータで NetFlow を有効にするには、フロー レコード、フロー エクスポータ、およびフロー モニタという 3 つの要素が必要です。3 つすべてのコンポーネントの設定が完了したら、L2/L3 ポート、VLAN、WLAN（SSID）などの有線または無線インターフェイスにフロー モニタを適用します。

フロー レコード

フロー レコードは、フロー内のパケットやフローごとに収集されるカウンタのタイプなど、NetFlow のプロセスで収集する情報を定義します。カスタム フロー レコードは、発信 NetFlow レコードに含めるフィールドをシスコ デバイスに伝える一連の match および collect コマンドを指定します。

match フィールドは、フローの一意性を決定するために使用されることを意味するキー フィールドです。collect フィールドは、レポートと分析のためにコレクタに詳細を提供するためのレコードに含まれる追加情報です。フロー レコードを作成するときは、デバイスに入る（入力）、またはデバイスから出て行く（出力）すべてのフロー データ トラフィックを示すようデバイスに指示します。

コンフィギュレーション モードでは、適切なインターフェイス方向コマンドを使用して入出力フロー レコードを作成します。" match interface output" と " match interface output" は、入力フロー レコードで設定できません。また、同じフロー レコードでは、インターフェイスの入力とインターフェイスの出力の両方はサポートされません。1 つのフロー レコードでは、match および collect 要素に対して 1 つのインターフェイス方向（input/output）だけを設定します。

この設定には、Stealthwatch で必要なフロー レコード フィールドだけでなく、オプションのフロー レコード フィールドも含まれています。

すべてのデバイスが、これらのオプションすべての収集と送信をサポートしているわけではありません。

ステップ 1：入力レコードを作成します。

```
flow record StealthWatch-Record-IN
 description NetFlow record to StealthWatch
 match datalink mac source address input
 match datalink mac destination address input
 match ipv4 tos
 match ipv4 ttl
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 match transport source-port
 match transport destination-port
 match interface input
 match flow direction
 match flow cts source group-tag
 match flow cts destination group-tag
```

つ目次に戻る

```
 collect transport tcp flags
 collect counter bytes long
 collect counter packets long
 collect timestamp absolute first
 collect timestamp absolute last
```

ステップ 2：出力レコードを作成します。

```
flow record StealthWatch-Record-OUT
 description NetFlow record to StealthWatch
 match datalink mac source address output
 match datalink mac destination address output
 match ipv4 tos
 match ipv4 ttl
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 match transport source-port
 match transport destination-port
 match interface output
 match flow direction
 match flow cts source group-tag
 match flow cts destination group-tag
 collect transport tcp flags
 collect counter bytes long
 collect counter packets long
 collect timestamp absolute first
 collect timestamp absolute last
```

ラボで実装される Cisco Industrial Ethernet スイッチは、次のレコード要素をサポートしません。

```
 match ipv4 ttl
 match flow direction
 match flow cts source group-tag
 match flow cts destination group-tag
```

さらに、タイムスタンプ オプションでは、次のような別の構文が使用されます。

```
 collect timestamp sys-uptime first
 collect timestamp sys-uptime last
```

ネットワーク アドレス変換を実行するデバイスに関しては、次のコマンドを追加してそれらの置換を追跡します。

```
ip nat log translations flow-export v9 udp destination 10.9.10.32 2055
```

VLAN 情報を収集するために、ノンルーテッド インターフェイスの レコードに任意で match ステートメントを追加できます。

```
 match datalink vlan input/output
```

つ目次に戻る

フロー エクスポータ

フロー エクスポータは、NetFlow（フロー レコード）の送信場所と送信方法を定義します。実際には、フロー エクスポータはフロー コレクタの IP アドレスとポートを宛先として定義します。このケースでは、Stealthwatch フロー コレクタが宛先になっています。

ステップ 3：フロー エクスポータを作成します。

```
flow exporter StealthWatch-Exporter
 description StealthWatch Flow Exporter
 source Loopback0
 destination 10.9.10.32
 transport udp 2055
 option application-table
```

フロー モニタ

フロー モニタは、NetFlow キャッシュまたはキャッシュに保存されている情報について説明します。また、フロー モニタは、フロー レコードとフロー エクスポータをリンクさせます。フロー モニタには、エクスポートのタイマー、キャッシュのサイズ、および必要に応じて、パケットのサンプリング レート（サンプリングされた NetFlow や sFlow）などのさまざまなキャッシュ特性が含まれます。ネットワーク トラフィックがシスコ デバイスを通過するとき、フローは継続的に作成され追跡されます。フローが期限切れになると、NetFlow キャッシュから Stealthwatch フロー コレクタにエクスポートされます。フローが特定の時間にわたって非アクティブの場合（たとえば、新しいパケットがフローで受信されていない場合）、またはフローが長時間存続しており（アクティブな状態で）、アクティブ タイマーよりも長く存続している場合（たとえば、長時間の FTP ダウンロードが行われている場合）、フローはエクスポートの準備ができています。フローが非アクティブか長時間存続しているかどうかを指定するタイマーがあります。

ステップ 4：レコードとエクスポータを使用して入出力フロー モニタを作成します。

```
flow monitor StealthWatch-Monitor-IN
 description StealthWatch Ingress Flow Monitor
 exporter StealthWatch-Exporter
 cache timeout active 30
 cache timeout inactive 30
 record StealthWatch-Record-IN

flow monitor StealthWatch-Monitor-OUT
 description StealthWatch Egress Flow Monitor
 exporter StealthWatch-Exporter
 cache timeout active 30
 cache timeout inactive 30
 record StealthWatch-Record-OUT
```

フロー モニタを作成したら、さまざまなデバイスのインターフェイスに適用できます。ネットワークのトポロジと追跡したいフロー情報により、入力モニタ、出力モニタ、または両方のモニタを適用できます。

つ目次に戻る

ステップ 5：該当するインターフェイスにフロー モニタを適用します。

```
interface range GigabitEthernet1/1-16
 ip flow monitor StealthWatch-Monitor-IN input
 ip flow monitor StealthWatch-Monitor-OUT output
```

トラブルシューティング コマンド

スイッチから NetFlow データのトラブルシューティングを行ったり、NetFlow データを表示したりするための show および clear コマンドがいくつか用意されています。以下の検証コマンドは、入力（IN）フローに使用します。これらのコマンドは出力（OUT）トラフィックで繰り返すことが可能です。

NetFlow データを表示するコマンド：

```
show flow record StealthWatch-Record-IN
show flow monitor StealthWatch-Monitor-IN statistics
show flow monitor StealthWatch-Monitor-IN cache
show flow exporter StealthWatch-Exporter statistics
```

NetFlow データをリセットするコマンド：

```
clear flow record StealthWatch-Record-IN
clear flow monitor StealthWatch-Monitor-IN statistics
clear flow monitor StealthWatch-Monitor-IN cache
clear flow exporter StealthWatch-Exporter statistics
```

ネットワーク デバイスの SNMP

さらに、Stealthwatch で検出時に自動的にインターフェイス名を収集できるように SNMP を設定することが可能です。ベスト プラクティスとして、また今日のコンプライアンス義務に対応するために、SNMP v1 や v2 ではなく、v3 を実装する必要があります。

ステップ 1：Stealthwatch で設定したユーザ クレデンシャルに一致するように SNMP ユーザを設定します（通常のデバイス設定ではこのユーザは表示されません）。

```
snmp-server user V3User V3Group v3 auth sha Cisco1234 priv aes 128 Cisco1234
```

ステップ 2：ユーザが割り当てられているグループの権限を設定します。

```
snmp-server group V3Group v3 auth read V3Read write V3Write
```

ステップ 3：読み取り/書き込みアクセスの適切なビューを定義します。

```
snmp-server view V3Read iso included
snmp-server view V3Write iso included
```

つ目次に戻る

ステップ 4：アクセスに使用する管理コンソールとコレクタの IP アドレスを定義します。

```
snmp-server host 10.9.10.19 version 3 auth V3User
snmp-server host 10.9.10.31 version 3 auth V3User
snmp-server host 10.9.10.32 version 3 auth V3User
```

ネットワーク ファイアウォール フロー

ASA では、次の設定で Network Secure Event Logging（NSEL）を使用してフローがエクスポートされます。

ステップ 1：グローバルなフローのエクスポート先とテンプレートを設定します。

```
flow-export destination management 10.9.10.32 2055
flow-export template timeout-rate 5
flow-export delay flow-create 5
```

ステップ 2：対象のトラフィック フローを定義するアクセス リストを作成します。

```
access-list StealthWatch extended permit ip any any
```

ステップ 3：class-map を作成してアクセス リストを指定します。

```
class-map StealthWatch_Map
 match access-list StealthWatch
```

ステップ 4：グローバルポリシー（または必要に応じて別の既存のポリシー）にクラス マップを適用します。

```
policy-map global_policy
 class StealthWatch_Map
  flow-export event-type all destination 10.9.10.32
```

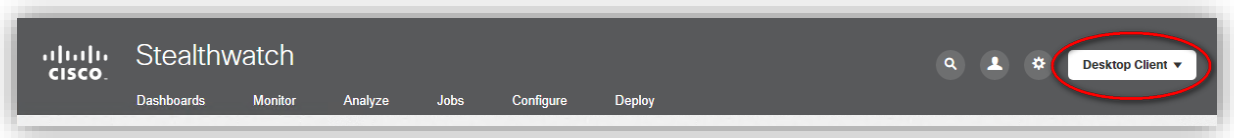
Cisco Stealthwatch のフロー収集

Stealthwatch コレクタに NetFlow を送信するようにデバイスを設定したら、Stealthwatch にそれらのフローを特定して分類し、ポリシーを作成する設定をさらに追加できます。

Cisco Stealthwatch エクスポータ

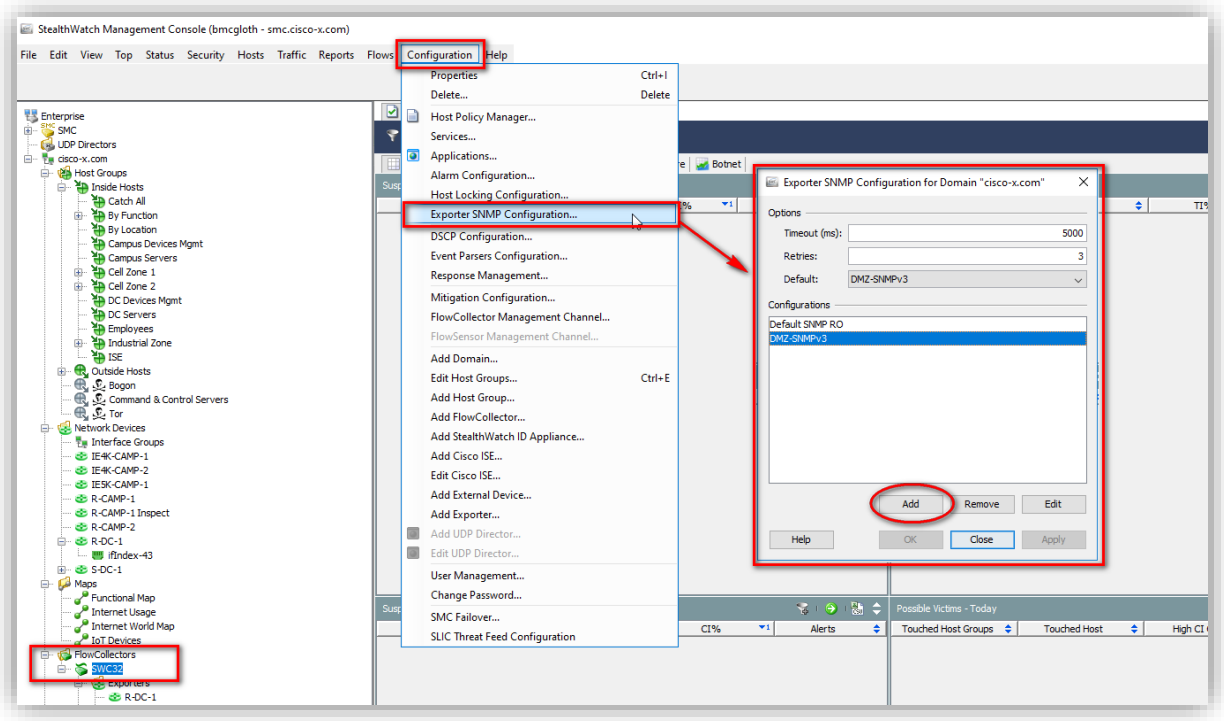
Stealthwatch にフローを送信するように設定した各デバイスは、エクスポータ インターフェイス ステータス テーブルに表示されます。エクスポータ リストにネットワーク デバイスを明示的に追加します。

ステップ 1：Stealthwatch の Java クライアントを起動してログインします。

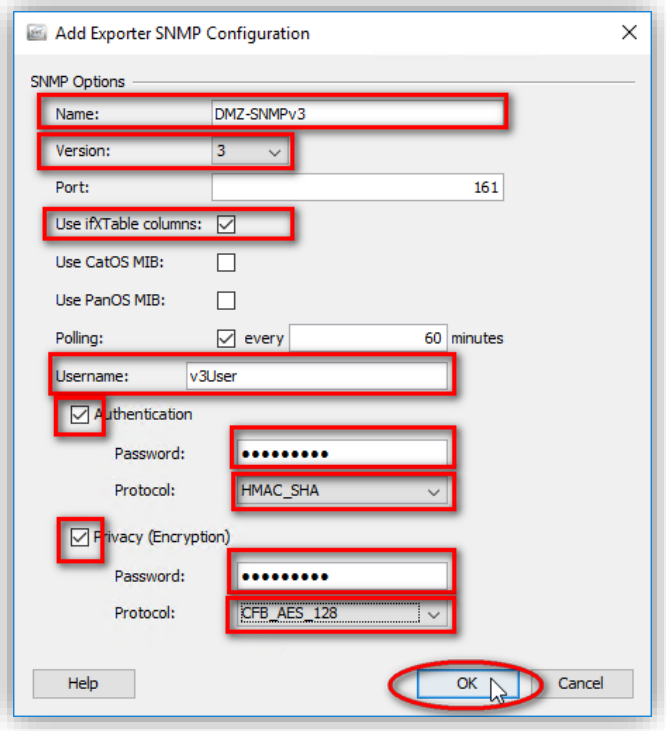


つ目次に戻る

ステップ 2：最初に新しいエクスポータ プロファイルに使用する SNMP エクスポータを追加します。Stealthwatch フロー コレクタを選択してから、メイン メニューで [設定（Configuration）] > [エクスポータの SNMP 設定（Exporter SNMP Configuration）] の順に選択します。ポップアップ メニューで [追加（Add）] をクリックします。

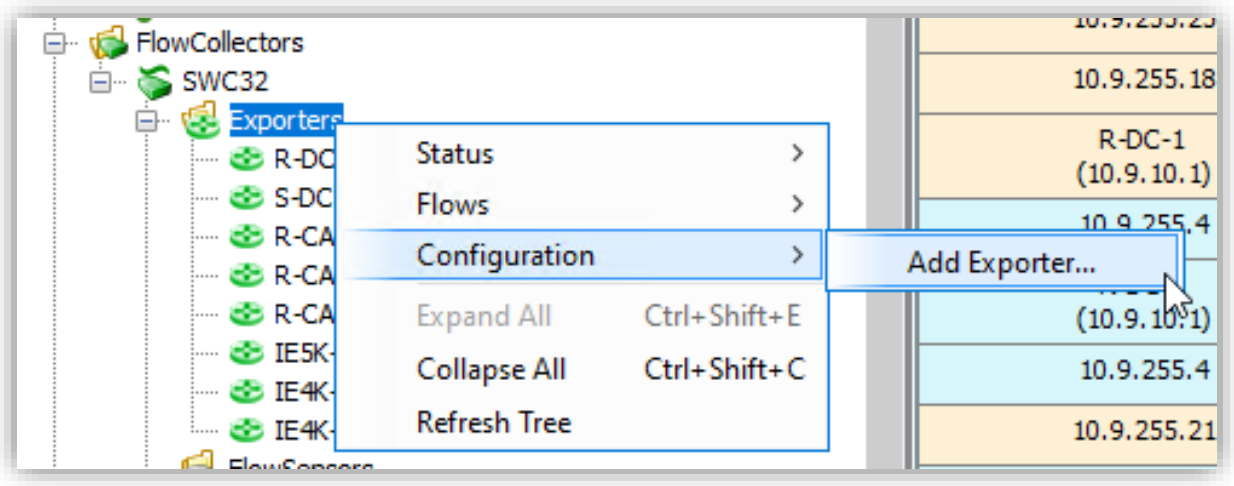


ステップ 3：ネットワーク デバイス用に作成された SNMP 設定を使用するように新しいエクスポータを設定します。[OK] をクリックしてから [閉じる（Close）] をクリックします。

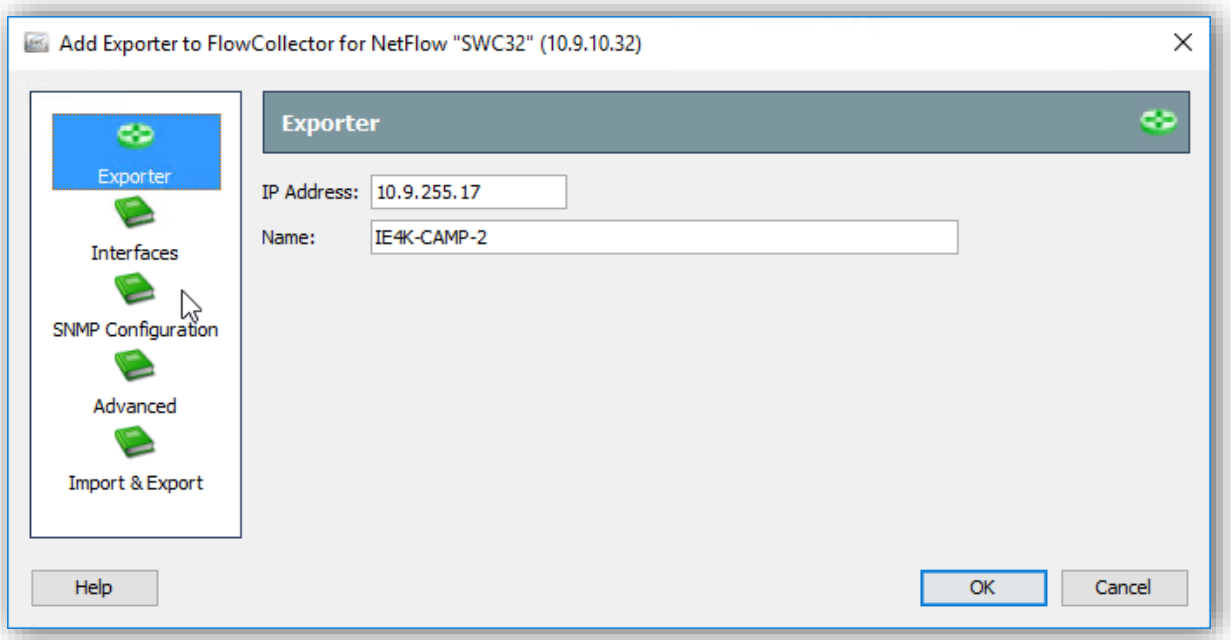


つ目次に戻る

ステップ 4：Stealthwatch フロー コレクタのフォルダを展開して [エクスポータ（Exporters）] フォルダを右クリックし、ポップアップ メニューで [設定（Configuration）] > [エクスポータの追加（Add Exporter）] の順に選択します。

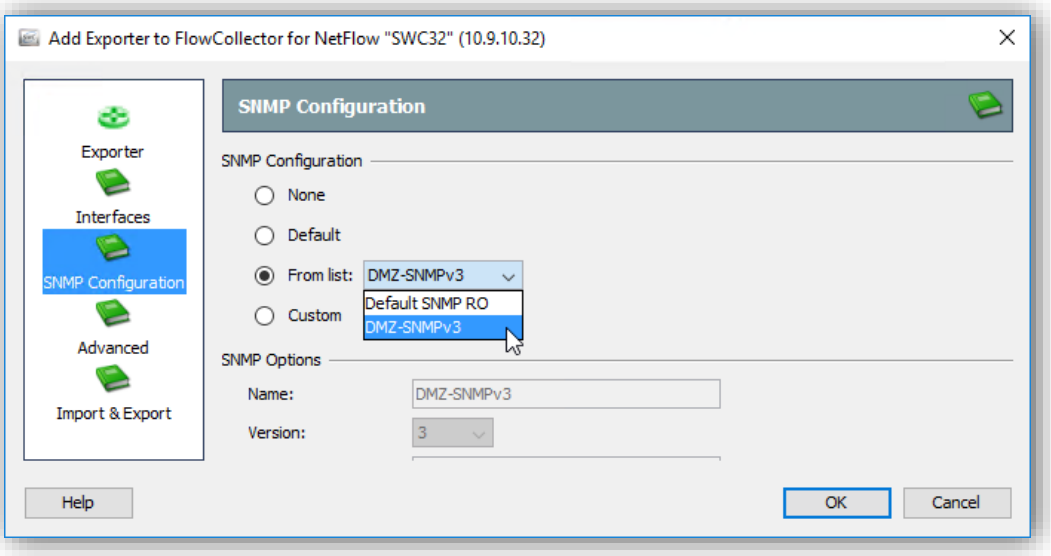


ステップ 5：デバイスで NetFlow の送信に使用する IP アドレスを設定し、デバイス名を追加します。



つ目次に戻る

ステップ 6：[SNMP 設定（SNMP Configuration）] アイコンを選択し、リストから SNMP 設定を選択して [OK] をクリックします。



Stealthwatch に NetFlow を送信するすべてのデバイスでステップ 4 ～ 6 を繰り返します。これらのステップが完了したら、以下のステップに従って Stealthwatch とネットワーク デバイスの通信チェックを実行します。

ステップ 7：[ドメイン名（Domain Name）] > [ホストグループ（Host Groups）] > [ネットワークデバイス（Network Devices）] に移動し、NetFlow を有効にしたすべてのネットワーク アクセス デバイスが表示されていることを確認します。

ステップ 8：フロー コレクタを展開し、NetFlow を有効にしたすべてのネットワーク アクセス デバイスが表示されていることを確認します。

ステップ 9：NetFlow のデータ収集を検証します。フロー コレクタを展開してフロー コレクタを右クリックし、[ステータス（Status）] > [NetFlow コレクションステータス（NetFlow Collection Status）] に移動します。[現在の NetFlow トラフィック（bps）（Current NetFlow Traffic (bps)）] でカウンタの増分を確認します。

ステップ 10：[フローコレクションステータス（Flow Collection Status）] テーブルのヘッダーを右クリックし、[最も長い継続時間のエクスポート（Longest Duration Export）] をクリックして列にフロー継続時間の関連付けを有効にします。

つ目次に戻る

Cisco Stealthwatch ホスト グループ

ホスト グループは、属性とポリシーを共有するホストまたは IP アドレスの「コンテナ」です。ホスト グループでは、さまざまなしきい値を設定したり、特定の動作に関するアラートをバイパスしたりできます。Stealthwatch システムでホスト グループを正しく使用すれば、イベントに関する警告が正しく行われ、より関連性の高い情報が提供されるようになります。一般的にグループ化される属性には、以下のようなものがあります。

- 機能を共有する。
- 同じような動作を示す。
- 1 つのオブジェクトとして管理できる。
- 1 つのポリシーを適用できる。
- 「所有」しているデバイスを特定する。

IoT システムでは、TrustSec SGT で使用するグループ分けのように、さまざまなセル ゾーンやその他の工場サービスをグループ分けします。IoT デバイスの動作がベースラインの動作やしきい値から外れると Stealthwatch でアラートが生成されますが、ホスト グループを使用すれば、その他のノイズを確実に減らすことができます。

Stealthwatch には、使用可能ないくつかのホスト グループが組み込まれています。また、独自のホスト グループを定義することも可能です。

- Catch All：すべての RFC 1918 アドレス、プライベート アドレス、およびパブリック IP アドレスが含まれています。別のホスト グループに追加した IP アドレスは、[Catch All] コンテナから削除されます。プライベート IP アドレスがまだ別のホスト グループに割り当てられていない場合の最終手段となるホスト グループです。
- By Function：このホスト グループには、事前定義済みのロール ポリシーがあるいくつかのサブグループが含まれています。サブグループには、以下のようなものがあります。
    - プロキシ
    - NAT ゲートウェイ
    - クライアント IP 範囲（DHCP 範囲）
        - エンド ユーザ デバイス
        - ゲスト無線ネットワーク
        - リモート VPN IP プール
        - 信頼できる無線
    - DMZ
    - ネットワークスキャナ
    - その他
        - ブロードキャスト
        - リンクローカルは
        - ローカルホスト
        - マルチキャスト
    - サーバ
        - ウイルス対策サーバ
        - バックアップ サーバ
        - BigFix
        - 機密サーバ
        - データベース サーバ
        - DHCP サーバ
        - DNS サーバ

つ目次に戻る

- ドメイン コントローラ
- ファイル サーバ
- メール サーバ
- 多機能
- NTP サーバ
- SMS サーバ
- ターミナル サーバ
- Web サーバ

o VoIP

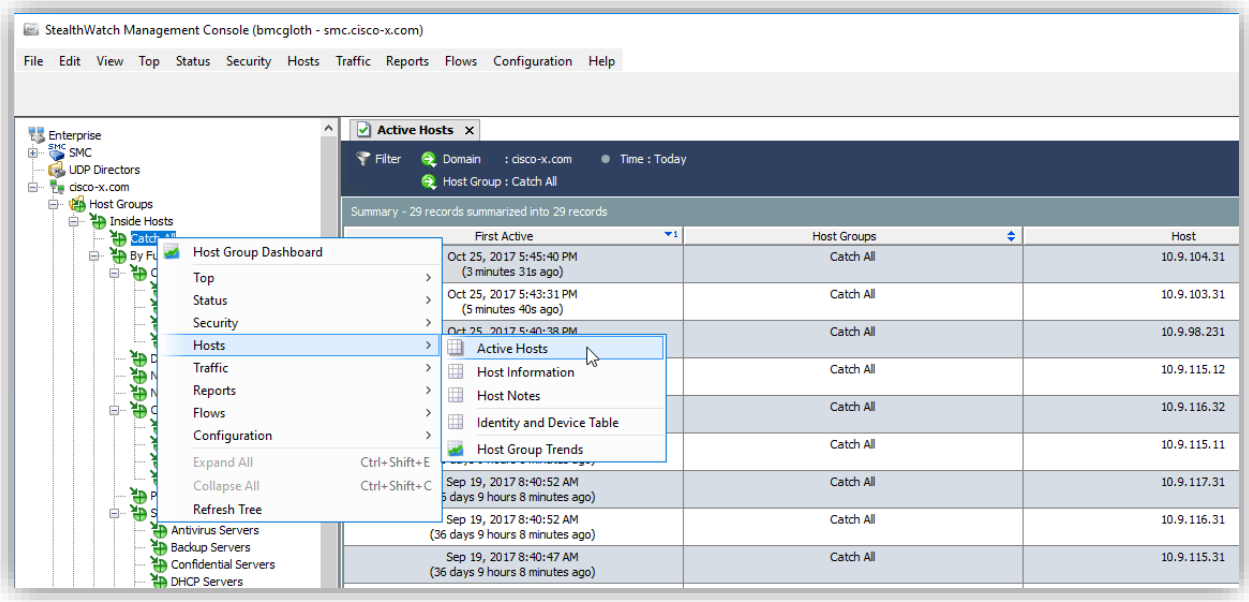
- VoIP エンドポイント
- VoIP ゲートウェイ

- By Location：ロケーション別にデバイスをグループ化しなければならない場合があります。各ロケーションには、それぞれに固有の DNS サーバや類似のデバイス タイプを含めることができます。
- Outside Hosts：ネットワークの一部ではないとみなされたすべてのホスト（基本的にはインターネット）が含まれます。
- Command & Control Servers：StealthWatch Labs Intelligence Center（SLIC）のライセンスがある場合にのみ使用できます。このホスト グループには、到達してはならない既知の悪意のあるホストが含まれており、接続を試行するホストが見つかると、間違いなくアラートが生成されます。

ホスト グループの定義と管理は Stealthwatch の Java クライアントで行われ、情報は Stealthwatch の Web インターフェイスでグループごとに表示できます。ホストは適切なグループに手動で割り当てる必要があります。特定のホスト グループに含まれるホストを表示するには、以下のステップを実行します。

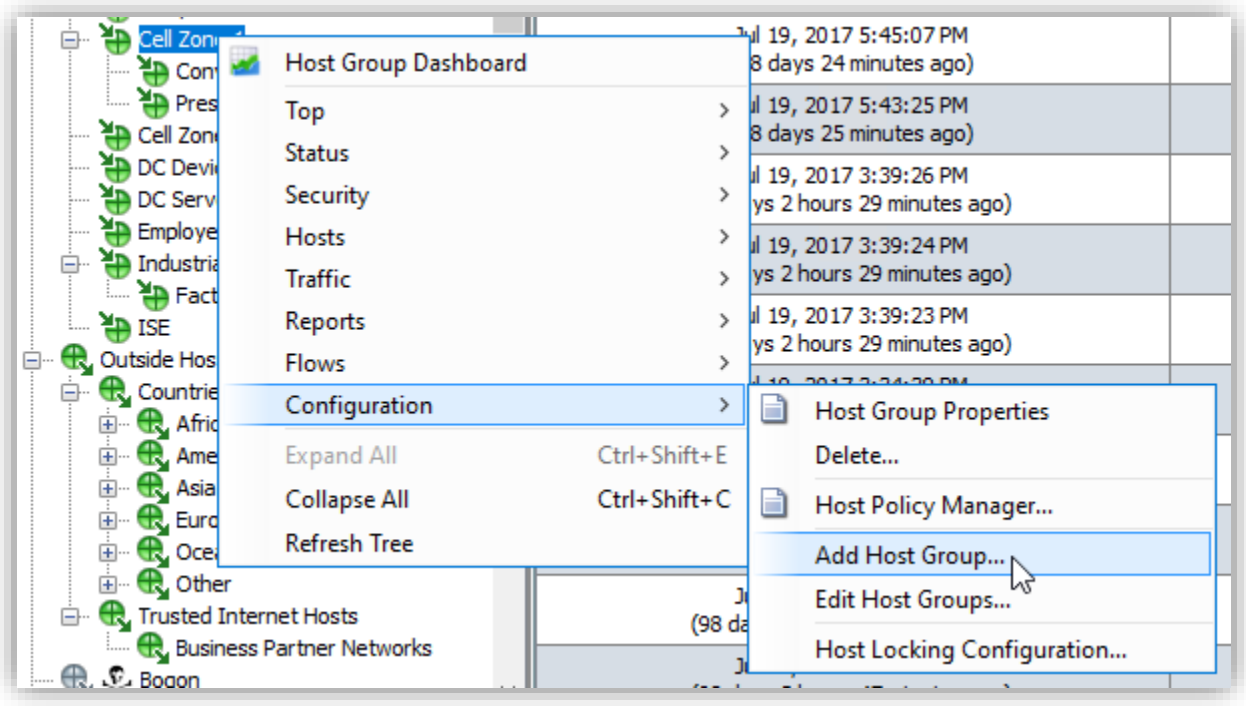
ステップ 1：Stealthwatch の Java クライアントを起動してログインします。

ステップ 2：ホスト グループをハイライトして右クリックし、メニューで [ホスト（Hosts）] > [アクティブホスト（Active Hosts）] に移動してホスト グループのアクティブ ホストを表示します。

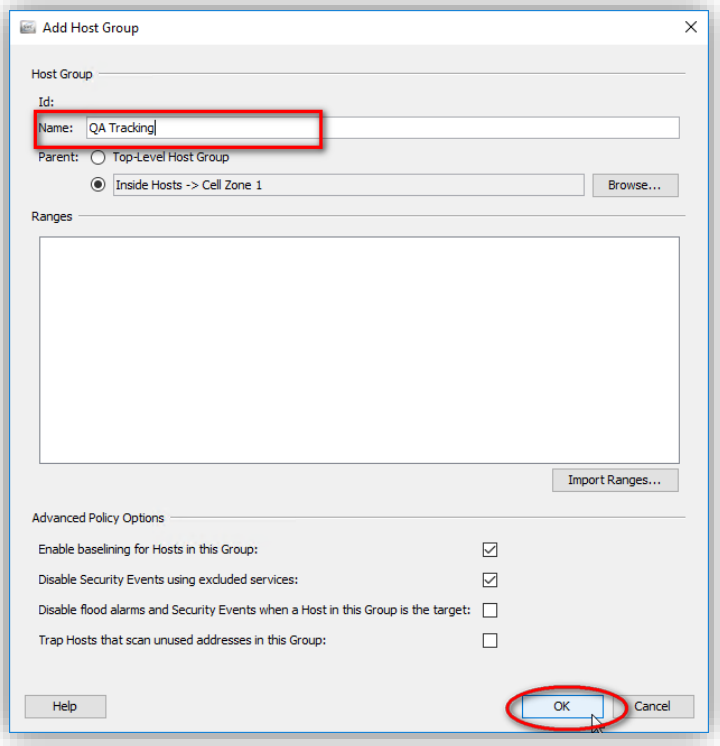


つ目次に戻る

ステップ 3：新しいホスト グループを作成するには、既存のグループをハイライトして右クリックし、[設定（Configuration）] > [ホストグループの追加（Add Host Group...）] に移動します。

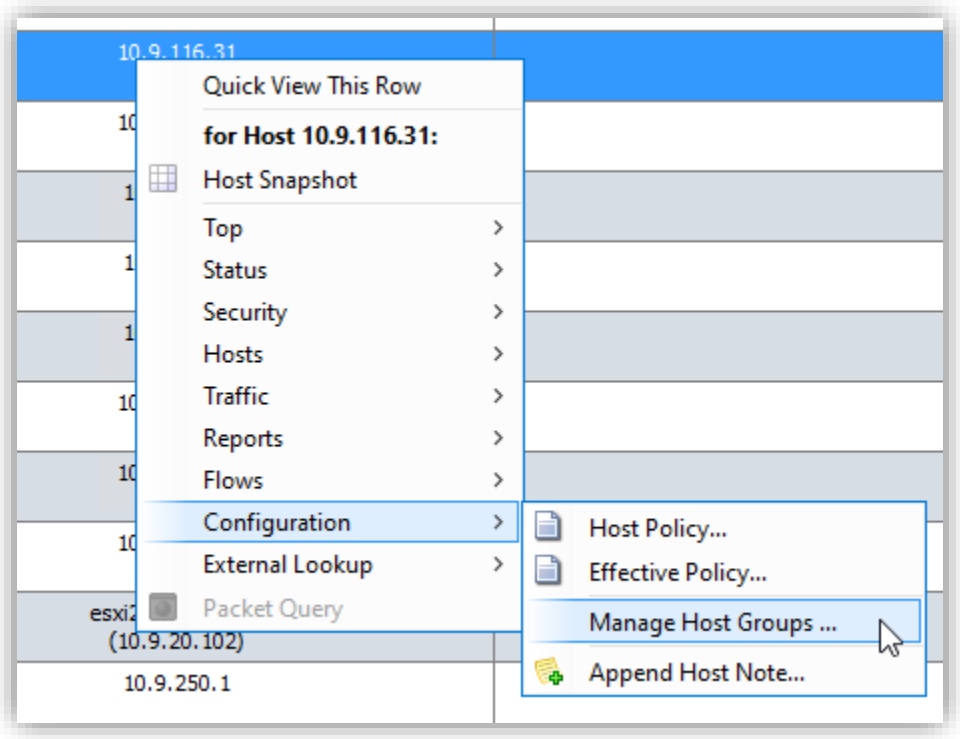


ステップ 4：名前を割り当てて [OK] をクリックします。

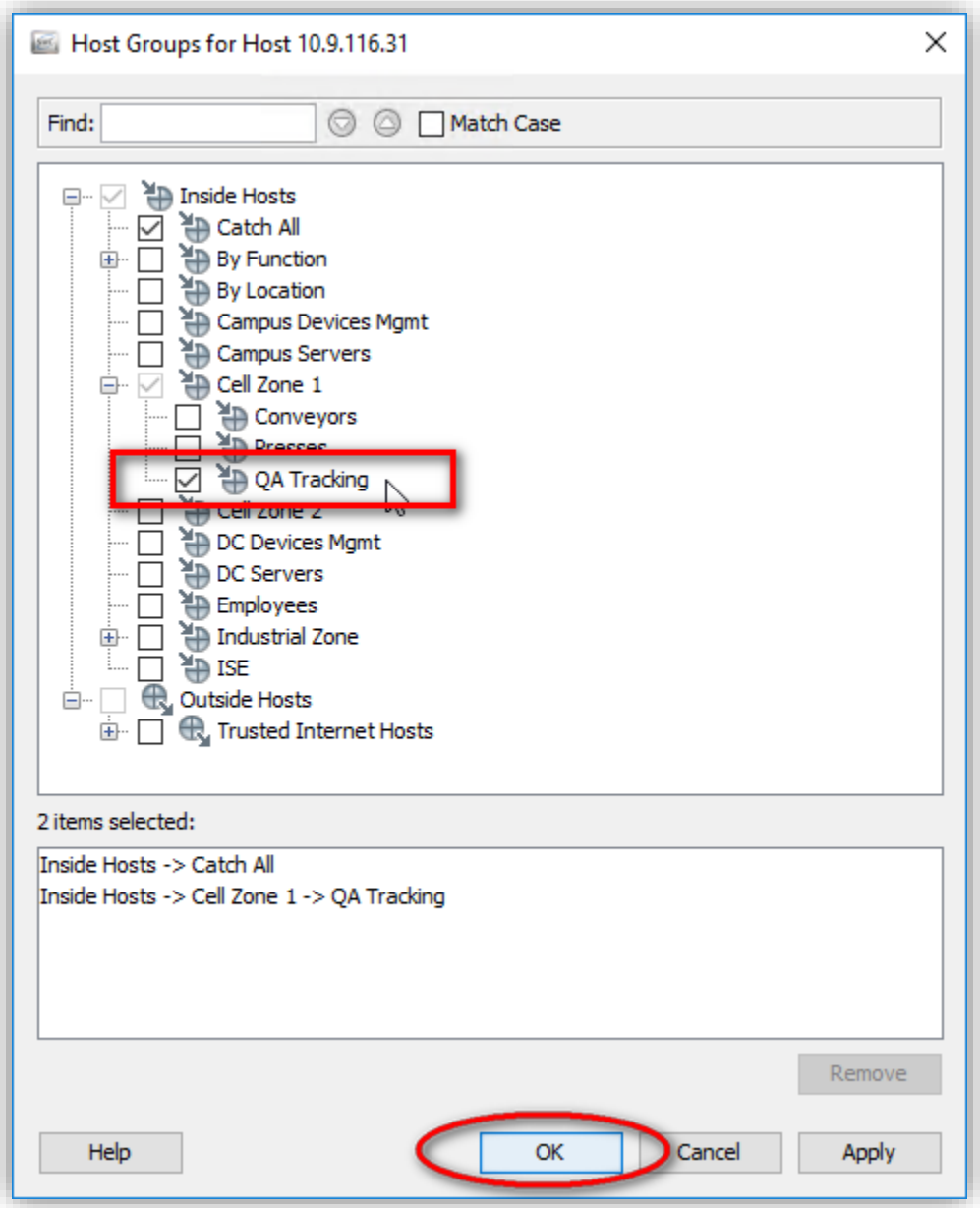


つ目次に戻る

ステップ 5：ホストを別のホスト グループに移動するには、[アクティブホスト（Active Hosts）] テーブルの IP をハイライトして右クリックし、[設定（Configuration）] > [ホストグループの管理（Manage Host Groups...）] に移動します。



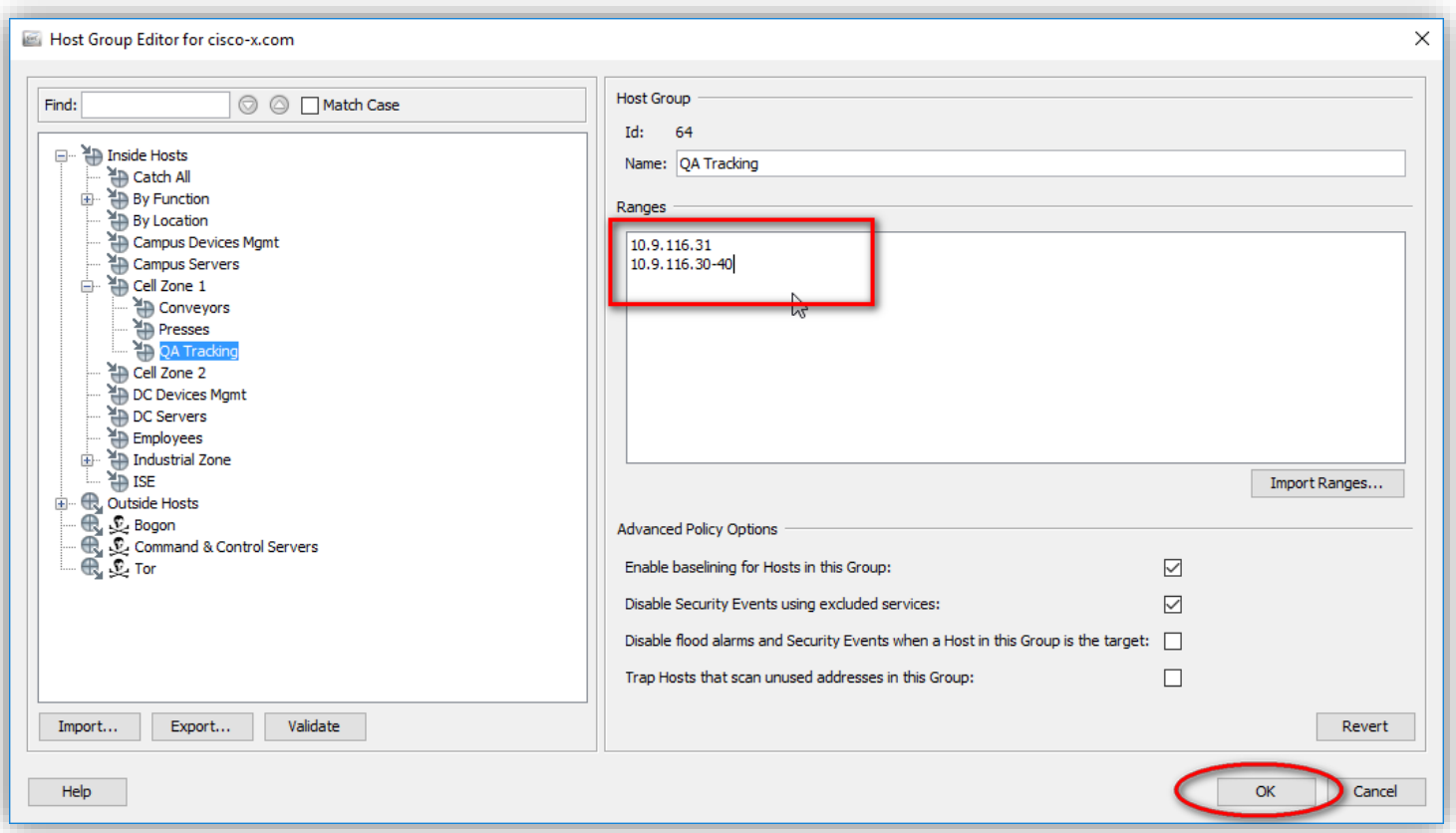
ステップ 6：ポップアップでデバイスを割り当てる新しいホスト グループを選択し、[OK] をクリックします。ホストは、1 つ以上のホスト グループのメンバーにすることができます。



グループにホストを静的に割り当てるだけでなく、ホスト グループで IP アドレスの範囲を定義すれば、より簡単に分類が行えます。これは産業用 IoT システムで有効です。多くの産業用 IoT システムは、DHCP ではなく静的 IP アドレスを使用して展開されているか、セグメンテーションに TrustSec が使用されていない場合に特定の VLAN で DHCP 範囲を使用するためです。

つ目次に戻る

ステップ 7：ホスト グループに範囲を割り当ててから、ホスト グループをハイライトして右クリックし、メインメニューで [設定（Configuration）] > [ホストグループの編集（Edit Host Group）] に移動します。デバイスの IP アドレス、アドレスの範囲、またはサブネットを追加します。完了したら [OK] をクリックします。

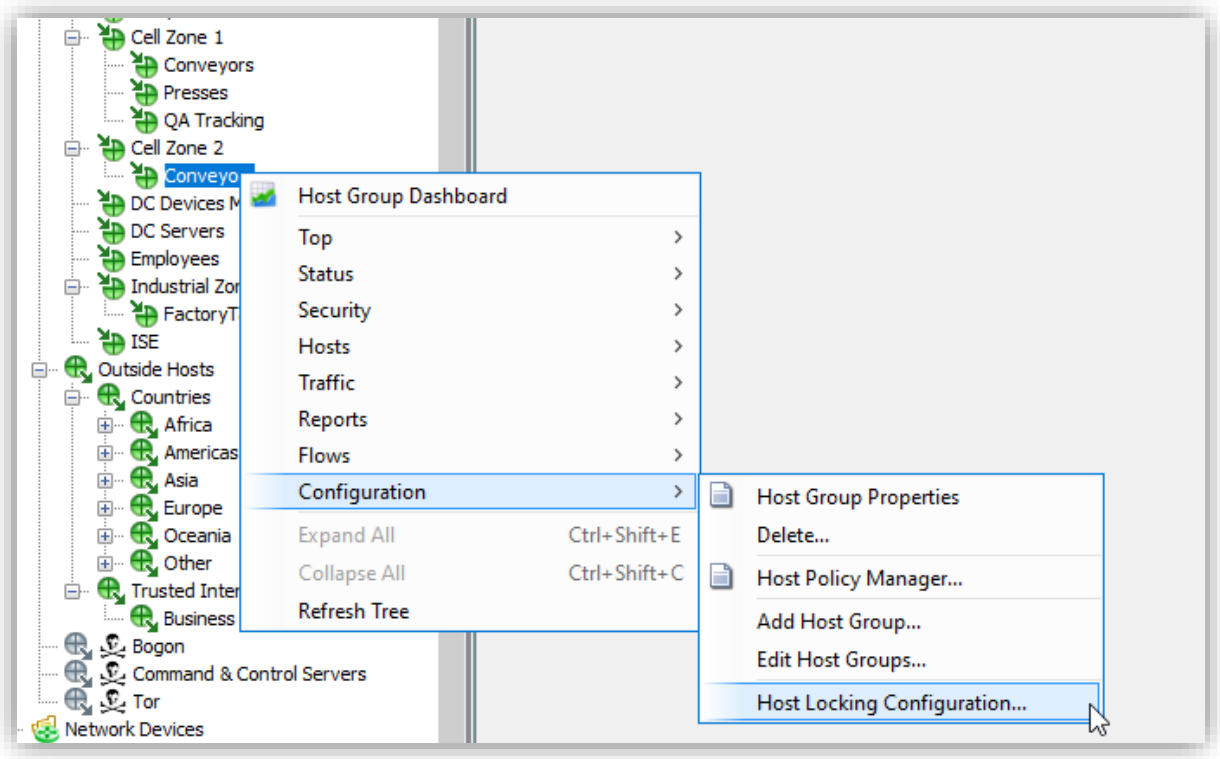


つ目次に戻る

これで関連するホスト グループの定義、およびホスト グループへのデバイスと IP 範囲の割り当てが完了し、ホスト ポリシーを更新して新しいロック ポリシーを指定できるようになります。これらのポリシーにより、展開したデバイスやプロトコルに固有のネットワークにおけるその他の異常を検出するのに必要な可視性が得られます。

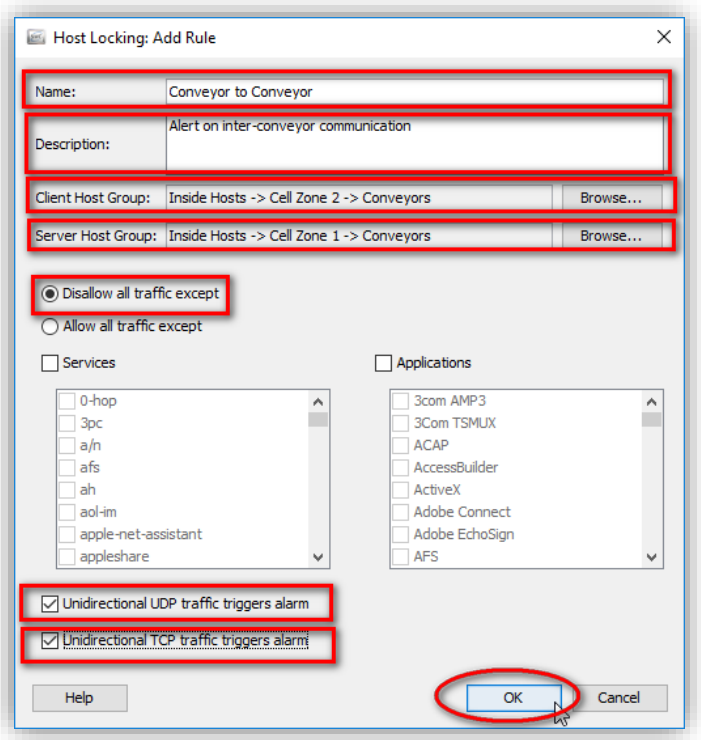
この例では、セル ゾーン 1 の PLC がセル ゾーン 2 のコンベヤ システムとやり取りすることはありません。これら 2 つのホスト グループに互いに通信させないホスト ロック ポリシーを作成した場合、それらの間で通信が行われると Stealthwatch でアラームが生成されます。このようにしてセキュリティ制御とセグメンテーションを正しく機能させるための可視性とアラートが提供されます。

ステップ 8：ホスト グループをハイライトして右クリックし、[設定（Configuration）] > [ホストロック設定（Host Locking Configuration）] に移動します。



つ目次に戻る

ステップ 9：表示されたポップアップ ウィンドウで [追加（Add）] をクリックし、適切な名前と説明を入力します。 ホスト グループと許可しないトラフィックを選択し、アラートを有効にして [OK] をクリックします。



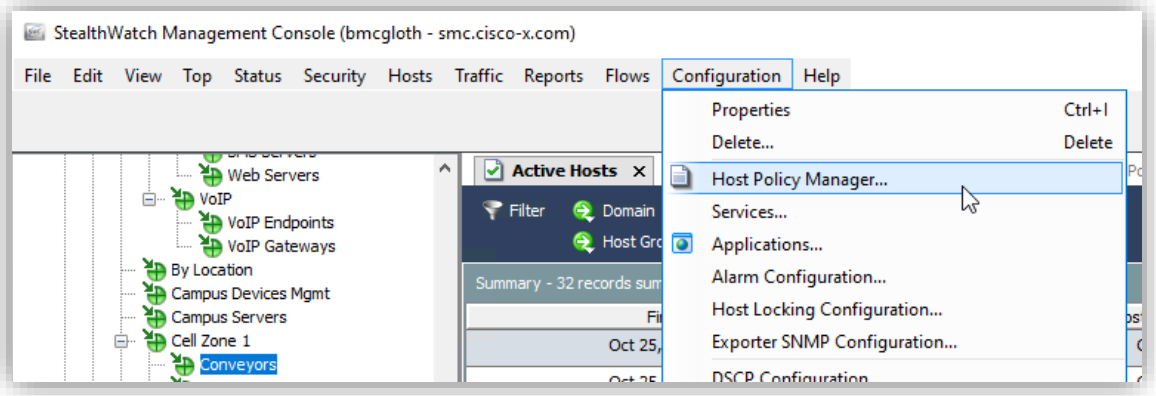
つ目次に戻る

[ホスト ポリシー マネージャ（Host Policy Manager）] ダイアログで、次のセクションを使用し、ポリシーを設定できます。

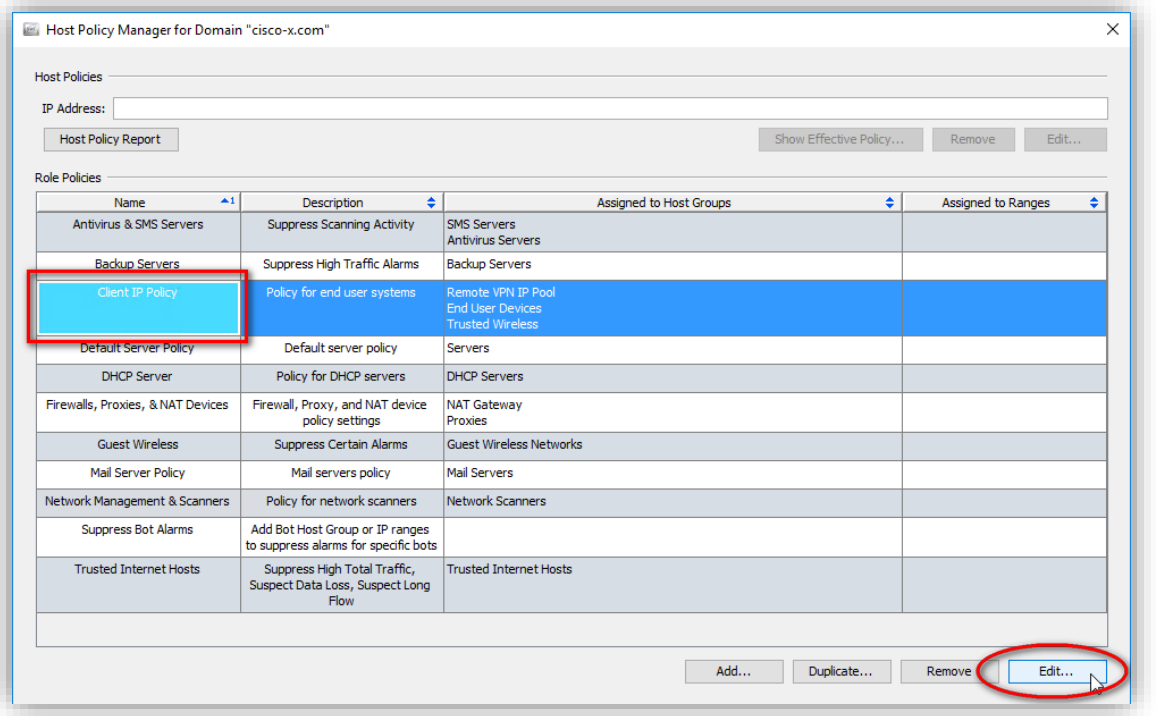
- [ホストポリシー（Host Policies）]：単一のホストのポリシーを管理できます。
- [ロールポリシー（Role Policies）]：システム内で実行するロールに従って、ホストのポリシーを管理できます。
- [デフォルトポリシー（Default Policies）]：内部ホストまたは外部ホストのデフォルト ポリシーを管理できます。

特定のホストに適用されるポリシーを判別する際、SMC は初めにデフォルト ポリシーを適用し、次に適用可能な 1 つ以上のロール ポリシーを適用して、最後にホスト ポリシー（ある場合）を適用します。ホストに複数のロール ポリシーが適用される場合、SMC はそれぞれのアラームについて、ホストに適用されたポリシーで使用されているポリシー設定を判断します。

ステップ 10：既存のポリシーに IoT ホスト グループを追加します。ホスト グループを選択します。メインメニューで [設定（Configuration）] > [ホストポリシーマネージャ（Host Policy Manager...）] の順に選択します。

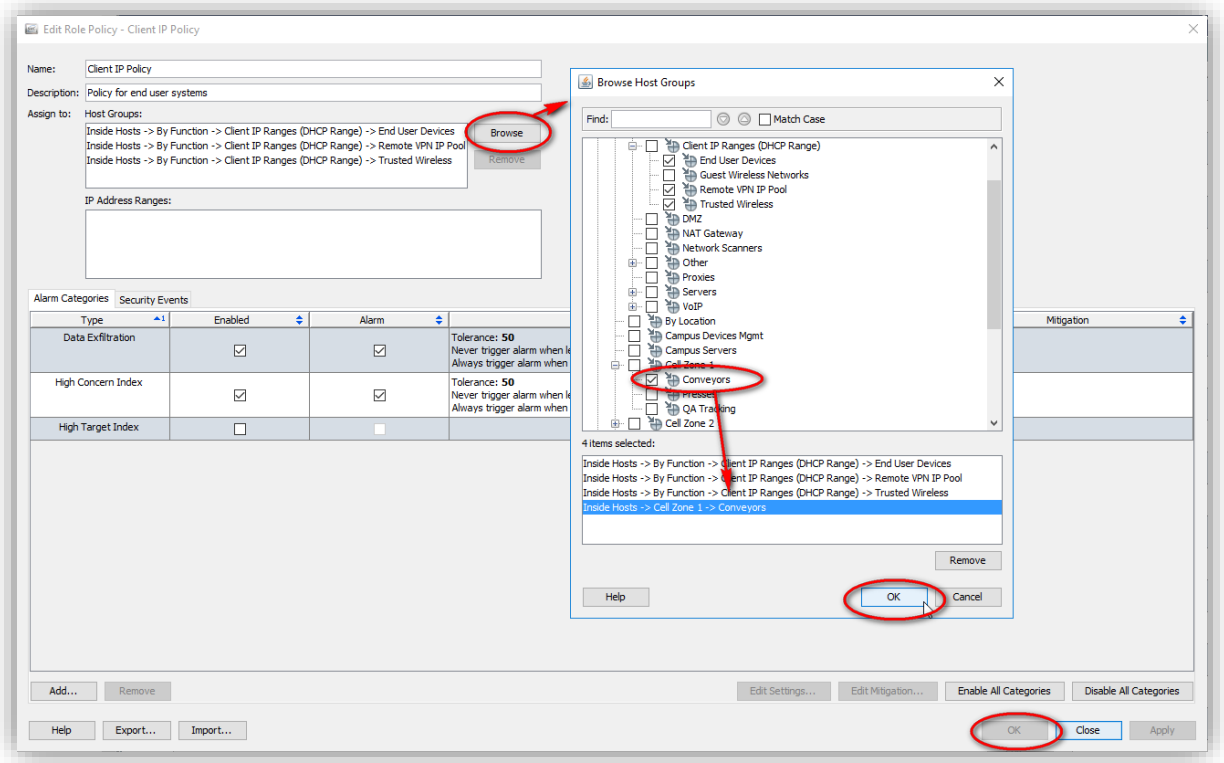


ステップ 11：クライアント IP ポリシーを選択し、[編集（Edit）] をクリックします。



ら目次に戻る

ステップ 12：ポリシーにセル ゾーン 1 のホスト グループ [Conveyors] を追加します。[OK]、[OK]、[閉じる（Close）] の順にクリックします。



組織に適した新しいポリシーを作成し、ホスト グループに適用します。

つ目次に戻る

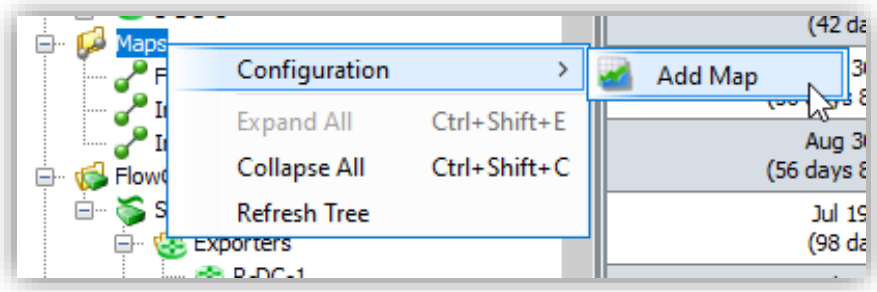
85

Cisco Stealthwatch マップ

SMC のマップ機能により、ドラッグアンドドロップ機能を使用してホスト グループをマップに追加してからそれらを接続し、ホスト グループ関係を作成できます。その後、マップには、ホスト グループのステータスが表示され、アクティブなアラームやトラフィックの帯域幅などのライブ データが示されます。さらにイメージ、線、テキスト ボックスを追加することで、環境を視覚的に表示できます。フィルタを使用してドメインやマップを変更できます。この機能を活用して、システム全体の状態をほぼリアルタイムで視覚的にモニタできます。

既存のマップを開くと、デフォルトでビュー モードが表示されます。ビュー モードでは、マップとすべての関連ステータス情報を表示することができます。マップを編集した後に保存すると、SMC は、Stealthwatch フロー コレクタにホスト グループ関係情報を送信します。マップがアクティブになり、1 分ごとに更新が開始されます。ここで IoT システムの新しいマップを追加します。

ステップ 1：エンタープライズ ツリーの [マップ（Maps）] ノードを右クリックします。ポップアップ メニューで [設定（Configuration）] > [マップの追加（Add Map）] の順に選択します。



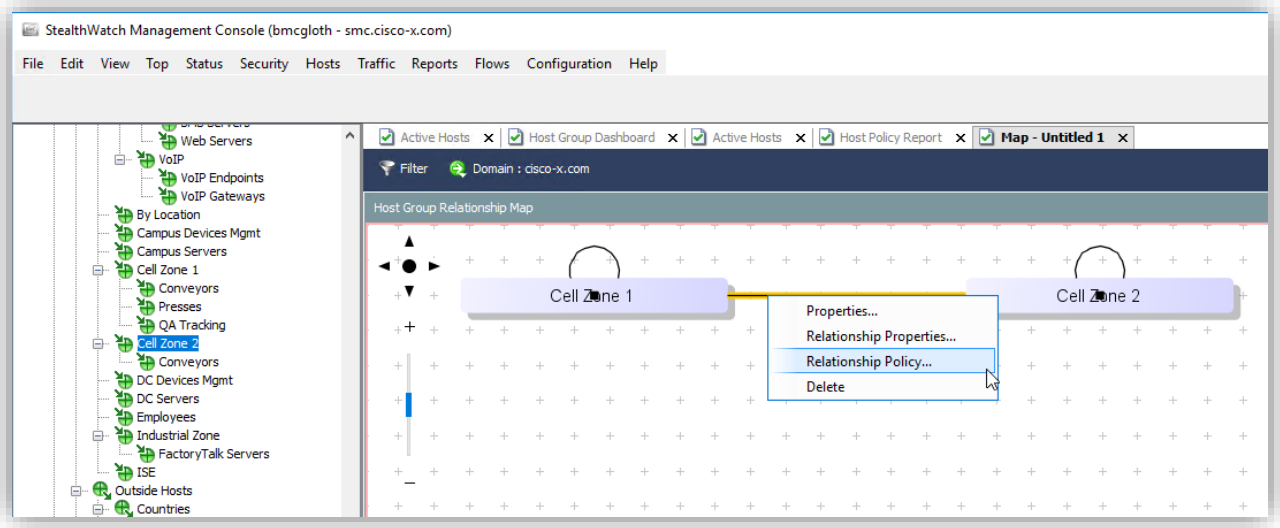
マップは新しいドキュメントとして表示されます。これで、カテゴリを設定する準備が整いました。

ステップ 2：マウスの左ボタンを使用して、目的のホスト グループをエンタープライズ ツリーからマップにドラッグ アンド ドロップします。

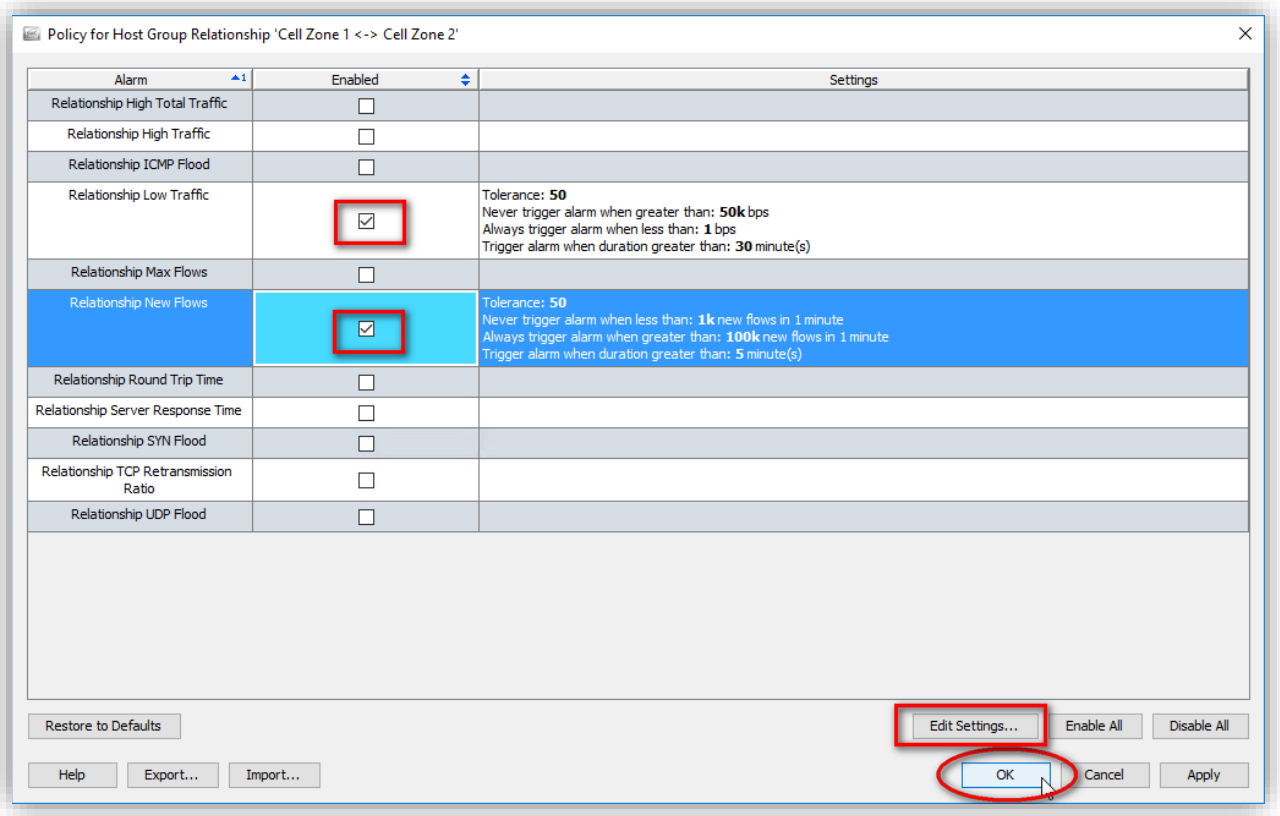
ステップ 3：マップ上のホスト グループ間の関係を作成します。これを行うには、マウスの左ボタンを使用して、1 つのホスト グループからもう 1 つのホスト グループに線を引きます。ホスト グループ内のトラフィックをモニタする場合、開始した同じホスト グループに戻るように線を引きます。

つ目次に戻る

ステップ 4：マウスの左ボタンでグループ間に引いた線を選択してグループ関係にポリシーを追加し、右クリックして [関係ポリシー（Relationship Policy）] を選択します。

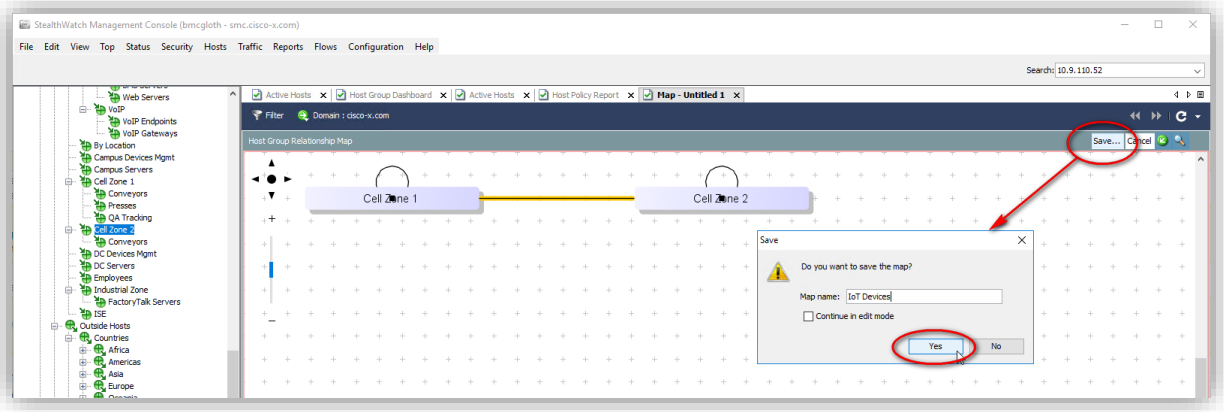


ステップ 5：目的のポリシーを有効にし、必要に応じて設定を編集します。[OK] をクリックしてマップを適用します。

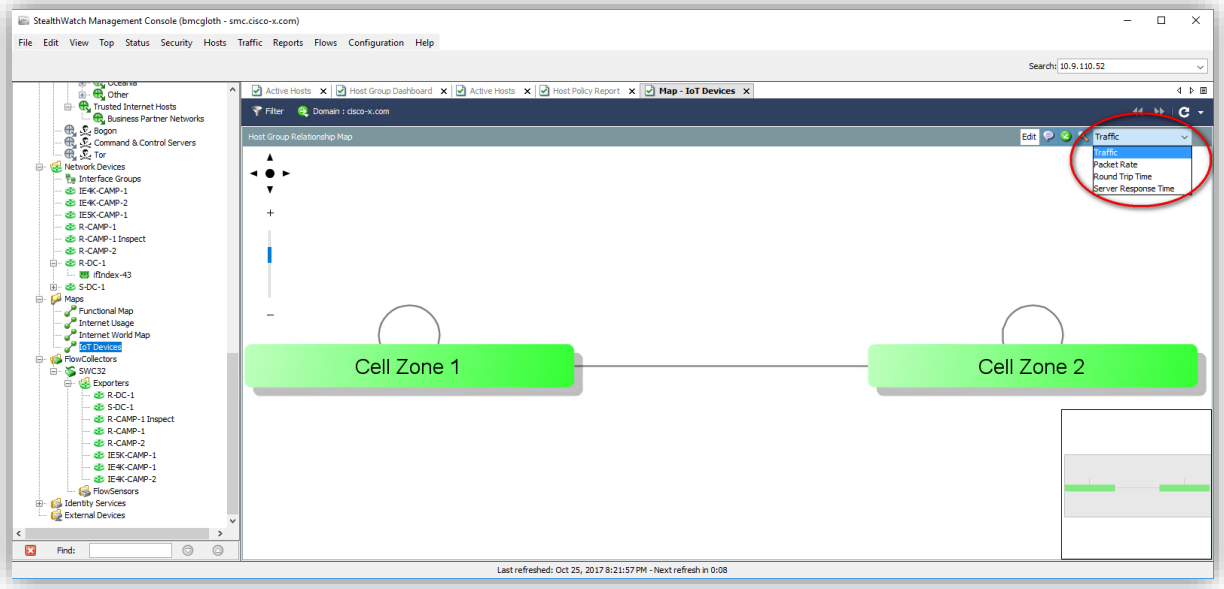


つ目次に戻る

ステップ 6：マップのカスタマイズが完了したら、マップの右上隅にある [保存（Save）] ボタンをクリックし、[マップ名（Map name）] を入力して [はい（Yes）] をクリックします。



SMC はマップを保存し、即座に有効になります。右上隅のドロップダウンを選択すれば、その他の情報を表示できます。



つ目次に戻る

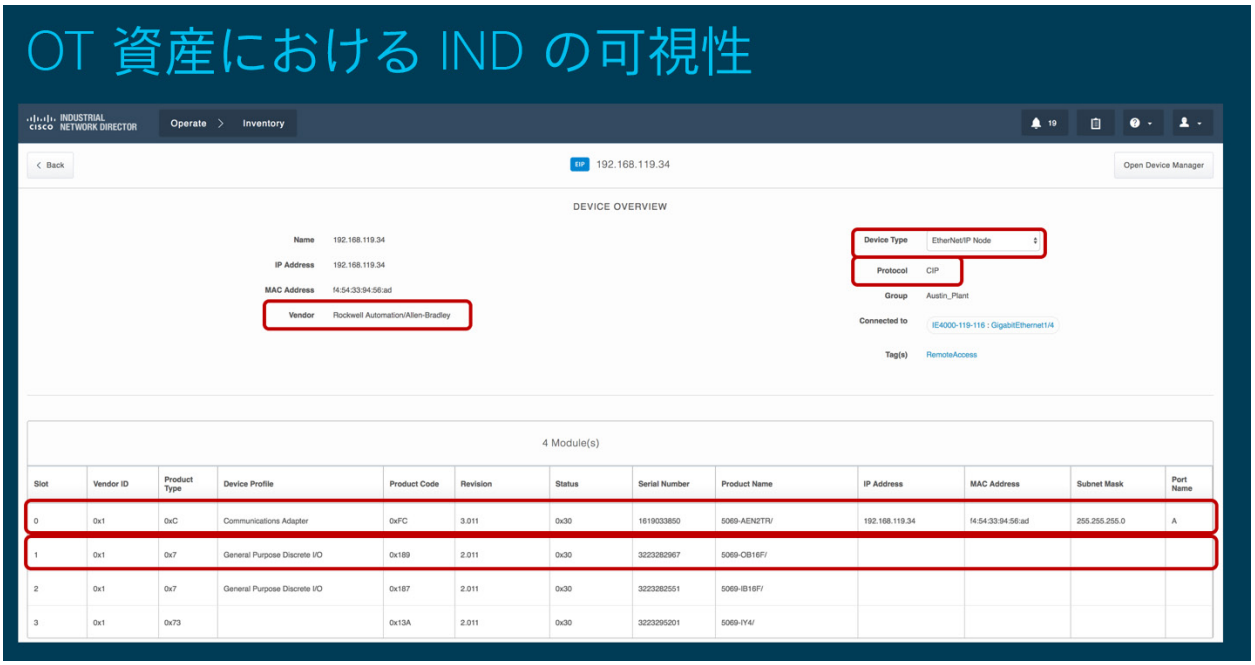
Industrial Network Director

産業用ネットワークの管理に特化したプラットフォームである Cisco Industrial Network Director は、運用チームが自動化プロセスに関してネットワークとオートメーション デバイスを詳細に把握できるように設計されており、システムの可用性とパフォーマンスを向上させることで総合設備効率（OEE）を高めます。産業用イーサネット ネットワークの管理機能を搭載する Industrial Network Director では、PLC、IO、RTU デバイスなどの OT エンドポイントも検出できます。IND は、ネイティブの通信プロトコルで通信を行ってこれらのデバイスを検出します。IND は、次の産業用プロトコルで通信する OT エンドポイントの検出をサポートしています。

- CIP（Common Industrial Protocol）
- Profinet
- BACNet
- Modbus

Cisco IND は OT エンドポイントから属性を収集し、以下の図に示すような OT 資産に対する可視性を提供します。IND では、ベンダー、通信、プロトコル、製品名、シリアル番号、デバイス タイプ（PLC や I/O などの場合）といった資産情報を表示できます。

図 17：IND の属性



つ目次に戻る

89
Cisco Industrial Network Director（IND）と Cisco Identity Services Engine（ISE）の統合

IND と ISE は、pxGrid（Platform Exchange Grid）を使用して統合されます。IND は図 *18* に示すように pxGrid パブリッシャとして機能する OT 資産の属性の送信元であり、ISE は図 *19* に示すように pxGrid サブスクライバとしてこれらの属性を受け取ります。

図 18：IND pxGrid サーバ/ISE の設定

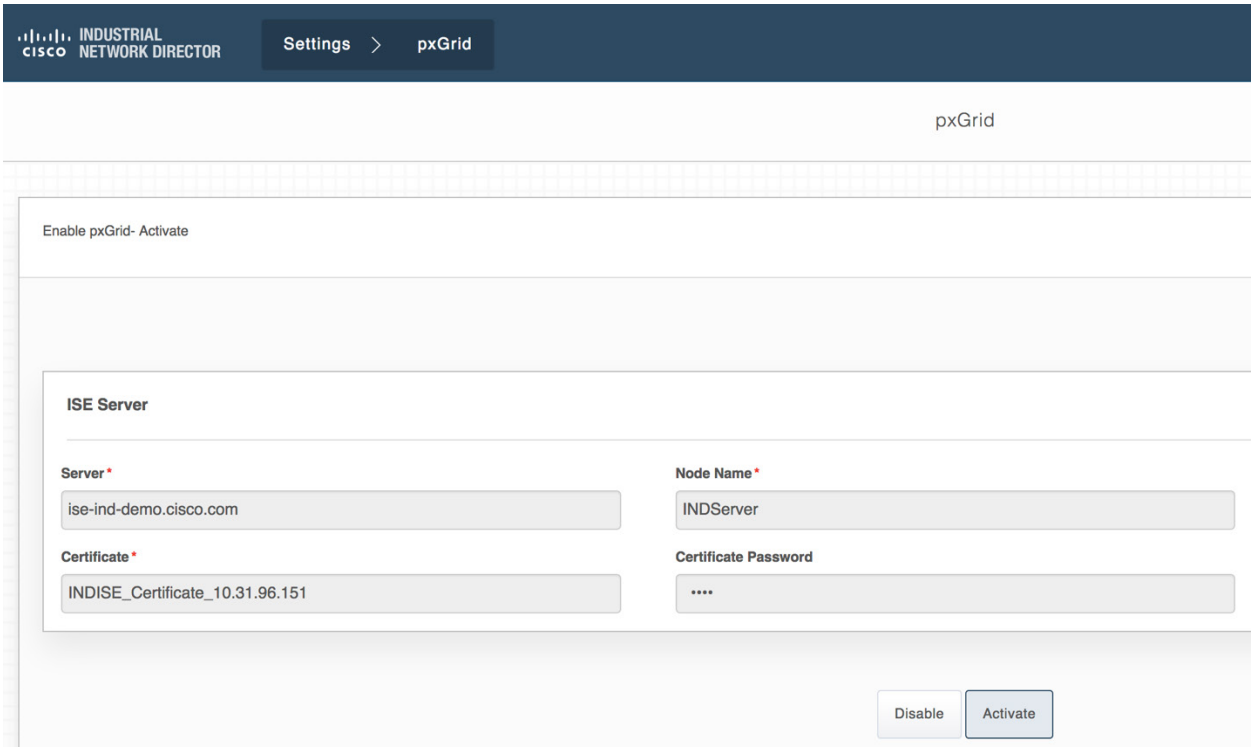
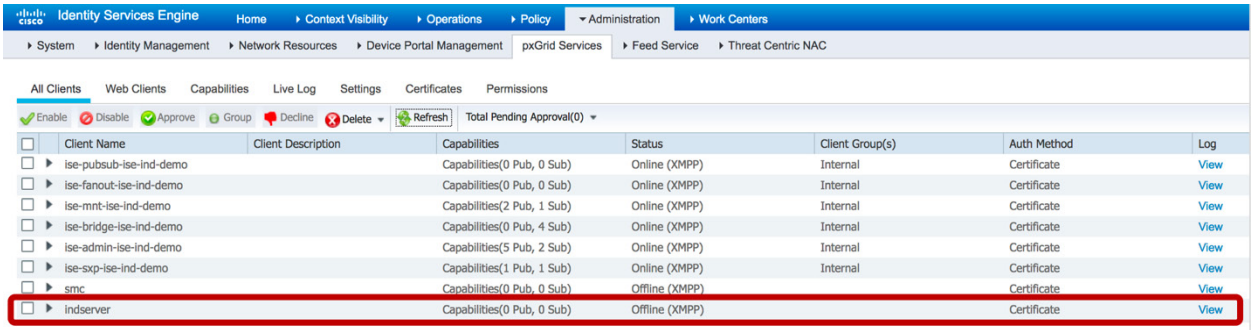


図 19：pxGrid パブリッシャとして登録された IND

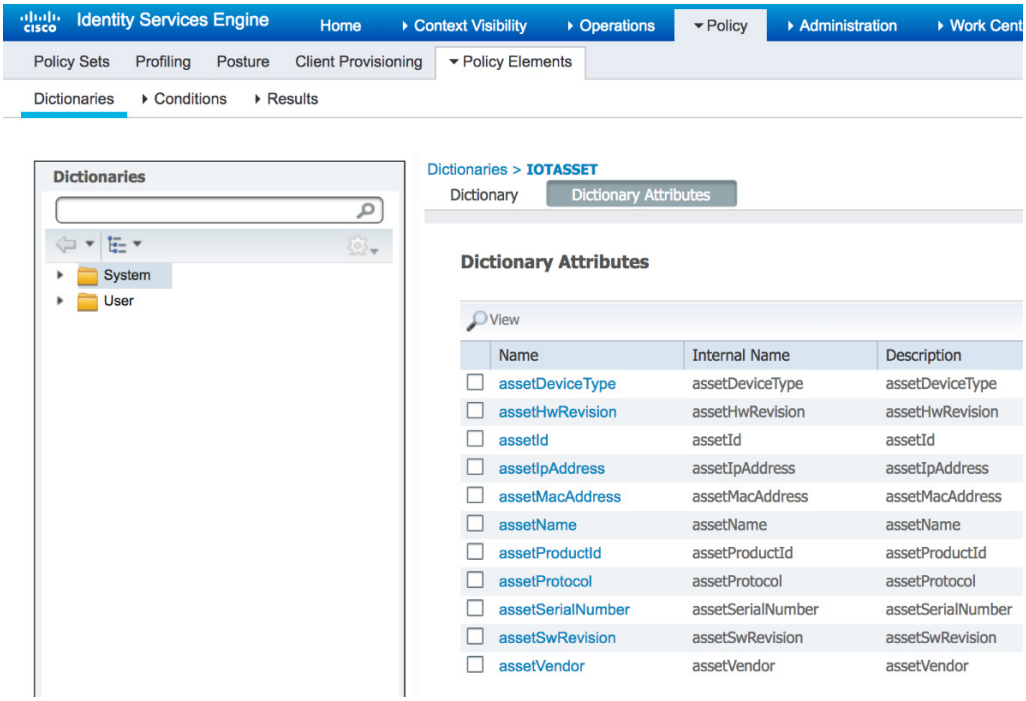


つ目次に戻る

90
IOTASSET ディクショナリ

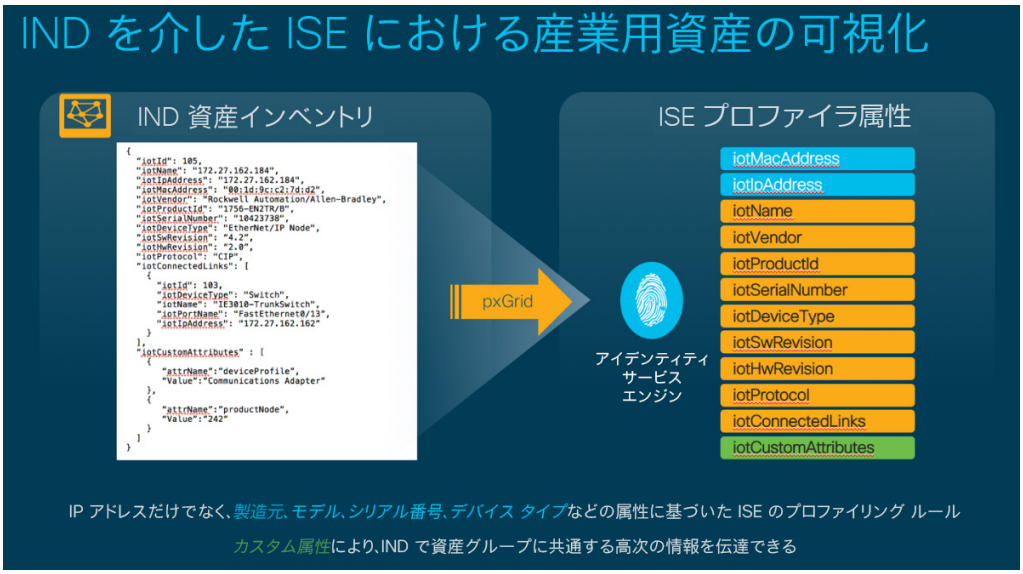
Cisco IND は、pxGrid（Platform Exchange Grid）を使用して OT 資産のコンテキスト情報を共有します。IND から OT 資産の情報を受け取るために、ISE で新しい「IOTASSET」ディクショナリが作成されます。以下の *図 20* に OT 資産に固有の IOTASSET ディクショナリと属性を示します。

図 20：IOTASSET ディクショナリ属性



IOTASSET ディクショナリ属性を使用すれば、（スイッチやファイアウォールなどの）ネットワーク インフラストラクチャに適切かつ安全なアクセス ポリシーをプッシュする際に使用できる、OT デバイスの特性に固有のプロファイリング ポリシーを作成することが可能です。

図 21：インベントリ属性



つ目次に戻る

図 *22* に IND から受け取った ISE の資産属性を示します。

図 22：資産の可視性

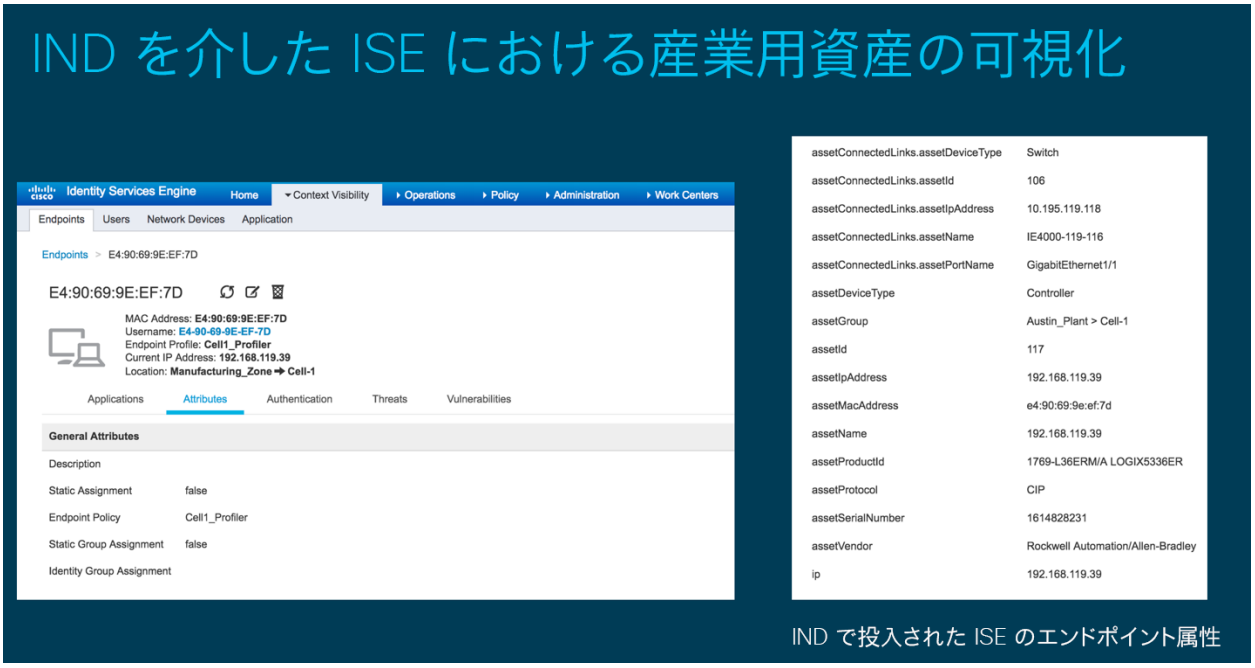
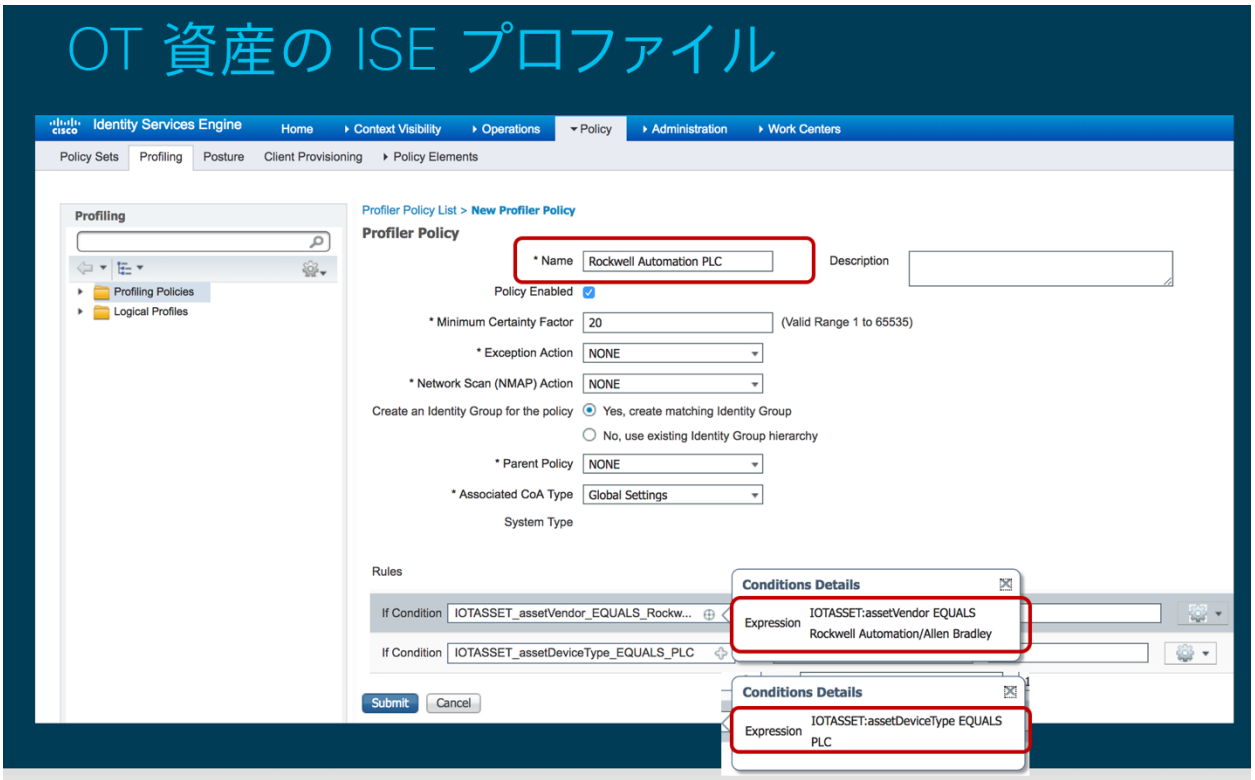


図 *23* に示すように、IND から受け取った属性に基づいて ISE で新しいデバイス プロファイルを作成します。

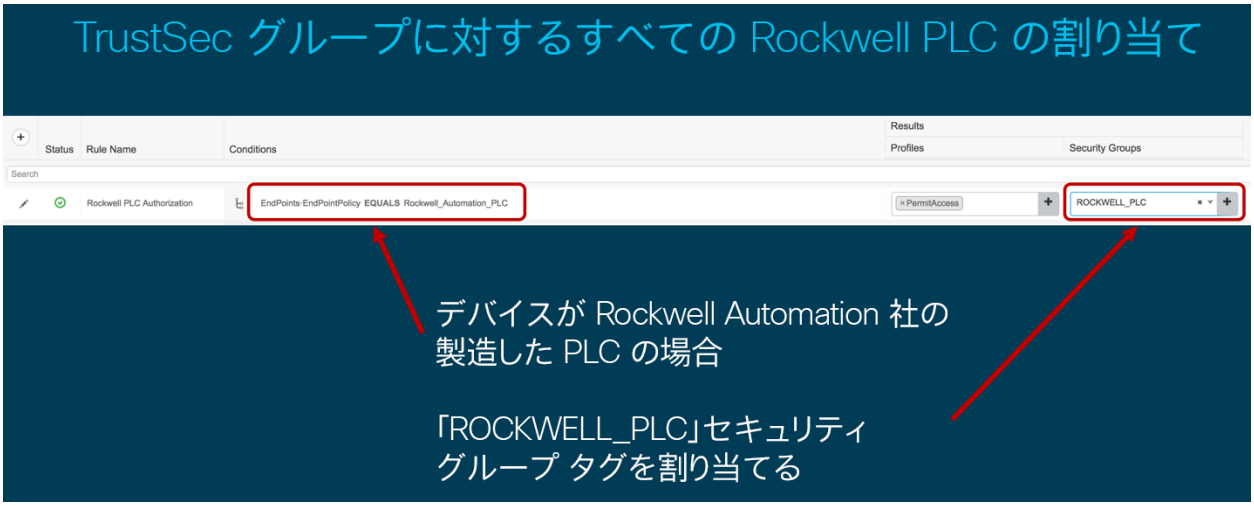
図 23：ISE プロファイラ ポリシーの作成



つ目次に戻る

図 *24* に示すように、IOTASSET 属性に基づいて ISE でセキュリティ ポリシーを作成し、Rockwell Automation 社製のすべての PLC をグループ化します。

図 24：セキュリティ グループのポリシー



OT のインテント ベースのセキュリティ

カスタム属性：

ISE で作成される新しいカスタム属性は 2 つあり、これらの属性の値は 1 つのデバイスに対して IND から送信できます。

1. assetGroup
2. assetTag

カスタム属性は、ISE の通常の OT 資産属性としても使用できます。また、プロファイリングで使用し、デバイスのセキュリティ ポリシーを割り当てることも可能です。

デバイスのカスタム属性の値は IND でローカルに定義されるため、「ユーザの目的」に基づいて操作し、ISE でポリシーの変更をトリガーできます。

つ目次に戻る

使用例

ここでは、IND と ISE を連携し、ユーザの目的に基づいて実行できる使用例を 2 つ示します。

1. OT ネットワークでのセグメンテーション
2. OT のインテント ベースのオンデマンド リモート アクセス

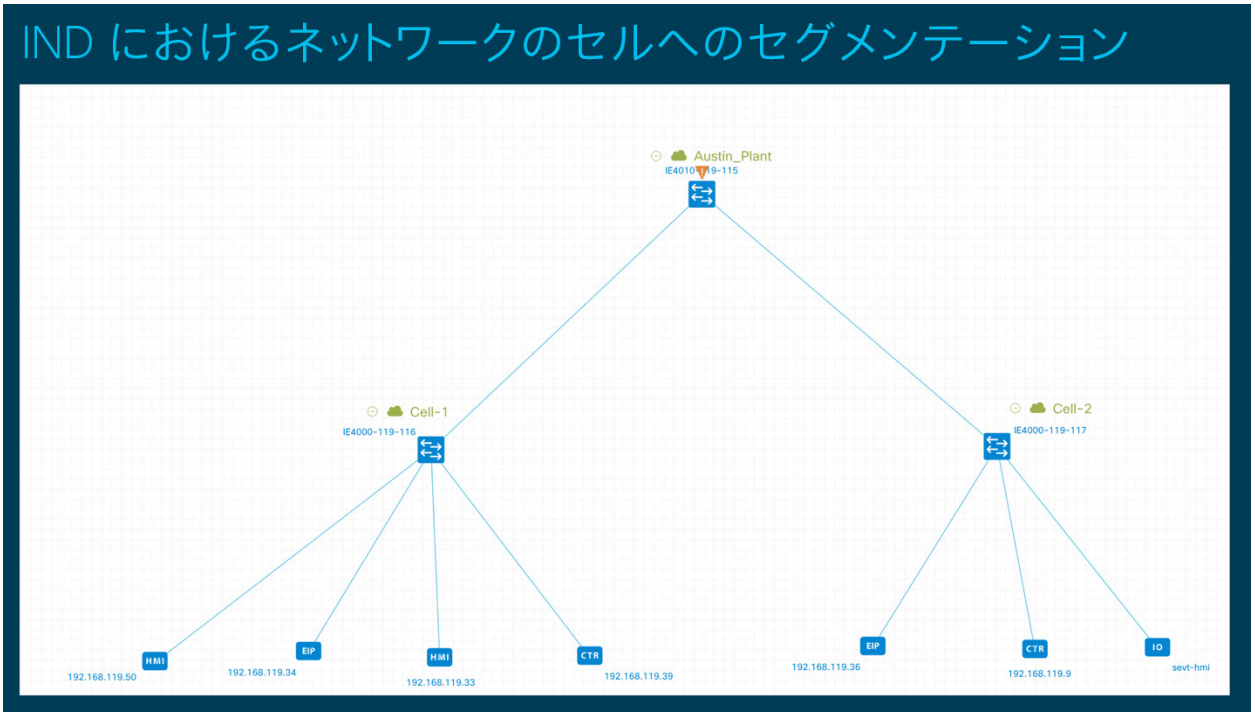
OT ネットワークでのセグメンテーション

産業用ネットワークのセグメンテーションは、セキュリティを確保するうえで非常に重要です。（ISA99 や IEC62443 などの）産業用ネットワークを管理するセキュリティ標準はいずれも、セキュリティ プロセスの開始時に行うセグメンテーションを規定します。

IND では、すべての資産をさまざまなグループに分けてネットワークの物理的な場所と階層のようにできます。IND のグループは、ISE のエンドポイント プロファイルに影響を与えるカスタム属性（assetGroup）の値として ISE に送信できます。

図 *25* に示すように、ネットワークは Cell-1 と Cell-2 という 2 つのセルにセグメント化されます。

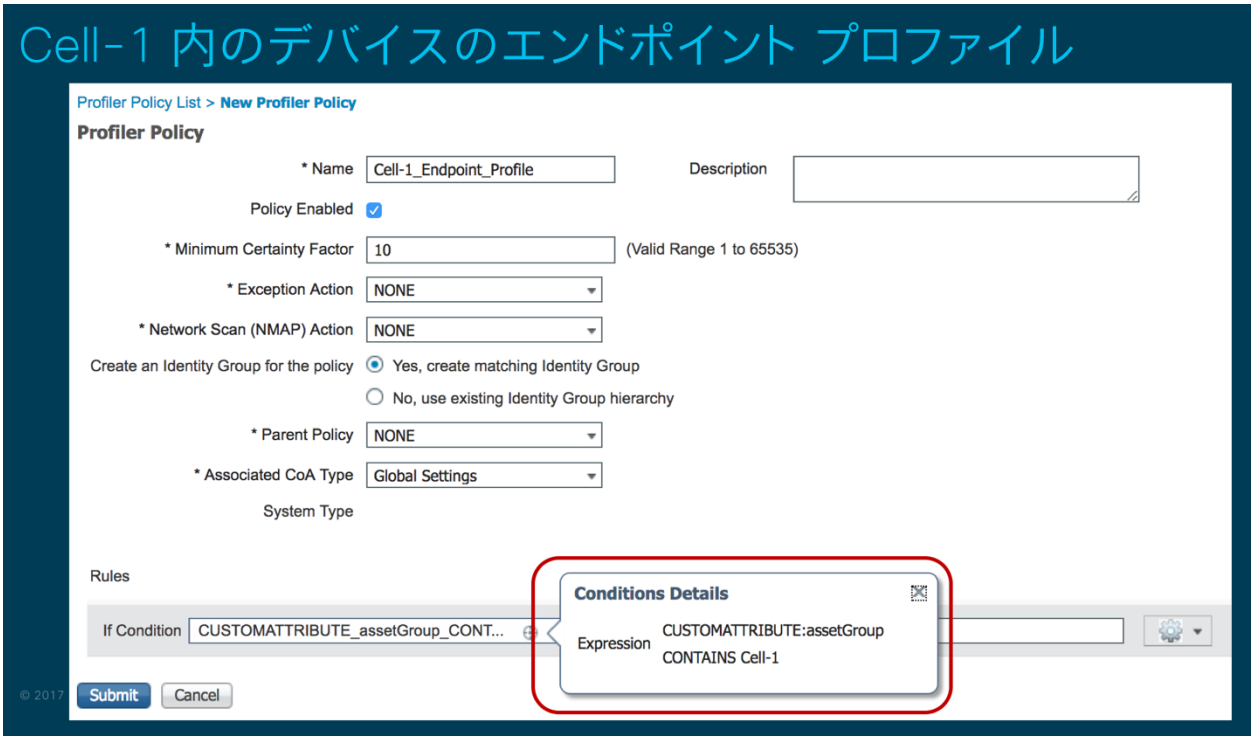
図 25：IND のトポロジ図



つ目次に戻る

ISE では、assetGroup カスタム属性の値が IND で定義したグループです。*図 26* は、IND から受け取った 2 台のデバイスのエンドポイント属性を示しています。これらのデバイスは、どちらも IND 上の 2 つの異なるセル/グループに属しているため、assetGroup カスタム属性の別の値を持ちます。

図 26：エンドポイントの属性



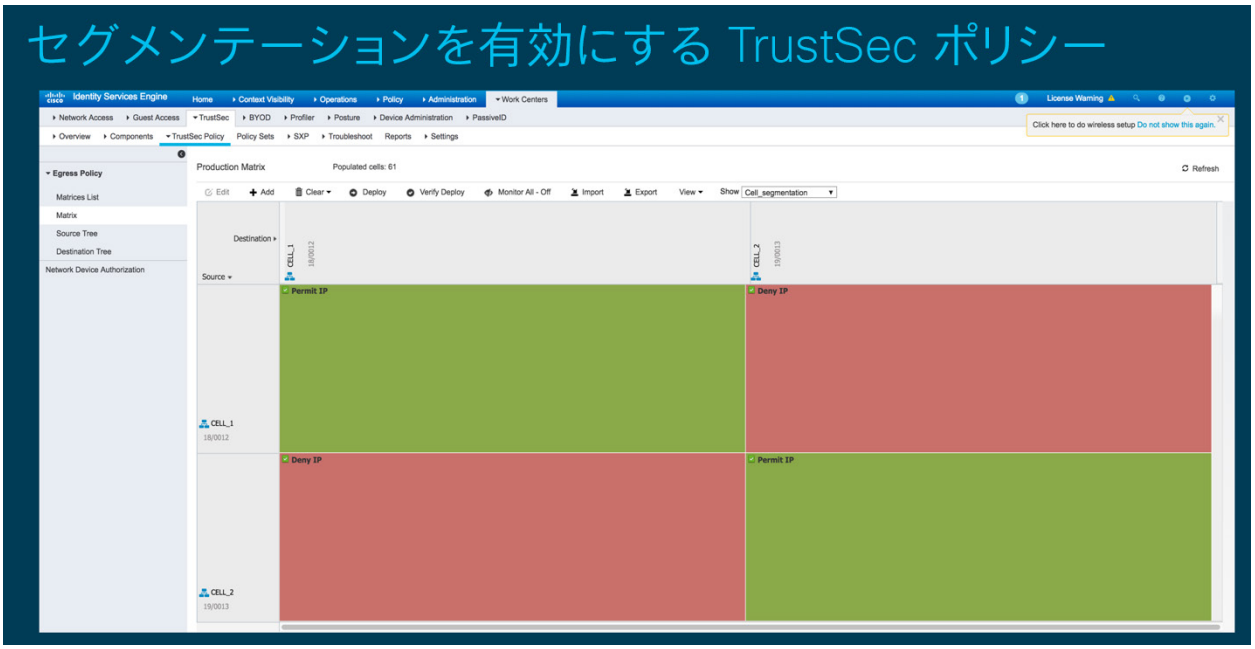
ISE のエンドポイント プロファイルは、assetGroup カスタム属性に基づいて作成することが可能です。図 *27* に示すように、セキュリティ グループ タグ（SGT）は、エンドポイント プロファイルのベースとなる認可ポリシーの結果としてエンドポイントに割り当てることができます。

図 27：割り当てられたセキュリティ グループ

つ目次に戻る

これで図 *28* に示すように、ISE の SGT を使用して、Cell-1 セグメントのデバイスが Cell-2 セグメントのデバイスと通信できないようにするといったセグメンテーション ルールを作成することが可能になります。このように OT のオペレータはセグメンテーション ポリシーを作成する必要はありませんが、ネットワークのデバイスを完全に制御し、IND のデバイス グループを変更することによってセグメンテーション ポリシーに影響を与えることができます。

図 28：ISE のセグメンテーション ポリシーの例



つ目次に戻る

OT のインテント ベースのオンデマンド リモート アクセス

この使用例では、ベンダーや機械メーカーが遠隔地からメンテナンスを行う必要がある場合に OT ユーザがリモート アクセスを有効にする方法を示します。

ここでは、リモート アクセスを有効にするために ISE の「assetTag」カスタム属性を使用してリモート アクセスが必要な資産を特定し、スイッチとファイアウォールをカバーするセキュリティ ポリシーをプッシュして VPN で接続されたリモート ユーザからのトラフィックを許可します。

図 29：IND のリモート アクセス タグの追加

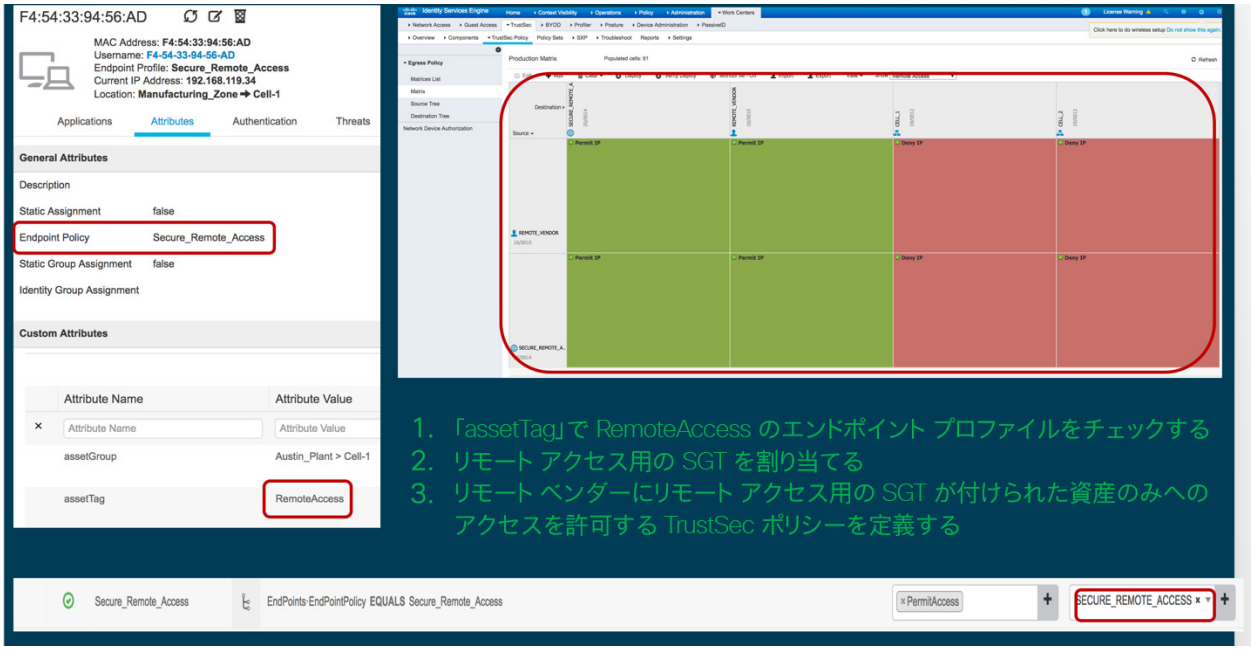
注：

すべての VPN インフラストラクチャがすでに配置されており、ISE に対する VPN ユーザの認証が完了しているという前提です。

つ目次に戻る

デフォルトでは、認証が完了していてもすべてのユーザが OT ネットワークにアクセスできません。OT 資産のメンテナンスが必要な場合は必ず、工場のオペレータが IND 内で「assetTag」属性を「RemoteAccess」に変更してリモート ベンダーのアクセスを許可します。

図 30：ISE と IND のリモート アクセス ポリシーの例



つ目次に戻る

Cisco Firepower Next-Generation Firewall（NGFW）

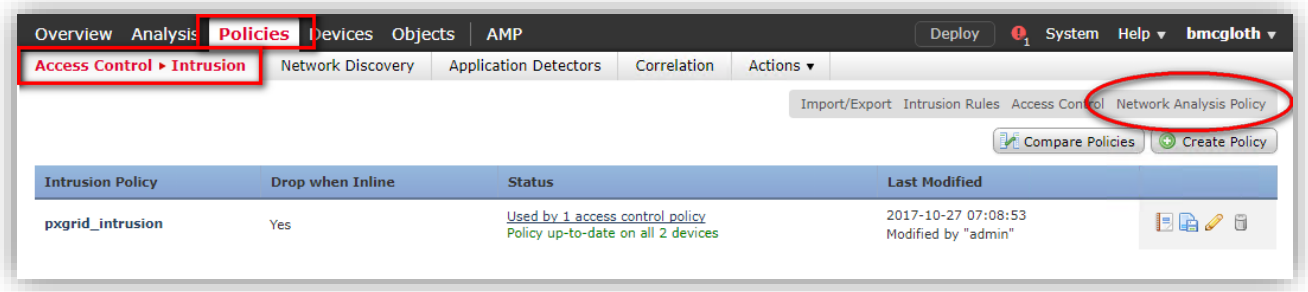
Firepower のセグメンテーション機能に加えて、ディープ パケット インスペクション機能も利用できます。Firepower には、特定のコマンドをテストする目的で作成できるカスタム ルートとともに、既知の脆弱性を保護するいくつかの産業用プロトコル（DNP3、Modbus、IEC 60870、CIP）のサポートが含まれています。

パケットに対する優れた可視性

Supervisory Control and Data Acquisition（SCADA）プロトコルは、製造、生産、水処理、配電、空港、輸送システムなどの産業プロセス、インフラストラクチャ プロセス、および設備プロセスからのデータを監視、制御、取得します。Firepower システムは、ネットワーク分析ポリシーの一部として設定できる Modbus および DNP3 SCADA プロトコル用のプリプロセッサを提供します。

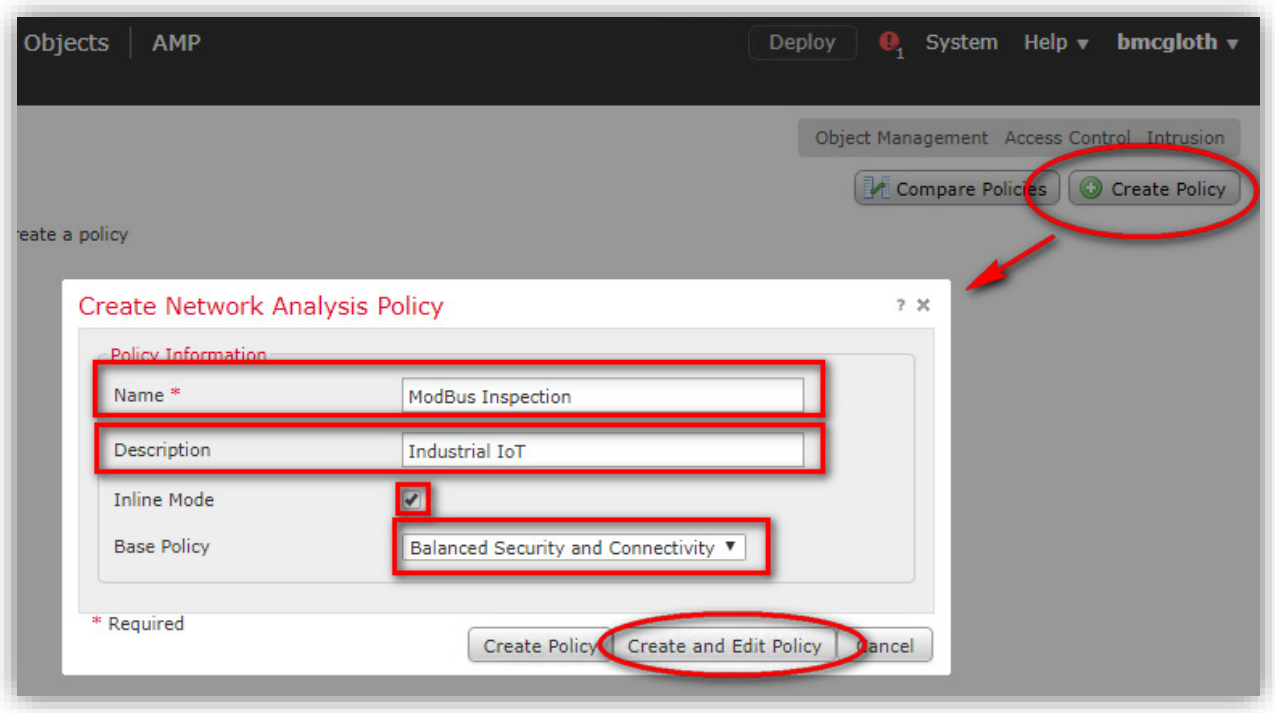
Modbus プロトコルは 1979 年に Modicon 社が初めて発表した、広く利用されている SCADA プロトコルです。Modbus プリプロセッサは、Modbus のトラフィックの異常を検出し、ルール エンジンによる処理のために Modbus プロトコルをデコードします。ルール エンジンは Modbus キーワードを使用して特定のプロトコル フィールドにアクセスします。Modbus およびコマンド プロトコルの詳細については、http://modbus.org [英語] を参照してください。Modbus のインスペクションはデフォルトで無効になっています。Modbus のインスペクションを有効にするには、ネットワーク分析ポリシーを作成してアクセス コントロール ポリシーに適用する必要があります。次のステップでは、ポリシーを作成して適用します。

ステップ 1：[ポリシー（Policies）] > [アクセスコントロール（Access Control）] > [侵入（Intrusion）] の順に選択し、[ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。

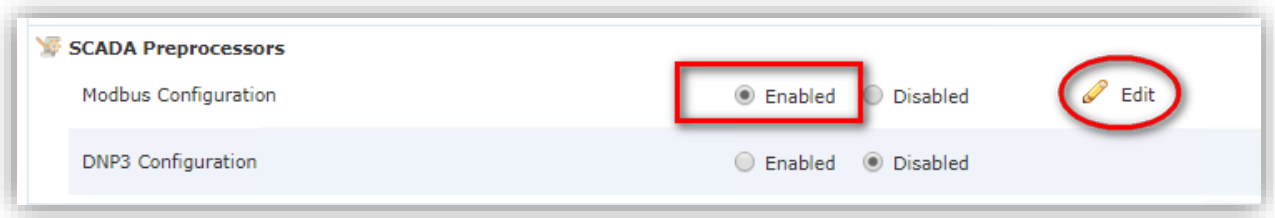


つ目次に戻る

ステップ 2：右上の [ポリシーの作成（Create Policy）] ボタンをクリックしてポリシーに名前を付け、[ポリシーの作成と編集（Create and Edit Policy）] ボタンをクリックします。



ステップ 3：ナビゲーション パネルで [設定（Settings）] をクリックします。[SCADA プリプロセッサ（SCADA Preprocessors）] の [Modbus の設定（Modbus Configuration）] が無効になっている場合は、[有効化（Enabled）] をクリックします。[Modbus の設定（Modbus Configuration）] の横にある編集アイコンをクリックします。



ステップ 4：[ポート（Ports）] フィールドに値を入力します。ポート 502 がデフォルトです。複数の値を指定する場合は、カンマで区切ります。

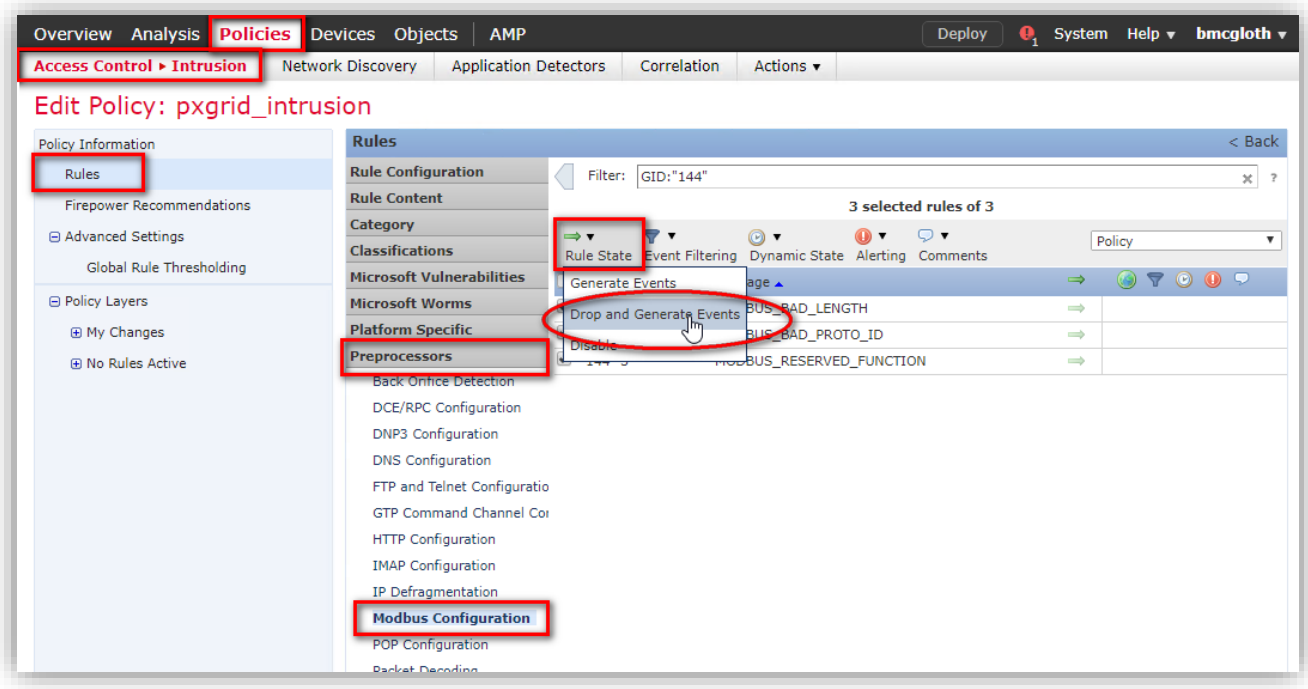
ステップ 5：最後のポリシーを確定した後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックしてから [変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合、別のポリシーを編集すると、最後に確定してから加えたキャッシュされている変更は破棄されます。

つ目次に戻る

次に [侵入ポリシー（Intrusion Policy）] で Modbus プリプロセッサのルールを有効にする必要があります。イベントを生成し、インライン展開では問題のあるパケットをドロップするようこれらのルールを有効にします。

ステップ 6：[ポリシー（Policies）] > [アクセスコントロール（Access Control）] > [侵入（Intrusion）] の順に選択し、ポリシーの横にある [編集（Edit）] をクリックします。[ルール（Rules）] > [プリプロセッサ（Preprocessors）] > [Modbus の設定（Modbus Configuration）] の順に選択します。3 つすべてのルールのチェックボックスをオンにし、[ルール状態（Rule State）] メニューの [ドロップしてイベントを生成する（Drop and Generate Events）] を選択します。



ステップ 7：最後のポリシーを確定した後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックしてから [変更を確定（Commit Changes）] をクリックします。

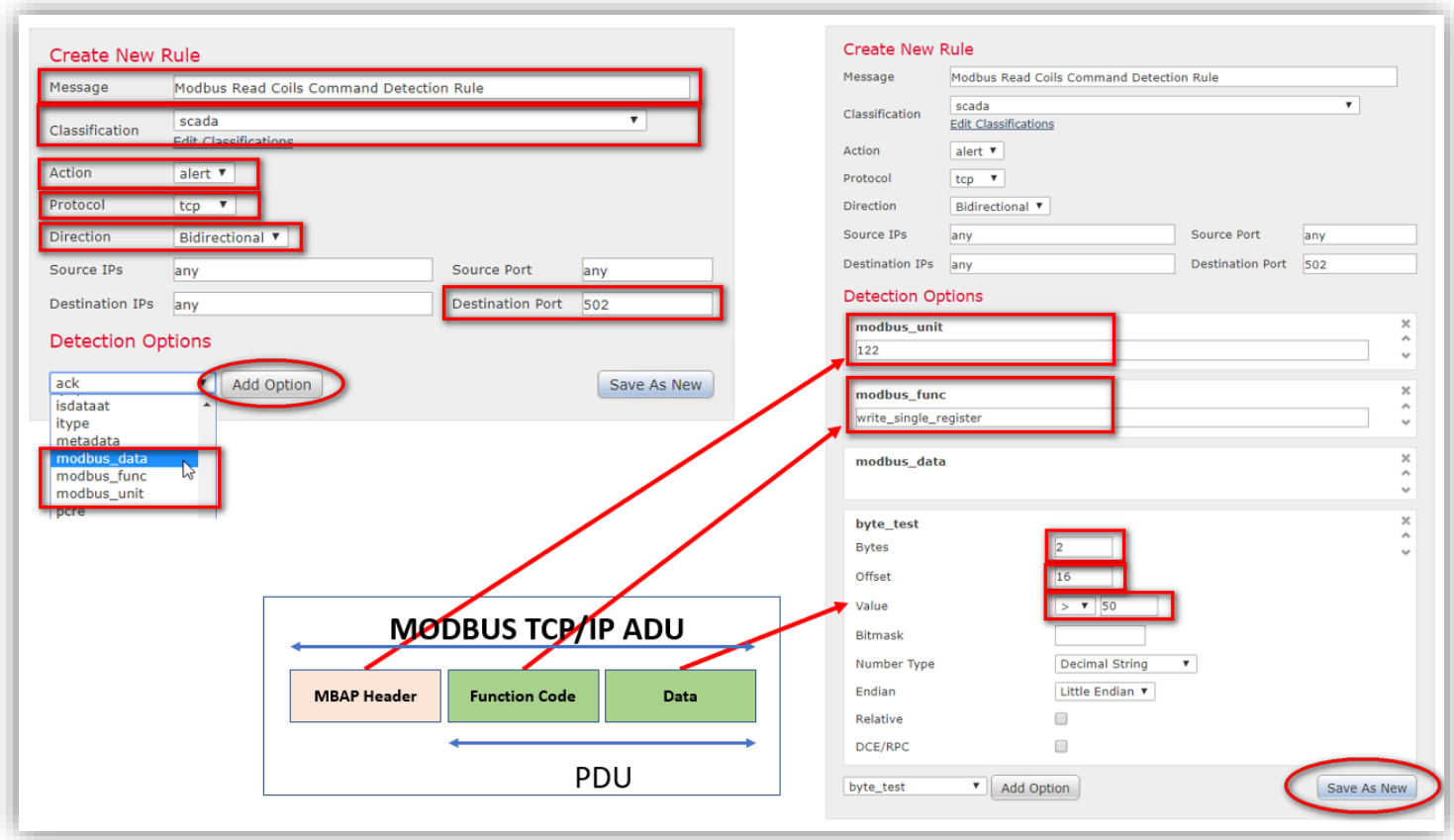
つ目次に戻る

101
Modbus コマンドのインスペクション

ネットワークを通過するコマンドをテストして不正なコマンドが産業用 IoT システムに到達するのをブロックする、カスタム調査ルールを作成します。

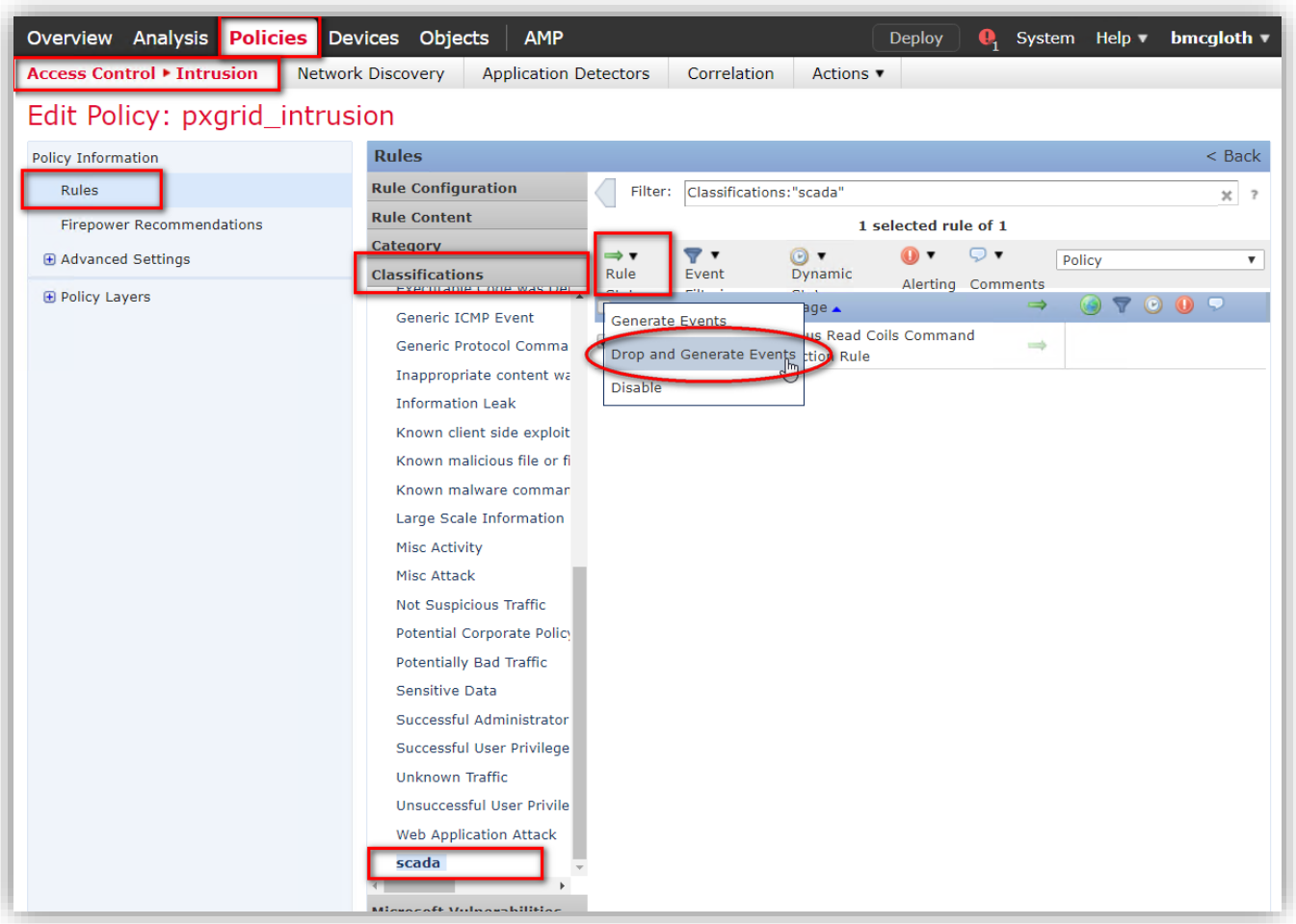
たとえば、RTU-0122 に対する 50 を超える設定値の変更を防止するルールを作成します。

ステップ 1：Modbus コマンドをチェックする新しいルールを作成します。[オブジェクト（Objects）] > [侵入ルール（Intrusion Rules）] > [新しいルールの作成（Create New Rule）] の順に選択します。ルールに名前を付け、[検出オプション（Detection Options）] で Modbus の要素を指定します。[新規として保存（Save as New）] をクリックします。



つ目次に戻る

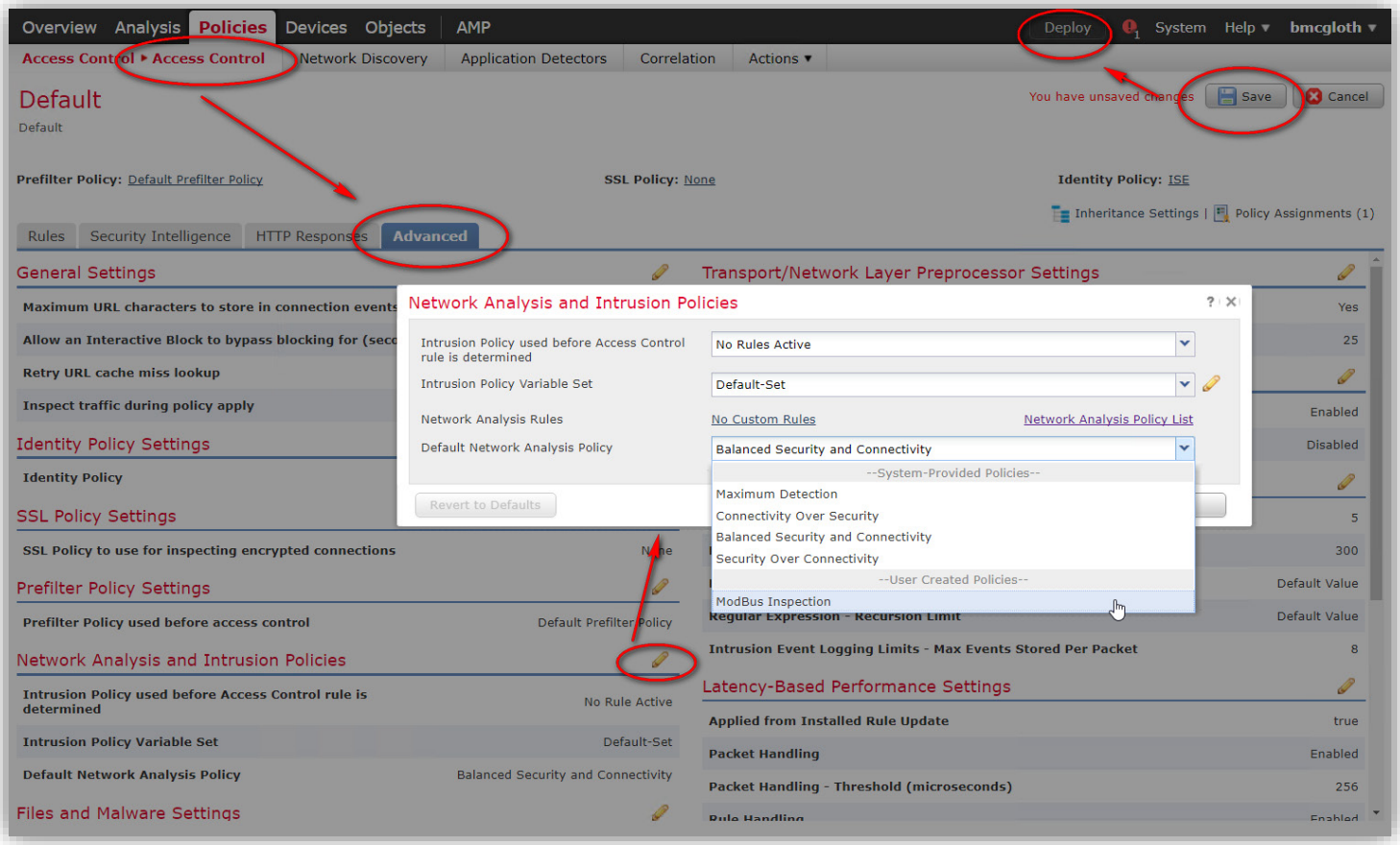
ステップ 2：[ポリシー（Policies）] > [アクセスコントロール（Access Control）] > [侵入（Intrusion）] の順に選択し、ポリシーの横にある [編集（Edit）] をクリックします。[ルール（Rules）] > [分類（Classifications）] > [SCADA] の順に選択します。ルールのチェックボックスをオンにし、[ルール状態（Rule State）] メニューの [ドロップしてイベントを生成する（Drop and Generate Events）] を選択します。



ステップ 3：最後のポリシーを確定した後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックしてから [変更を確定（Commit Changes）] をクリックします。

つ目次に戻る

ステップ 4：更新した侵入防御ポリシーを使用して、アクセス コントロール ポリシーにネットワーク分析 Modbus インスペクション ポリシーを追加します。[ポリシー（Policies）] > [アクセスコントロール（Access Control）] > [アクセスコントロール（Access Control）] > [デフォルトの編集（Edit Default）] の順に選択してから [詳細設定（Advanced）] タブをクリックし、[ネットワーク分析（Network Analysis）] を編集します。ポリシーを [Modbus ポリシー（Modbus Policy）] に変更します。[OK]、[保存（Save）]、[展開（Deploy）] の順にクリックします。



つ目次に戻る

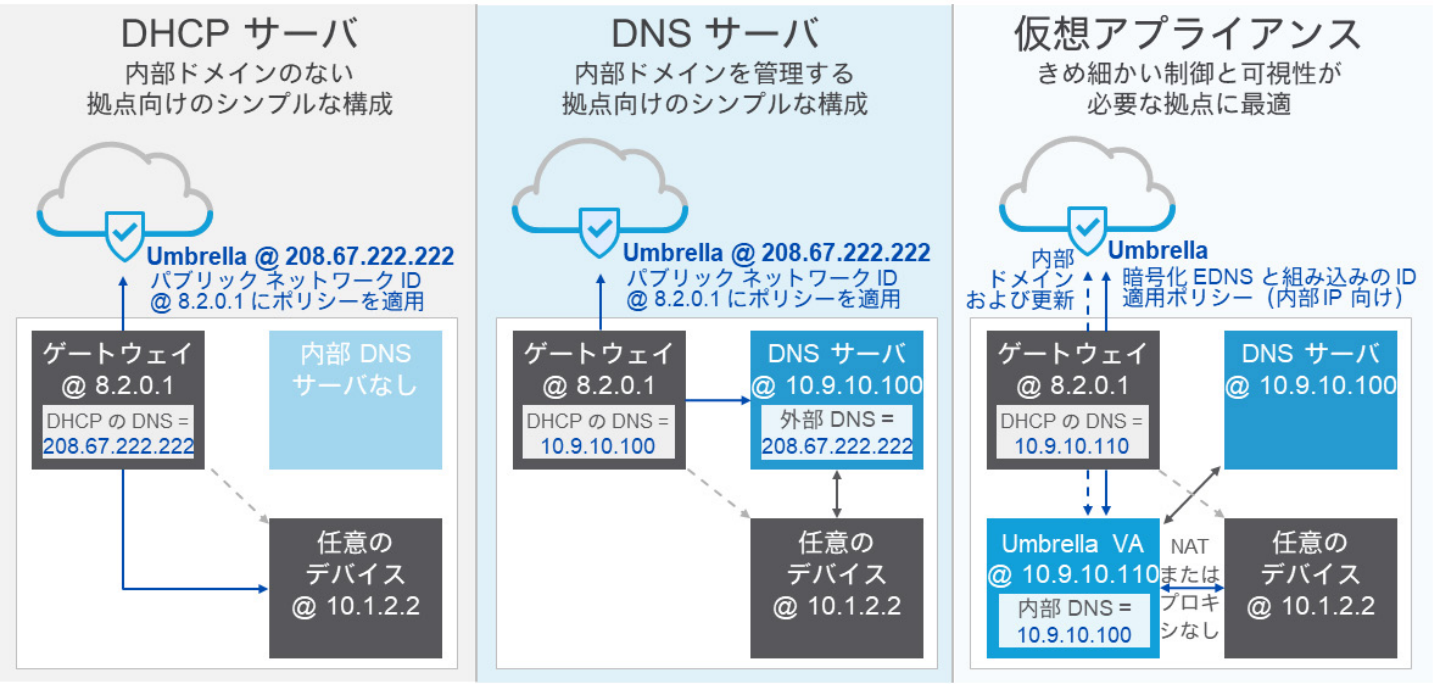
Cisco Umbrella

Cisco Umbrella は、DNS を使用して最も簡単にネットワークの基本的な可視性を得ることができるメソッドの 1 つです。ほとんどのデバイスは、すべてのプロトコルで接続を確立するために DNS を使用してドメイン名からシステムの IP アドレスを解決します。図 31 に示すように、Cisco Umbrella では、最もシンプルな展開オプションにより、ユーザやデバイスからは見えない形で可視性を得ることができます。

最も一般的な展開オプションとしては、次の 3 つが挙げられます。

1. DHCP サーバ：主にインターネットと通信するリモートの IoT デバイスに最適です。
2. DNS サーバ：内部通信をいくらか利用しつつ、主にインターネットと通信する、内部の IoT デバイスに最適です。エンドポイントは可視化されませんが、不正なドメインから IoT デバイスが保護されます。
3. 仮想アプライアンス：内部システムとインターネット システムの両方と通信する、内部の IoT デバイスに最適です。内部におけるアイデンティティ情報に基づいて、可視性、保護、およびポリシー オプションが提供されます。

図 31：Umbrella の展開オプション



シスコの産業用 IoT 環境では、工場からのほぼすべての通信が産業ゾーン内にとどまりますが、ベンダーはクラウド サービスへのテレメトリのレポートを有効にするよう顧客に要求しています。多くの顧客は、IoT デバイスがインターネット サービスと通信しているかどうかをまったくわかっていません。このレベルのきめ細かな可視性を得るには、ネットワークでのローカル プレゼンスが必要です。

このソリューションは、VMware または Hyper-V で仮想アプライアンスとして展開される軽量の DNS フォワーダを実装します。DHCP サーバか静的に割り当てられた DNS サーバを使用することにより、内外のドメインに対するすべての要求を最初に仮想アプライアンスに送信します。仮想アプライアンスは内部ドメイン向けの要求を既存のローカル DNS サーバに転送します。インターネット ドメインに対する要求が Umbrella に転送される前に、ローカル IP が RFC 準拠の DNS 拡張方式に組み込まれるため、要求元の内部ネットワーク デバイスを特定できます。これらのインターネット宛先クエリのレポートは、Cisco Umbrella のレポート コンソールで入手できます。

つ目次に戻る

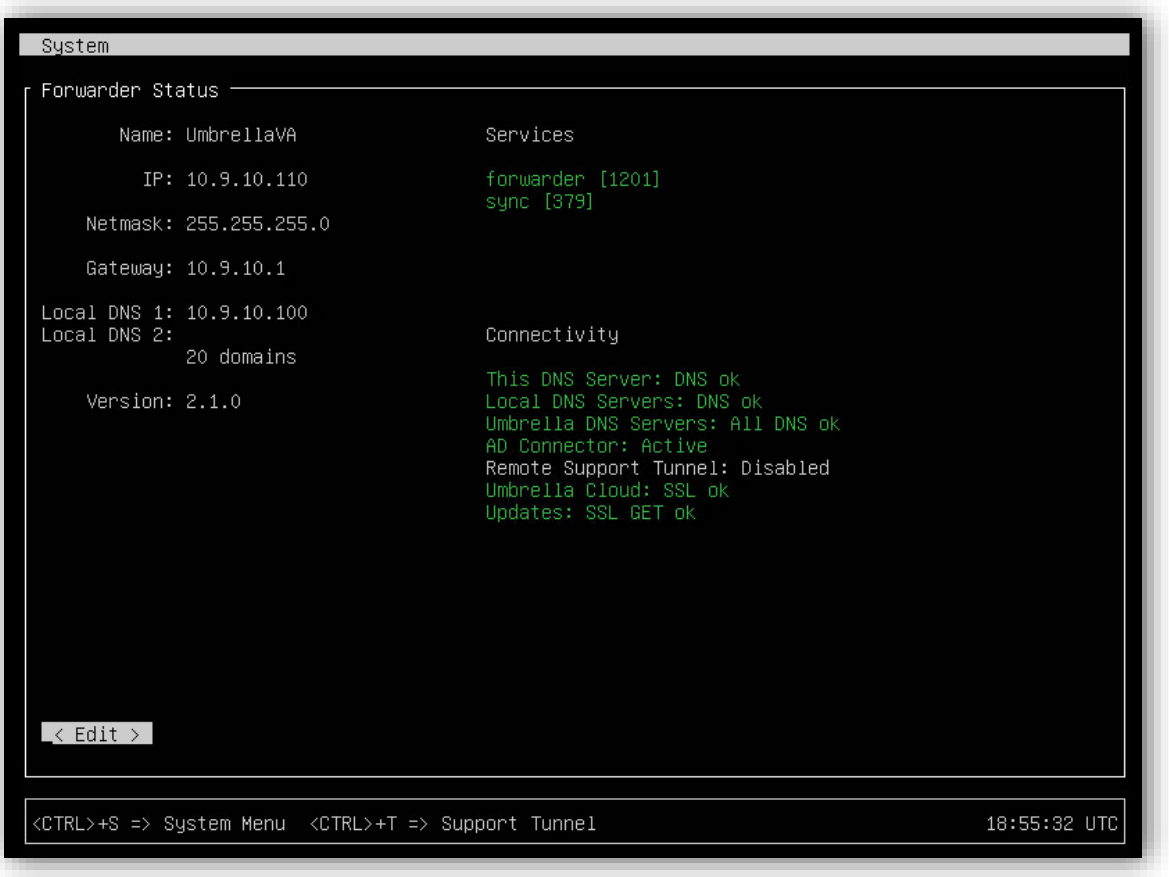
105

Cisco Umbrella 仮想アプライアンス

Cisco Umbrella 仮想アプライアンスは、https://docs.umbrella.com/product/umbrella/1-introduction/ にあるインストール ガイドに従って、ラボ内の VMware システムにインストールできます。

インストールの手順が完了すると、Umbrella 仮想アプライアンスのステータス コンソールは図 32 のようになります。

図 32：Umbrella VA のステータス

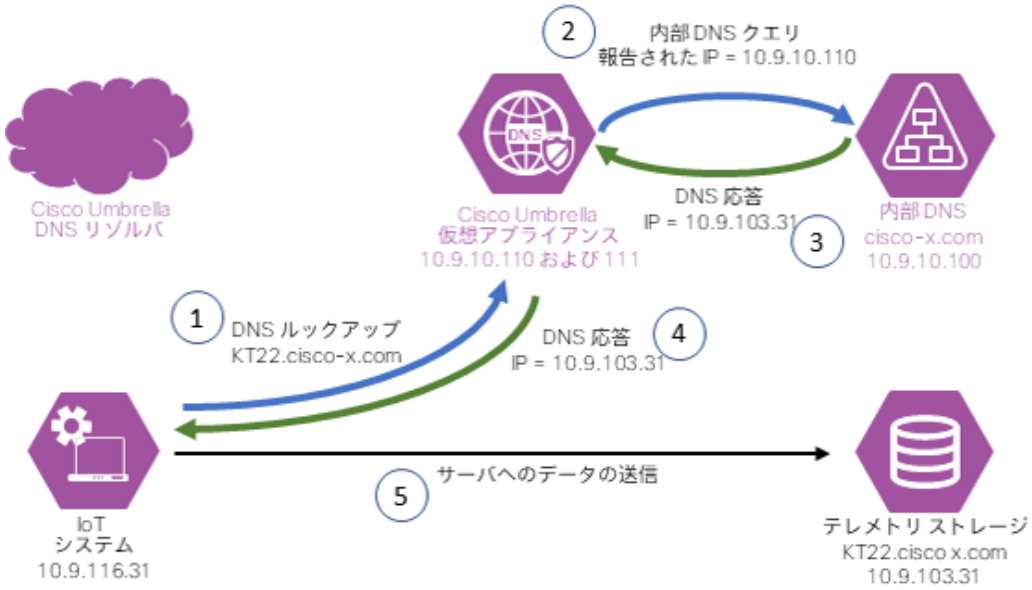


IoT システムは、DNS サーバとして（高可用性を実現するために展開された 2 つの）Umbrella 仮想アプライアンスを使用するように設定しました。仮想アプライアンスでは、内部解決用に Microsoft Active Directory DNS サーバを使用しました。

つ目次に戻る

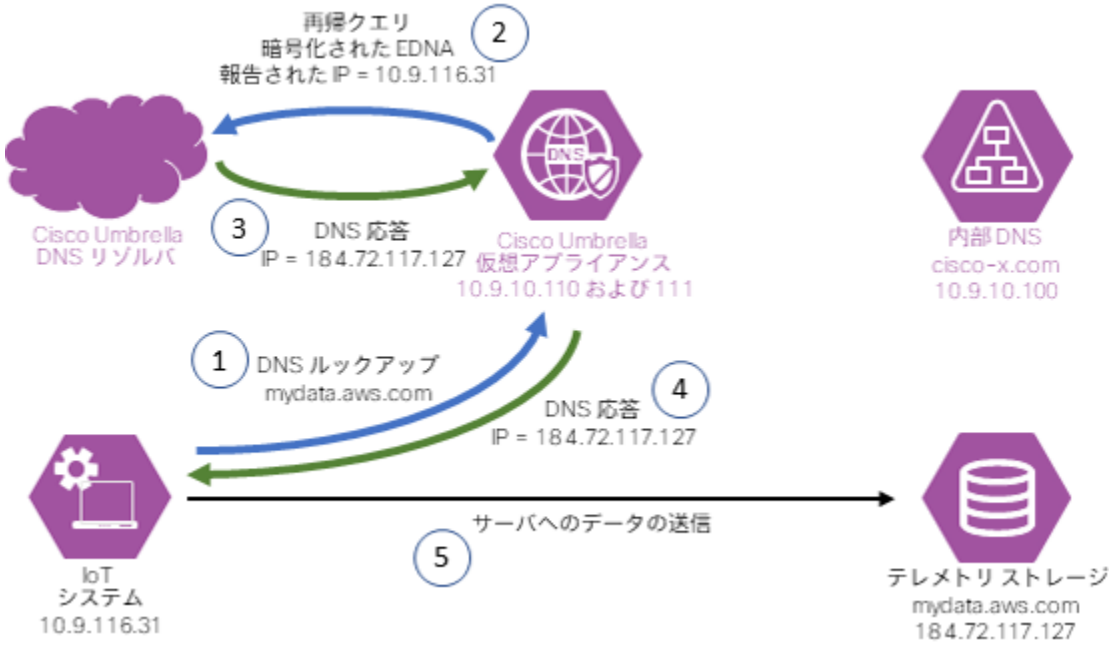
内部ドメインの検索に関しては、図 33 に示すように、Umbrella 仮想アプライアンスは内部の DNS サーバに要求を送信し、その応答を IoT システムに転送します。これらの要求は仮想アプライアンスには記録されず、内部 DNS サーバでは仮想アプライアンスが要求の送信元として表示されます。

図 33：内部ドメインの検索



外部インターネット ドメインの検索に関しては、図 34 に示すように、Umbrella 仮想アプライアンスはクラウド内の Umbrella のリゾルバに要求元の IP アドレスの情報を付加した要求を送信します。このような詳細な情報を使用するポリシーは、要求元のデバイスに応じてカスタマイズできます。すべてのポリシーが要求に適用されると IoT システムに応答が転送され、そのシステムで通信を確立できます。

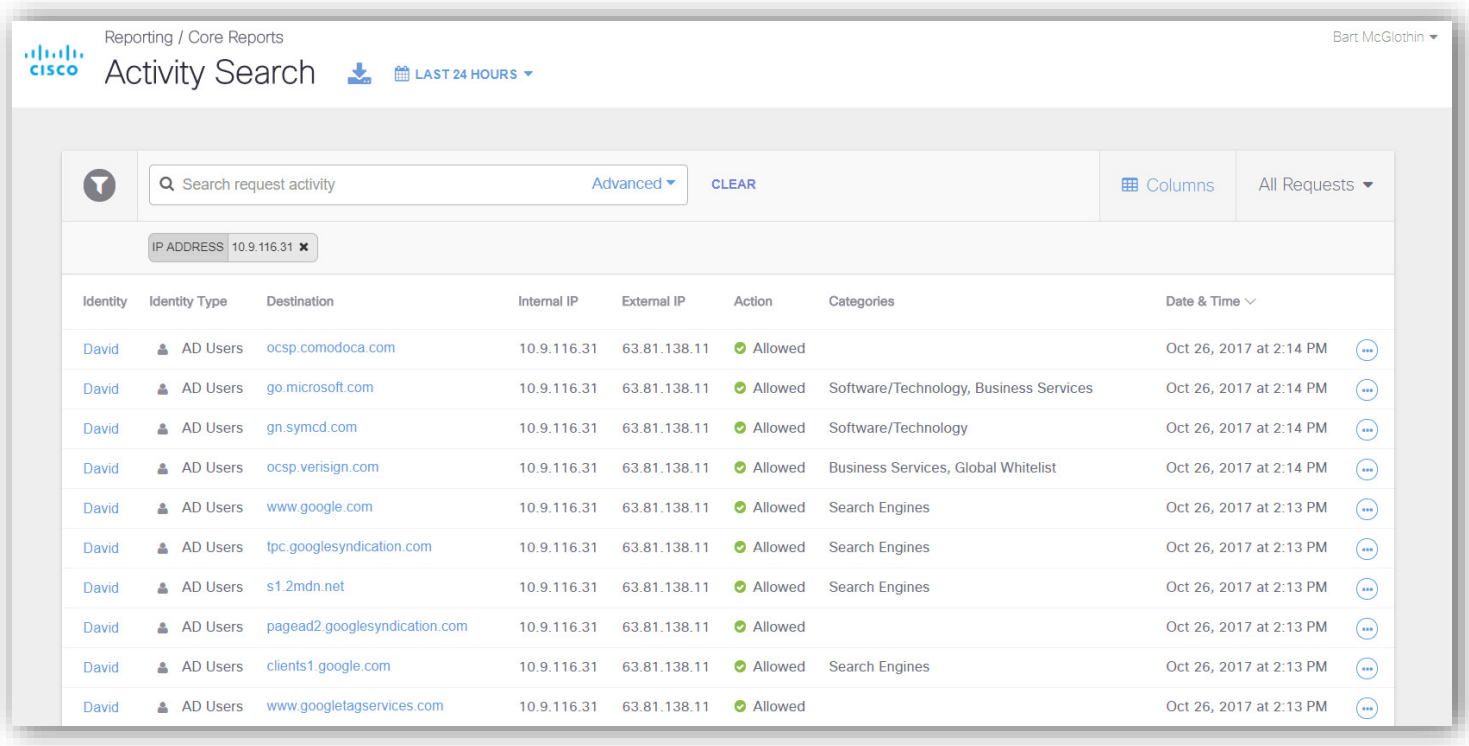
図 34：外部インターネット ドメインの検索



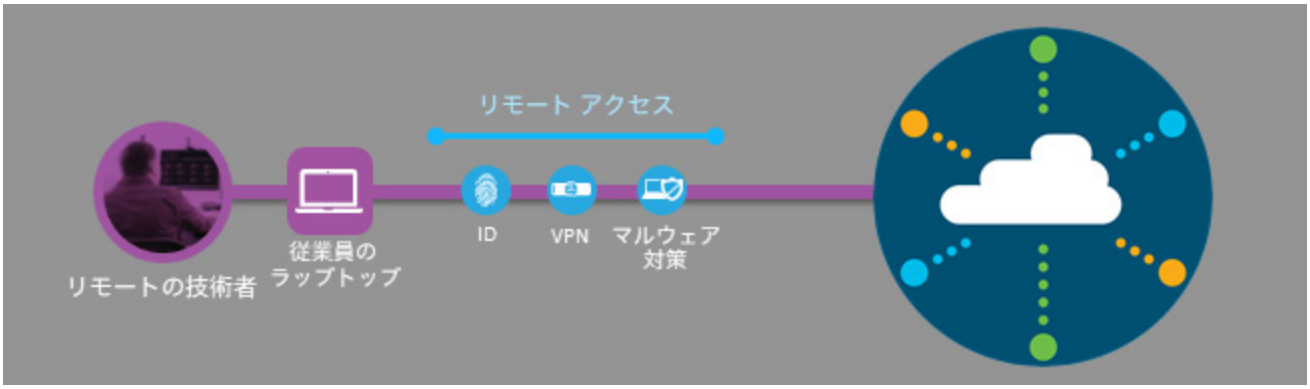
つ目次に戻る

107

これらの要求は記録され、Umbrella のレポート コンソールで確認できます。



つ目次に戻る



Cisco AnyConnect

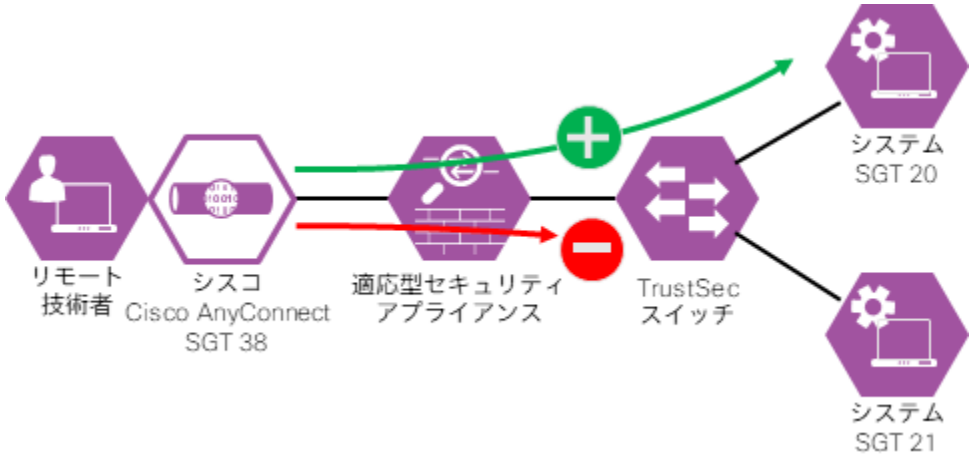
高額かつ高度な最新化への投資を維持するために、デバッグとメンテナンスをベンダーに頼らなければならなくなる可能性があります。そのためにベンダーに工場のネットワークへのリモート アクセスを許可したり、ベンダーの担当者に製造現場への直接アクセスを許可したりするシナリオは複数あります。いずれの場合でも、そうしたアクセスはさまざまな管理者が管理する複数のネットワークを通過する必要があります。そのようなアクセスを必要に応じて安全に行うのは容易ではありません。シスコでは、ネットワークとセキュリティ面で一意の強固な環境を提供することで容易にしています。

1. まず、外部の技術者が対応を依頼されたデバイスにたどり着くには、インターネットで企業にアクセスし、Industrial DMZ を通過して踏み台に入ってから工場のネットワークを通過しなければなりませんが、このようなプロセスは複雑です。
2. 次に、外部の技術者が現場にいて、本社のリソースにアクセスする必要がある場合は、プロセスが逆になります。

ASA は、VPN セッションのセキュリティ グループのタグ付けをサポートしています。セキュリティ グループ タグは、ASA におけるグループ ポリシーの利用を簡素化します。Cisco AnyConnect VPN は、ASA ファイアウォールで実装されます。リモートのベンダーとパートナーは、Active Directory のユーザ/グループ アカウントに基づいて ISE で認証されます。ISE は、認可ポリシーに基づいて適切な SGT を割り当てます。図 35 に示すように、ASA のアクセス ポリシーでは、デバイスとセキュリティ グループの IP-SGT マッピングに基づいて許可されたシステムのみへのアクセスをパートナーに許可します。

つ目次に戻る

図 35：Cisco AnyConnect と SGT



AAA サーバの属性に VPN ユーザに割り当てる SGT が含まれていない場合、ASA はグループ ポリシーの SGT を使用します。グループ ポリシーに SGT が含まれていない場合は、タグ 0x0 が割り当てられます。

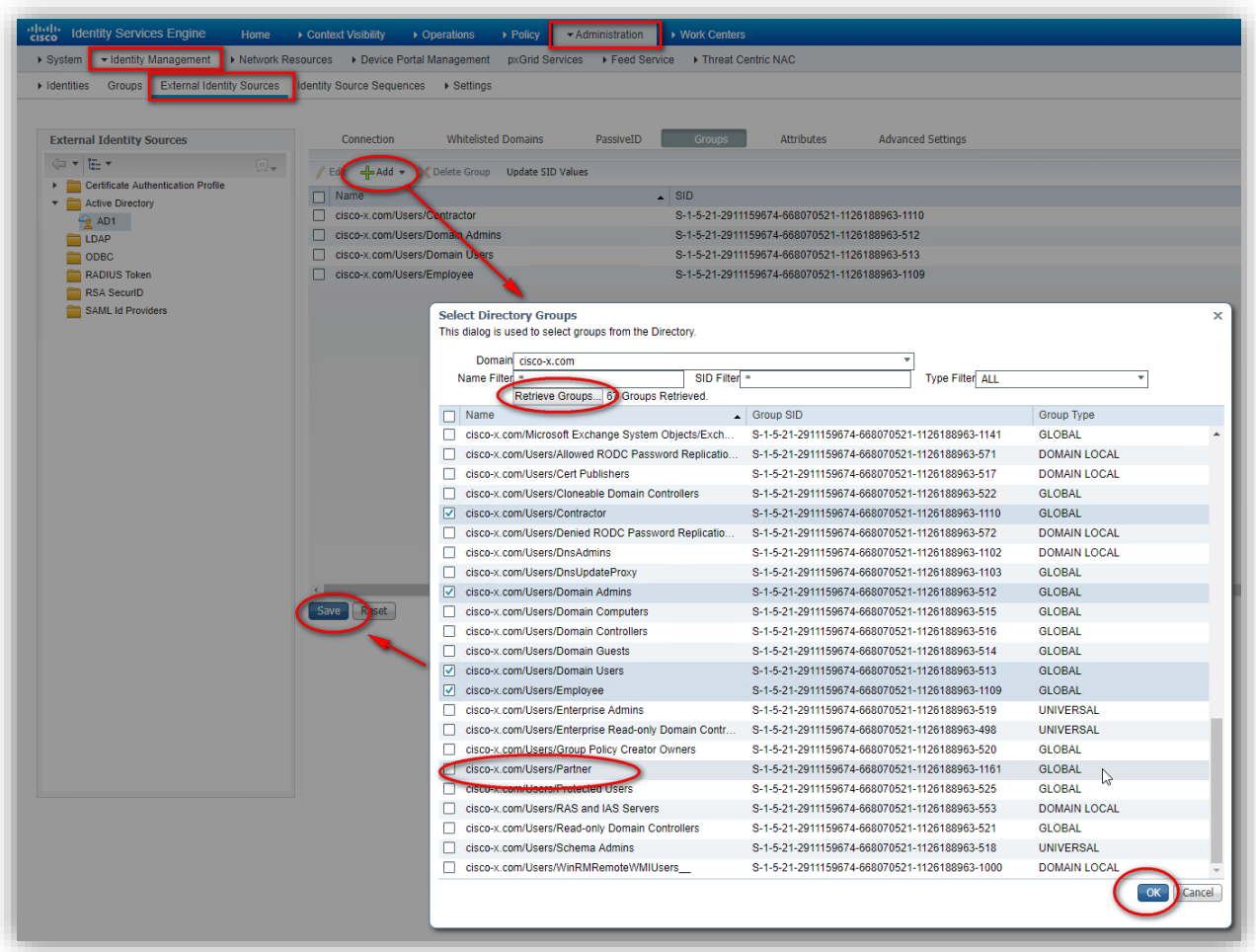
クライアント VPN と TrustSec の詳細については、次の URL を参照してください。

- https://www.cisco.com/c/en/us/td/docs/security/asa/asa98/configuration/firewall/asa-98-firewall-config/access-trustsec.html#ID-2135-000006a9
- https://www.cisco.com/c/ja_jp/support/docs/security/adaptive-security-appliance-asa-software/117694-config-asa-00.html#anc6

Cisco Identity Services Engine（ISE）の設定

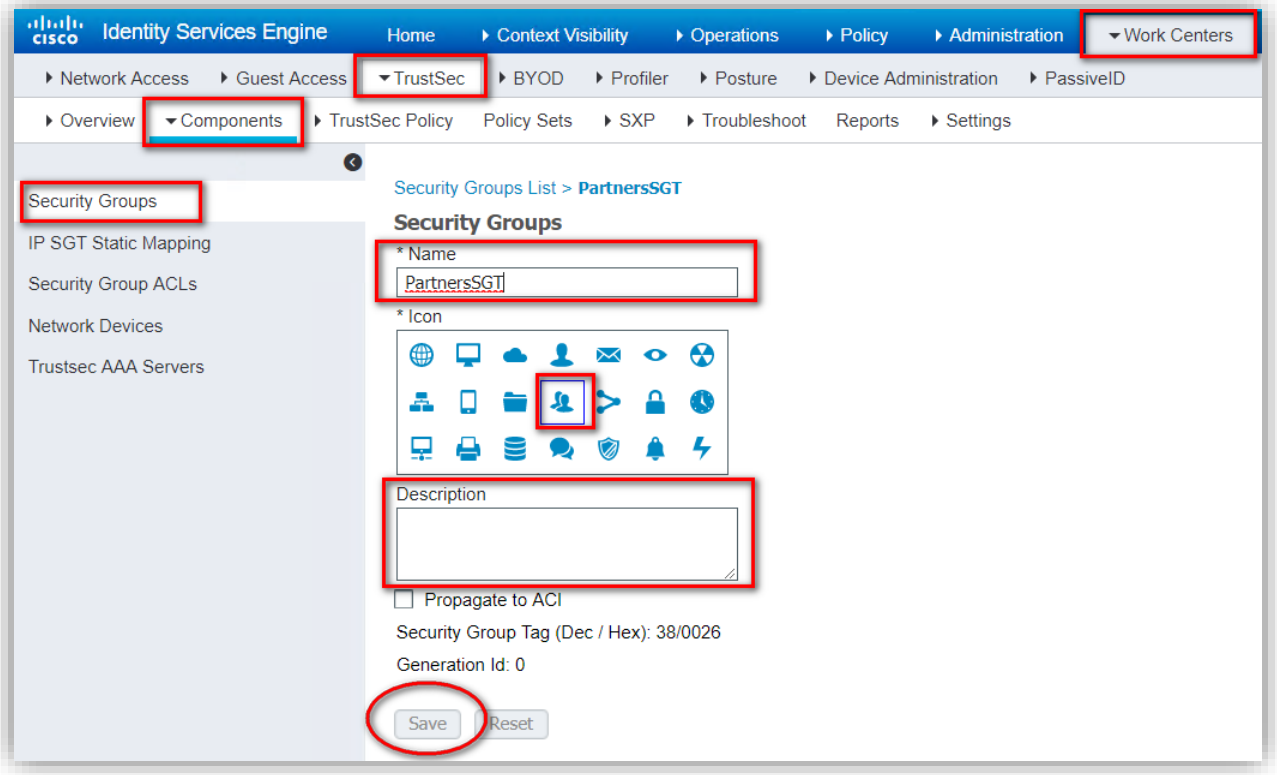
次のステップでは、Active Directory からパートナー グループを ISE のアイデンティティ ソースに追加、関連するパートナーのセキュリティ グループ タグを作成、パートナー向けの認可ポリシーを追加、そして ASA のリモートアクセスの認証として ISE を追加する方法を解説します。

ステップ 1：[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] の順に選択し、Active Directory ユーザからパートナー グループを追加して設定します。

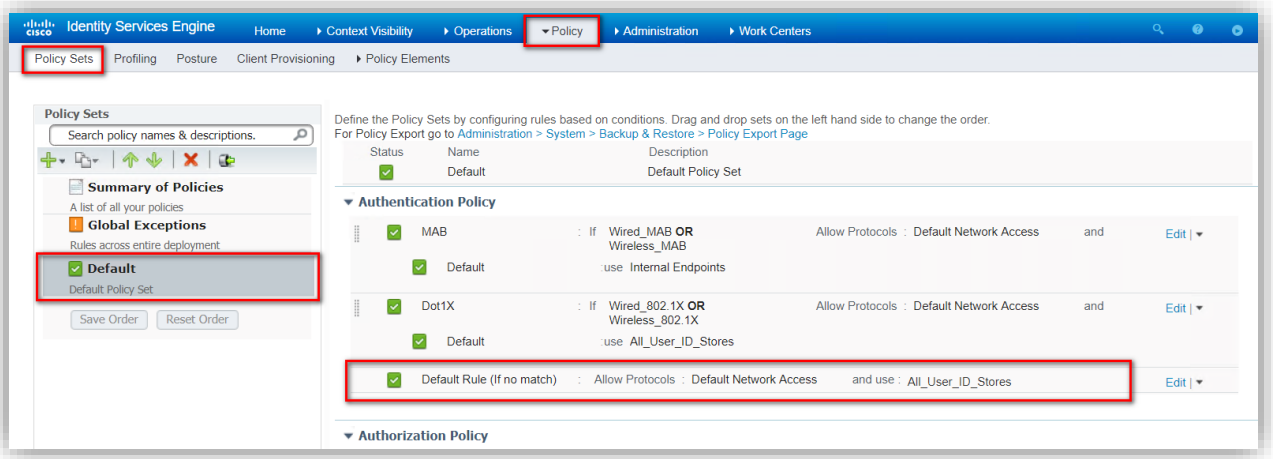


つ目次に戻る

ステップ 2：[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）] > [追加（Add）] の順に選択し、パートナーの SGT グループを追加して設定します。Name を入力してアイコンを選択し、Description を入力して [保存（Save）] をクリックします。

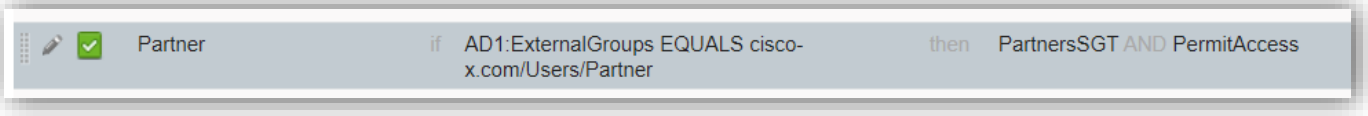


ステップ 3：認証ポリシーにパートナーのアイデンティティ ストアが含まれていることを確認します。[ポリシー（Policy）] > [ポリシーセット（Policy Sets）] > [デフォルト（Default）] に移動します。

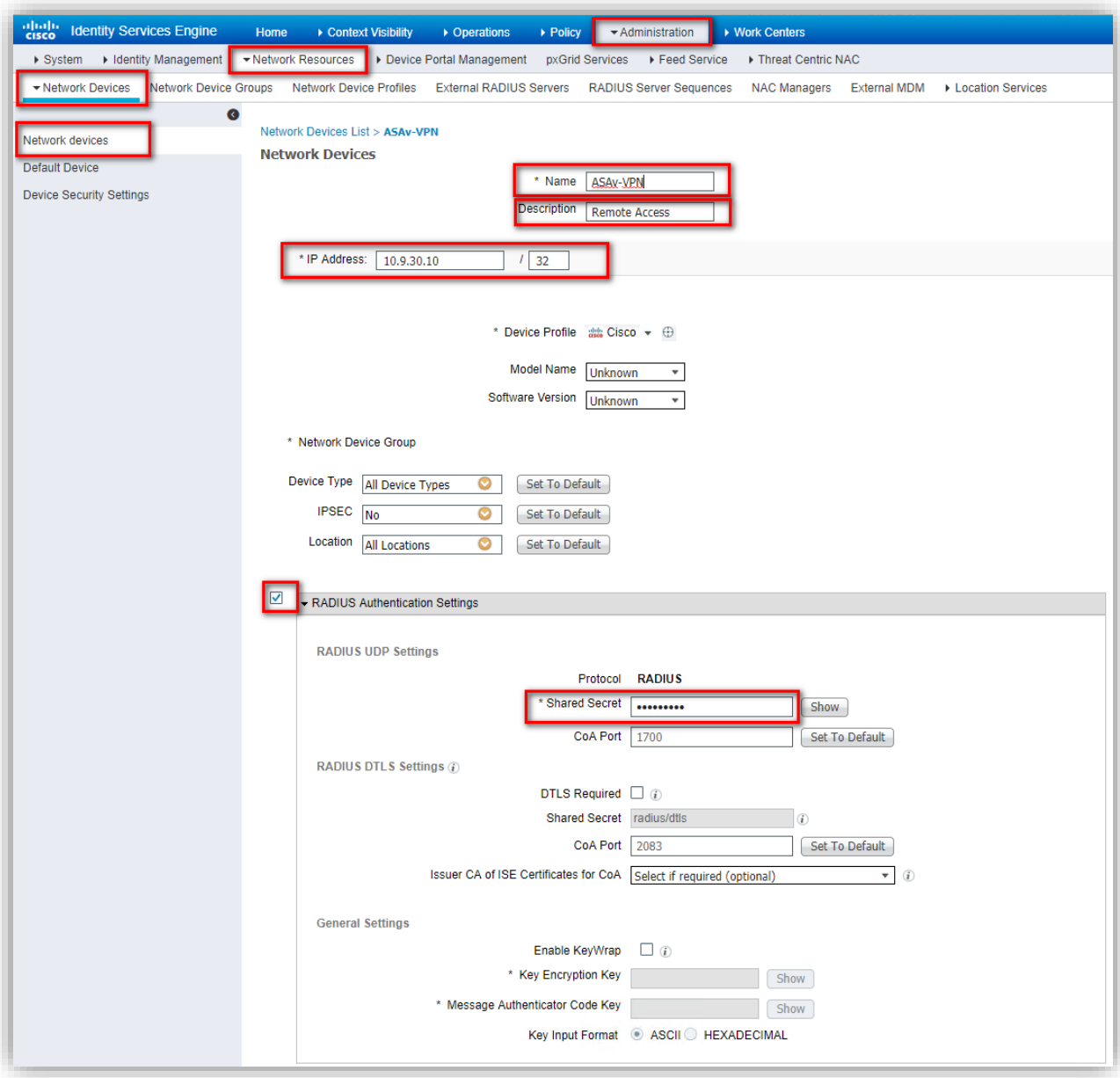


つ目次に戻る

ステップ 4：[ポリシー（Policy）] > [ポリシーセット（Policy Sets）] > [デフォルト（Default）] > [認可ポリシー（Authorization Policy）] の順に選択し、パートナーの認可プロファイルを追加して設定します。Active Directory のアイデンティティ グループを指定し、PermitAccess と SGT グループ PartnersSGT の権限を割り当てます。



ステップ 5：[管理（Administration）] > [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、ネットワーク デバイスとして ASA を追加して設定します。[保存（Save）] をクリックします。



つ目次に戻る

113

Cisco ASA VPN の設定

次のステップでは、AnyConnect クライアントを使用して ASA のリモート アクセス VPN を設定し、ISE でリモート ユーザを認証して SGT を割り当ててから、それらの SGT に基づいたセキュリティ ポリシーを実装する方法を概説します。

ステップ 1：CLI を使用して基本的な VPN 設定を行います。

VPN ユーザの IP プールを定義します。

```
ip local pool VPN_POOL 10.9.31.10-10.9.31.99 mask 255.255.255.128
```

VPN のプロファイルとポリシーを設定します。

```
webvpn  enable outside
 anyconnect image disk0:/anyconnect-win-4.5.00058-webdeploy-k9.pkg 1
 anyconnect image disk0:/anyconnect-macos-4.5.00058-webdeploy-k9.pkg 2
 anyconnect enable
 tunnel-group-list enable
 cache
  disable
 error-recovery disable
!
group-policy GroupPolicy_SSL_VPN internal
group-policy GroupPolicy_SSL_VPN attributes
 dns-server value 10.9.10.110 10.9.10.111
 vpn-tunnel-protocol ssl-client
 default-domain value cisco-x.com
 vpn-tunnel-protocol ikev1 ikev2 ssl-client ssl-clientless
!
tunnel-group SSL_VPN type remote-access
tunnel-group SSL_VPN general-attributes
 address-pool VPN_POOL
 authentication-server-group ISE
 accounting-server-group ISE
 default-group-policy GroupPolicy_SSL_VPN
tunnel-group SSL_VPN webvpn-attributes
 group-alias SSL_VPN enable

Add the Remote Access VPN Pool to the enterprise routing updates.

prefix-list VPN_PREFIX seq 1 permit 10.9.31.0/25
route-map VPN_RM_POOL permit 1
 match ip address prefix-list VPN_PREFIX
!
router eigrp 101
 redistribute static route-map VPN_RM_POOL
```

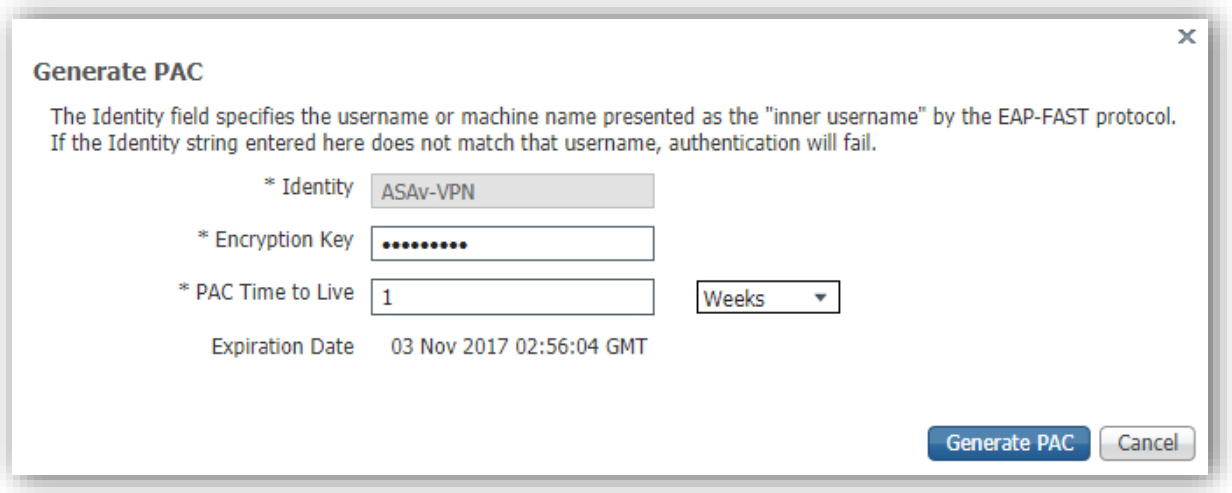
つ目次に戻る

ステップ 2：ASA AAA と TrustSec の設定を行います。

```
aaa-server ISE protocol radius
aaa-server ISE (inside) host 10.9.10.51
 key Cisco1234
 radius-common-pw Cisco1234
!
cts server-group ISE
cts sxp enable
cts sxp default password Cisco1234
cts sxp default source-ip 10.9.30.10
cts sxp connection peer 10.9.10.51 password default mode peer speaker
```

TrustSec クラウドに参加するには、ASA を Protected Access Credential（PAC）で認証する必要があります。ASA は自動 PAC プロビジョニングをサポートしていないため、そのファイルを ISE で手動で生成し、ASA にインポートする必要があります。

ステップ 3：[管理（Administration）] > [ネットワークリソース（Network Resources）] > [ネットワークデバイス（Network Devices）] > [ASAv-VPN] > [TrustSec の詳細設定（Advanced TrustSec Settings）] の順に選択し、ISE サーバで PAC を生成します。[アウトオブバンド（OOB）PAC（Out of Band (OOB) PAC）] プロビジョニングを選択してファイルを生成します。



ステップ 4：PAC を ASA にインポートします。

生成されたファイルは HTTP/FTP サーバに配置できます。ASA はこれを使用して、ファイルをインポートします。

```
ASA-VPN# cts import-pac ftp://10.9.10.19/ASAv-VPN.pac password Cisco1234 !PAC
Imported Successfully

ASA-VPN# show cts pac

PAC-Info:
Valid until: Jan 04 2018 19:48:53
AID:         f27245406549e7f85ace32f2bceb8a5e
I-ID:        ASAv-VPN
A-ID-Info:   Identity Services Engine
PAC-type:    Cisco TrustSec
PAC-Opaque:
000200b000030001000400010f27245406549e7f85ace32f2bceb8a5e0006009400030100da505
e29bedc2771e9b15748dd79aeb70000001359ee79c500093a80ade9899465c87f6a366a8bab90
56215c153c9b86e96e33e90ca49298fe0b144cd2a08748b9dd942150f51f40002a06f34a9ab59
17d8a2152164c1e6307ded78db2b79a8ee8a1e0a5b415e9f0661b97d9c2c9e8c3cb90d849d1c3
c5b4aabddb0f69ef913e3c26f7571c525e46ec7c9de4a4b1a
```

適切な PAC がある場合は、ASA が自動的に環境情報の更新を実行します。これにより、現在の SGT グループに関する情報が ISE からダウンロードされます。

```
ASA-VPN# show cts environment-data sg-table

Security Group Table:
Valid until: 19:50:32 PDT Oct 27 2017
Showing 40 of 40 entries
SG Name                          SG Tag     Type
-------                          ------     -------------
ANY                               65535     unicast
ContractorsSGT                        5     unicast
EmployeesSGT                          4     unicast
IoT_DeviceSGT                        20     unicast
IoT_Manufacturing_Contorl_Sys        25     unicast
IoT_Manufacturing_Monitor_Sys        26     unicast
Network_Services                      3     unicast
OTHER_UNTAGGED                       37     unicast
PartnersSGT                          38     unicast
Quarantined_SystemsSGT              255     unicast
TrustSec_DevicesSGT                   2     unicast
Unknown                               0     unicast
```

ステップ 5：インラインでパケットにタグを付け、タグ付きパケットを信頼します。

```
interface GigabitEthernet0/1
 nameif inside
 cts manual
  propagate sgt
```

リモート アクセスにおけるグループ ポリシーの access-list フィルタは、security-group 属性をサポートしていません。そのため、VPN ユーザ ポリシーで TrustSec SGT を活用できるようにインターフェイスベースのアクセス権限を設定する必要があります。

つ目次に戻る

ステップ 6：インバウンド VPN セッションのインターフェイス アクセス リストをバイパスするために、VPN のデフォルト機能を無効にします。

```
no sysopt connection permit-vpn
```

ステップ 7：タグではなくセキュリティ グループ名を使用して外部接続用インターフェースで *PartnersSGT* から *IoT_DeviceSGT* へのトラフィックを許可する ACL を設定します。さらに、Industrial DMZ 内のリモート デスクトップ アクセス サーバにアクセスを追加します。

```
object network RemoteAccessServer
 host 10.9.103.31
!
access-list outside_access_in extended permit ip security-group name
PartnersSGT any security-group name IoT_DeviceSGT any
!
access-list outside_access_in extended permit ip security-group name
PartnersSGT any object RemoteAccessServer
!
access-group outside_access_in in interface outside
```

これで ASA は VPN ユーザを分類し、SGT に基づいたアクセス制御を実行できるようになります。

Cisco TrustSec の監視

Cisco TrustSec を管理するコマンドは、次のとおりです。

- show running-config cts
- show running-config [all] cts role-based [sgt-map]：このコマンドは、ユーザが定義した IP-SGT バインディング テーブルのエントリを表示します。
- show cts sxp connections：このコマンドは、複数のコンテキスト モードが使用されている場合に、ASA における特定のユーザの SXP 接続を表示します。
- show conn security-group：すべての SXP 接続のデータを表示します。
- show cts environment-data：ASA のセキュリティ グループ テーブルに含まれる Cisco TrustSec 環境の情報を表示します。
- show cts sgt-map：制御パスの IP address と security グループのテーブル マネージャのエントリを表示します。
- show asp table cts sgt-map：このコマンドは、データパスで維持される IP address-security グループ テーブル マッピング データベースの IP address と security グループ テーブルのマッピング エントリを表示します。
- show cts pac：ISE から ASA にインポートされた PAC ファイルの情報を表示します。また、PAC ファイルが有効期限切れになるか、有効期限まで 30 日以内になったときに表示される警告メッセージが含まれます。

検証テスト

シスコでは、Converged Plantwide Ethernet（CPwE）の設計から、広範な可視性を得るために、ネットワークのフローをキャプチャおよび分析できる Stealthwatch を追加しました。Cisco Identity Services Engine、Firepower Management Center、および Stealthwatch 間で pxGrid の通信を実装し、CPwE 設計向けの Network as an Enforcer（NaaE）および Rapid Threat Containment 設計ガイドで説明されている機能を使用できるようにしました。

IoT デバイスに対しては、MAB、SGT を利用した TrustSec、ベンダー固有のプロファイリング等に基づいて、プロファイル ベースのセグメンテーションができるようになりました。Industrial DMZ に TrustSec の SGT とポリシーを追加することにより、CPwE への安全なリモート アクセスを強化しました。

ソリューション検証テストは、Windows サーバ、クライアント ワークステーション、およびさまざまな IoT システムと IoT デバイスで構成される代表的な企業ネットワークを作成して実施しました。IoT デバイスは、両方のハードウェアのプログラマブル ロジック コントローラ（PLC）、PIC、ビルディング システム、および Arduino などの仮想 OS がベースになっています。通信フローおよびポリシー適用テストの大部分は、（ping、トレース、Web コール、ファイル転送、認証、MAB などの）テストのためにより簡単に通信を制御できる PC から行いました。

テクノロジー

- セグメンテーション：ISE + TrustSec、Firepower
- 可視性：ISE、Stealthwatch、Firepower、Umbrella
- 安全なリモート アクセス：AnyConnect VPN

タスク リスト/検証：

- 802.1X、MAB を利用したデバイス認証、SNMP によるプロファイリング、SGT の割り当て
- すべてのデバイスからの通信フローを Stealthwatch で収集、監視、分析
- システムで通信が変更された場合にアラートを生成するよう Stealthwatch のポリシーを設定（PLC-PLC 変更マップ）
- TrustSec SGT と SGACL を使用して産業用スイッチでネットワークをセグメント化
- Stealthwatch のコンソールからシステムを使用して手動隔離を実施
- PxGrid により Firepower Management Center を ISE と統合し、リモート ユーザの自動的な隔離を実施することで、マルウェアに感染したシステムをネットワークから排除
- Umbrella Enterprise を使用してインターネットで通信を行っている IoT デバイスを可視化

これらのタスクはいずれも、このガイドに記載されている実装設定を使用して正常に行われました。

つ目次に戻る

IoT デバイスの統合に関するベスト プラクティス

このソリューションを補完するベスト プラクティスは、次のとおりです。

1. IoT デバイスからアクセスする必要があるすべてのサービスを特定します（通信に関するポリシーを作成します）。
2. それぞれの IoT デバイスのシステムをセグメント化し、そのセグメンテーションを定期的にテストします。
3. 可能な限りすべて（デバイス、リモート、企業）のネットワークへのアクセスを認証します。
4. IoT のネットワーク通信を監視して正常なフローを文書化し、必要に応じてレビューと更新を行います。
5. 特定された異常を迅速にエスカレーションして処理を行えるよう、IoT デバイスの所有者と管理者/監視者を明らかにします。

119

まとめ

IoT システムのセキュリティは、今後数年で 300 億台を超えるデバイスがネットワークに接続されるようになると見られている中で拡大し続けている課題です。攻撃が成功されてしまうと、組織のビジネスに大きな悪影響をもたらされます。

このソリューションは、ユーザのデバイスと IoT システムのセグメンテーションを強化したり、ネットワーク上にどのようなものがいるのか、誰と通信しているのかという可視性を向上させたり、安全でないモデムやリモート サポート システムを安全な VPN ベースのリモート アクセスに置き換えたりすることにより、組織の運営を維持するという目標を達成します。これにより、重要なシステムの制御が失われる可能性が非常に低くなります。

IoT のデジタル化と展開におけるセキュリティのリスクを最小限に抑えるには、まず自社の準備状況を評価し、セキュリティと IoT の取り組みを統合することで IoT とデジタル ビジネスの変革に向けた強力なセキュリティの基盤を築きます。

セキュリティ ネットワーク侵入評価から開始し、それに続いて自動化および制御システム リスク評価を行います。これらの評価でリスクと脆弱性を特定したら、現在のビジネスに合ったインシデント対応計画を作成して影響評価を行います。最後に、セグメンテーションの強化、分析による可視性の向上、および IoT と従業員の環境をデジタル化するための安全なリモート アクセスの実現に向けたロードマップを作成します。このガイドに記載されているベストプラクティスに従えば、インシデント対応計画を改善し、攻撃が成功した場合のビジネスへの影響を軽減できます。

つ目次に戻る

120

参考資料

Cisco SAFE によるセキュリティの簡素化：
https://www.cisco.com/c/ja_jp/solutions/enterprise/design-zone-security/landing_safe.html

Network as a Sensor：
https://www.cisco.com/c/ja_jp/solutions/enterprise-networks/enterprise-network-security/net-sensor.html
https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Feb2017/CVD-NaaS-Stealthwatch-SLN-Threat-Visibility-Defense-Dep-Feb17.pdf

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：
https://www.cisco.com/c/en/us/solutions/enterprise-networks/rapid-threat-containment/index.html

Cisco StealthWatch：
https://www.cisco.com/c/ja_jp/products/security/stealthwatch/index.html
http://www.network-node.com/blog/2016/5/31/stealthwatch-smc-client-part-1 [英語]

Cisco Umbrella セキュリティ：
https://www.cisco.com/c/m/ja_jp/umbrella/index.html?dtid=osscdc000334
DNS のベスト プラクティス：
https://www.cisco.com/c/en/us/about/security-center/dns-best-practices.html
Windows Server 2012 および 2012 R2 での DNS フォワーディングの設定：
https://support.opendns.com/entries/47071344-Windows-Server-2012-and-2012-R2

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

アイデンティティ サービスのための ISE と Firepower 統合のトラブルシューティング
https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200319-Troubleshoot-ISE-and-FirePOWER-Integrati.html

Cisco TrustSec スイッチ コンフィギュレーション ガイド
https://www.cisco.com/c/en/us/td/docs/switches/lan/trustsec/configuration/guide/trustsec.html

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

Cisco Industrial Network Director：
https://www.cisco.com/c/ja_jp/products/cloud-systems-management/industrial-network-director/index.html

つ目次に戻る

121

付録

ラボ図

図 36：Cisco IoT Threat Defense ラボ - サンノゼ

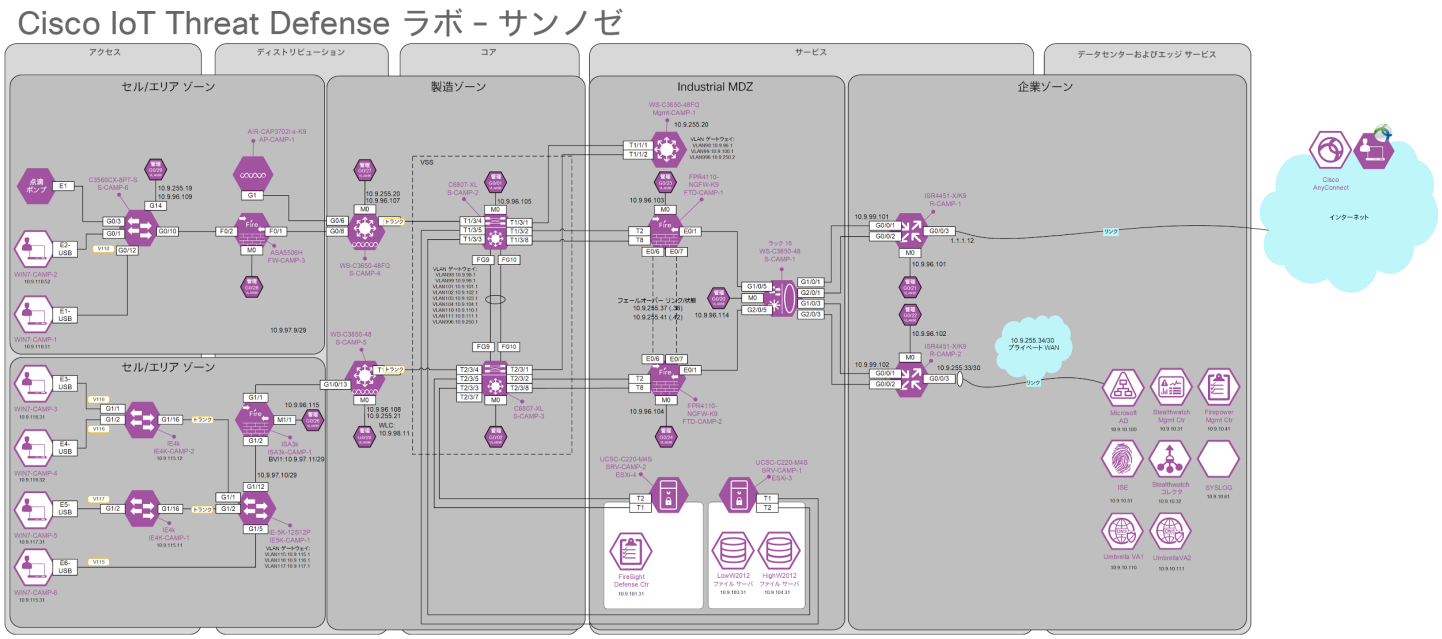
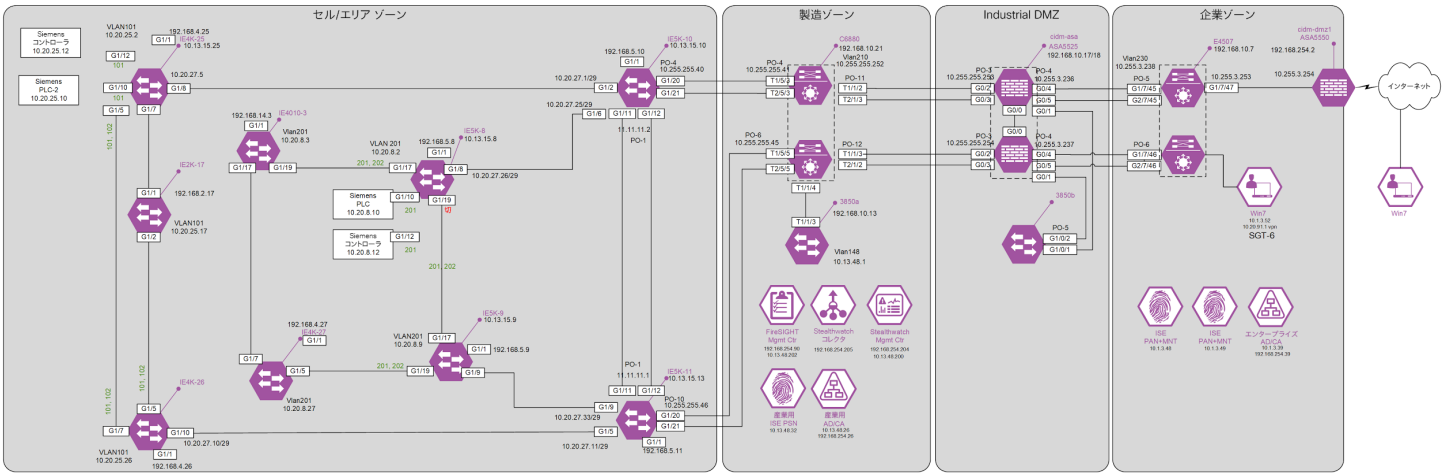


図 37：Cisco CPwE ラボ - RTP（選択されたセグメント）



つ目次に戻る

122

ソリューション製品

IoT Threat Defense ソリューションの検証テストを行うにあたり、以下の製品が実装されました。

表 1：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
Cisco Identity Services Engine（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	仮想または物理アプライアンス	2.4.0.357
Cisco Industrial Network Director（IND）	産業用イーサネット インフラストラクチャの完全な可視性と制御の実現	ソフトウェア	1.4.0-216
Cisco Firepower Management Center	Firepower Threat Defense システムの管理	仮想または物理アプライアンス	6.2.0
FireSIGHT Defense Center	ISA 3000 ファイアウォール（FTD 非搭載）の管理	仮想	5.4.1.9
Cisco Stealthwatch	NetFlow の収集と分析	仮想または物理アプライアンス	6.9.0
Cisco Cognitive Threat Analytics	Stealthwatch からのフローの分析	クラウド	該当なし
Cisco Umbrella	ネットワーク上の IoT のセキュリティを確保する DNS ベースのセキュア インターネット ゲートウェイ	クラウド	2.1.0
Cisco AnyConnect	セキュア モビリティ クライアント	Windows	4.5.00058
Cisco 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
Cisco ASA	ファイアウォール	ISA 3000、ASA 5500-X	9.7(1)4
ASA-ASDM	ローカル FW 管理	ISA 3000、ASA 5500-X	7.7(1)
ASA 上の NGIPS	保護と制御	ISA 3000、ASA 5500-X	5.4.1.8+
産業用イーサネット スイッチ	IPSERVICES を有効にした高耐久性スイッチ	IE 4000、IE 5000、3560-CX	15.2(6)E1
Cisco Catalyst スイッチ	コア	6807-XL	15.4(1)SY
	アクセス/ディストリビューション	3650、3850	16.3.3

つ目次に戻る

お問い合せ先

シスコシステムズ合同会社

〒107 - 6227 東京都港区赤坂 9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp