Cisco TrustSec

セキュア ボーダレス ネットワークの基本コンポーネント

At-A-Glance

顧客の課題に対応

物理的な境界線はなくなろうとしています。顧客が求めるのは、モバイルワーカーのサポート、アウトソーシングの管理、および IT のコンシューマ化への対応です。また、脅威にさらされる環境下で、ビジネスインフラストラクチャと貴重な情報資産をより効果的に保護することも求められています。さらに、法規制や業界での義務により、多くの組織が厳しいコンプライアンスへの対応を強いられています。セキュア ボーダレス ネットワークの基本コンポーネントである Cisco® TrustSec ソリューションは、コラボレーションの保護、セキュリティの強化、およびコンプライアンス要件への対応を容易にします。

主要な機能

Cisco TrustSec は、すべてのユーザに適用される可視性と制御を確率し、IP 対応デバイスの検出および監視により、ネットワークや業務に欠かせないリソースへのアクセスを包括的に保護します。その手段として、ポリシーベースのアクセス制御、ID 認証ネットワーキング、およびネットワーク内でのデータの機密性と整合性の保護が行われます。

ポリシーベースのアクセス制御：Cisco TrustSec は、ユーザ（従業員、請負業者、ゲストなど）、エンドポイントのデバイス（ノートパソコン、IP フォン、プリンタ）、およびネットワーキングデバイス（スイッチ、ルータなど）に対して、一貫するポリシーに基くネットワークアクセス制御を提供します。Cisco TrustSec には、どのような方法でユーザまたはデバイスがアクセス許可を得るか、どのセキュリティポリシー（ポスチャ準拠性など）をエンドポイントデバイスが満たす必要があるか、どのネットワークリソースについてネットワーク内での使用をユーザに許可するかを制御する機能があります。

ID 認証ネットワーキング：Cisco TrustSec では、エンド ユーザやデバイスの ID 情報に時間、場所、組織でのユーザの役割などの情報も加えて、セキュリティポリシーが厳密に制御されます。TrustSec にはロールベースのネットワーキングサービス機能もあり、Cisco メディアネットのサポートや、特定のロールを持つユーザに関連付けられた業務上欠かせないアプリケーションの QoS（Quality Of Service）などが提供されます。

データの整合性と機密性：Cisco TrustSec は、IEEE 802.1AE 規格の暗号を使ってスイッチング環境のデータパスを保護します。データの整合性と機密性は、デバイス間でホップバイホップをベースとするスイッチポートレベルで実現されます。シスコのスイッチングインフラストラクチャは、ファイアウォール、侵入防御、コンテンツインスペクションなどの重要なセキュリティアプリケーションがデータ ストリームの可視性を保てるよう制御を維持します。

利点

コラボレーションをセキュリティで保護：Cisco TrustSec では、アクセスとサービスがユーザおよびデバイスに動的に割り当てられるため、従業員はどこにいても業務ができます。TrustSec から提供される一貫性、効率性、およびロール認識性を兼ね備えたネットワーキング機能は、安全性の高いコラボレーション業務環境とシームレスなユーザ エクスペリエンスを実現します。

セキュリティの強化：Cisco TrustSec は、ネットワークとリソースへのアクセスを保護します。有線、ワイヤレス、または VPN のいずれであっても、エンドポイントデバイスは認証され、健全であることが確認されます。TrustSec は、セキュリティポリシーをネットワーク全体に適用します。また、TrustSec は、スイッチポートレベルの暗号化を使ってネットワークデータの機密性と整合性を保護します。

コンプライアンスへの対応：Cisco TrustSec では、誰がネットワークを利用しているか、その利用者がネットワークで何をしているか、どの種類のリソースへのアクセスが利用者に許可されているかを把握できるので、コンプライアンス要件に対応することが容易になります。顧客は、この情報と機能を使って、管理、監査、およびレポーティングを通常の業務の一部として行い、コンプライアンス要件を満たすことができます。

製品ポートフォリオ

Cisco TrustSec は、インフラストラクチャ、ポリシー、およびエンドポイントの 3 つの製品コンポーネント グループで構成されます。

インフラストラクチャ コンポーネント：Cisco Catalyst® シリーズ 2900/3560/3700/4500/6500 スイッチおよび Cisco Nexus ™ 7000 スイッチは、対話方式でネットワークユーザの認証と承認を行います。ネットワークへのアクセスは、ポリシー、ユーザのアイデンティティ、およびその他の属性に従って決定されます。802.1X、Web 認証、MAC 認証バイパスなどの多様な認証方式が、スイッチポートごとに 1 つの設定によって完全に制御されます。さらに、シスコのスイッチは、データパケットにユーザのアイデンティティ情報をタグ付けできるので、ネットワーク内のどこへでも制御を展開できます。また、Cisco Nexus スイッチは、ネットワークで送信中のデータ（DIM：data-in-motion）の機密性と整合性を保護するために MACSec（IEEE 802.1AE 規格暗号化）をサポートしています。

ポリシーコンポーネント：Cisco Secure Access Control System（ACS）は、シンプルながら強力な機能を備えたポリシーサーバであり、中央集中型のネットワークアイデンティティとアクセス制御を処理できます。Cisco Secure ACS は、最適な制御と可視性を提供するために設計されたルールベースのポリシー モデルと新しい直感的な管理インターフェイスを備えています。最新の Cisco Secure ACS では、IT 管理者が総合的なモニタリングとトラブルシューティングの機能を使って、潜在的な問題を速やかに特定できます。

Cisco TrustSec

セキュア ボーダレス ネットワークの基本コンポーネント

Cisco Network Admission Control（NAC）Manager は、アプライアンスベースの NAC 展開環境において、ロールベースのユーザ アクセス ポリシーとエンドポイント セキュリティ ポリシーを定義するための管理センターとなります。

Cisco NAC Server は、アプライアンスベースの NAC 展開環境でのセキュリティポリシー準拠性を評価し、適用します。

Cisco NAC Profiler は、すべてのエンドポイントデバイスの検出、プロファイリング、ポリシーベースの配置、および接続後モニタリングを提供して、ポリシーベースのアクセス制御を展開しやすくします。

Cisco NAC Guest Server は、ゲストのネットワークアクセスを管理して、ゲストユーザのアカウントとネットワークでの活動に関するプロビジョニング、通知、管理、およびレポーティングを提供します。

エンドポイントコンポーネント：Cisco Secure Services Client（SSC）は、顧客が単一の認証システムを展開して有線とワイヤレスの両方のネットワークにアクセスできるようにします。Cisco SSC では、802.1X を使ってユーザとデバイスが認証され、ユーザとデバイスのアイデンティティ、およびアクセスを保護するためのネットワークアクセスプロトコルが管理されます。また Cisco NAC Agent は、エンドポイント デバイスで実行されるエージェントで、デバイスのレジストリ設定、サービス、およびファイルを分析して、セキュリティプロファイルの詳細なインスペクションを実行します。標準デバイスをサポートする上記 2 つのエンドポイントクライアントに加え、Cisco IP Phone には、Cisco TrustSec ソリューションと統合するための高度な組み込みのクライアント機能があります。

TrustSec 向けのプロフェッショナル サービス

シスコおよびパートナーが提供するインテリジェントでパーソナライズされたサービスは、TrustSec ソリューションを展開できるようにネットワークを準備するためにポリシーの確認、分析、および設計を行う専門知識を提供します。シスコのサービスは、ベストプラクティスを使って、組織が完全な認証とアクセスのソリューションをより速やかに、費用対効果に優れた方法で展開できると同時に、継続的な業務効率化のために知識伝達を行えるようにします。

使用例

展開オプション 1：802.1X ベースの展開

このシナリオでは、Cisco Secure ACS は、有線ネットワークに接続するユーザを認証するためのポリシーサーバです。ネットワークアクセスデバイス（スイッチ）は、ユーザの資格情報（Cisco SSC によって収集される）と組織での役割に基づいてネットワークとリソースへのアクセスを提供します。セキュリティグループタギング、セキュリティグループ ACL など、追加保護機能を適用すると、より厳密な制御が可能になります。Cisco NAC Profiler と Cisco NAC Guest Server を 802.1X ソリューションと共に展開することもできます。

展開オプション 2：アプライアンスベースの展開

アプライアンスベースのアプローチでは、Cisco NAC Manager がポリシーサーバとして Cisco NAC Server と連携してユーザを認証し、LAN、ワイヤレス、または VPN の接続を介してデバイスを評価します。ネットワークとリソースへのアクセスは、ユーザの資格情報と組織での役割のほか、エンドポイントデバイスのポリシー準拠状況に基づいて提供されます。

TrustSec の革新技術

TrustSec は、シスコの多数の革新技術を搭載しています。802.1X モニタリングモードと低影響モードは、高度な可視性、より柔軟な展開、および強化された運用サポートを提供できるように、認証に先立ってネットワークアクセスを制御下に置き、完全に設定可能な状態にします。Cisco NAC Profiler、Guest Server、および IP テレフォニーが 802.1X 環境でシスコのスイッチと統合されることで、IT と従業員の生産性が劇的に向上します。セキュリティグループ ACL は、IP アドレスに基づく ACL の代わりに、セキュリティグループメンバーシップをエンドユーザと適切なリソースアクセス権に割り当て、セキュリティポリシーの管理を簡略化します。TrustSec は、802.1X-REV、MACSec などの高度なセキュリティ技術を顧客に提供します。

シスコが選ばれる理由

Cisco TrustSec は、展開時の柔軟性、操作性、および効率性に優れた包括的なソリューションです。セキュリティをインフラストラクチャ内部に組み込んで、管理対象または管理対象外の資産および不明な資産、従業員、ゲスト、請負業者をサポートします。

シスコのネットワークは、TrustSec が提供する完全な可視性と制御によって保護されます。Trustsec は、ネットワークの復元力、一貫性、およびスケーラビリティを向上します。

シスコとパートナーは、顧客ごとに異なるコンプライアンスとセキュリティのニーズを満たすのに役立つプロフェッショナルサービスを提供します。

詳細については、http://www.cisco.com/jp/go/trustsec/ を参照してください。

C45-577269-00 03/10