Cisco NAC アプライアンス（Clean Access）概要

復元力のあるネットワークにはセキュリティ ポリシーの徹底が必要

ネットワークに害を与える脅威の多くは、システムに脆弱性を抱えたデバイスや、最新のセキュリティ対策が施されていないデバイスを使ってネットワークにアクセスしたユーザによってもたらされます。ネットワークへのログイン時点で、デバイスの種類や所有者に関係なくセキュリティ ポリシーを適用することが、脆弱性を持つデバイスによってネットワークのセキュリティが損なわれることを避けるための方策です。

Cisco NAC（ネットワーク アドミッション コントロール）は、ネットワークのコンピューティング リソースにアクセスするデバイスに対して、ネットワーク インフラストラクチャを使用してセキュリティ ポリシーを適用するソリューションです。

NAC では、セキュリティ ポリシーに準拠しないデバイスに関連するリスクを最小化し、復元力と安全性の高いネットワークを実現します。

また、NAC にはネットワーク レベルでユーザ認証を行う機能があるため、適切なユーザ クレデンシャルを持つユーザだけにネットワークへのアクセスを許可することができます。

効果的なソリューションの鍵

セキュリティ ポリシーの適用とは、接続を試みるデバイスをスキャンして活動中の感染がないかどうかを調べることだけを意味するのではありません。企業の生産性を低下させることなく、ユーザとデバイスに対して要件を一律に適用するための手段です。効果的にポリシーを適用するためには、以下を実行する必要があります。

- **識別と認証**：ユーザとデバイスを一意に識別し、その間に関連付けを作成します。
- **スキャンとポスチャの適用**：ネットワーク全体に対して一貫性のあるポリシーを評価し、適用します。
- **検疫と感染修復**：ポスチャ評価の結果に基づいてデバイスを隔離し、その結果を基準に取り込みます。
- **管理と構成**：簡単な操作によって包括的で詳細なポリシーを作成し、ユーザのグループやロールにマップします。

アプライアンスによるネットワーク アドミッション コントロールの実装

Cisco® NAC アプライアンス（Clean Access）は、ポリシー適用のための機能を包括的に提供する製品です。Cisco NAC アプライアンスを導入することでネットワーク管理者は、ネットワークへの接続を許可する前に、有線および無線経由のユーザ、リモートのユーザおよびそのマシンを認証、承認、評価、感染修復することができます。Cisco NAC アプライアンスは、マシンがセキュリティ ポリシーに準拠しているかどうかを判別し、脆弱性を修復してから、ネットワークへのアクセスを許可します。

Cisco NAC アプライアンスの利点

Cisco NAC アプライアンスは、現在の市場で最も多く導入されているソリューションであり、すでに 600 を超えるさまざまな規模のお客様が利用しています。他のソリューションでは、状況に応じて異なる複数の製品を必要とします。しかし、このソリューションの場合は、Cisco NAC アプライアンスを導入するだけで、LAN、リモート アクセス/VPN、ワイヤレス、ブランチ オフィス、エクストラネットのすべてのユーザにポリシーへの準拠を適用することができます。

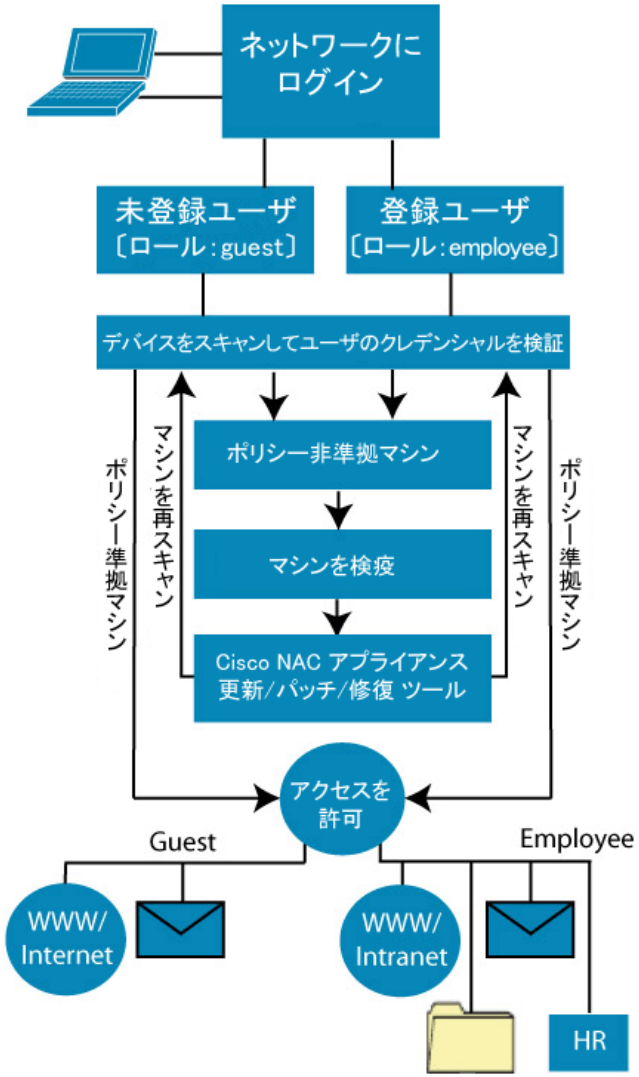
Cisco NAC アプライアンスは、ネットワークの安全性を高めるためのプロアクティブなツールであるだけではありません。

- インフラストラクチャ、企業の機密情報、社内の知的財産を守ることにより、ビジネスの利益を保護します。IT 部門は、セキュリティの境界が消えつつあること、不正なアクセス、および内部からの攻撃によってもたらされる、機密に関する脅威を防御することができます。
- 悪意のある動作および攻撃がネットワークの機能を損なうのを阻止することにより、組織の信頼感、ブランド名、社会的なイメージを守ります。
- 脆弱性に起因する不正利用と攻撃を軽減および排除することにより、従業員の生産性を向上させます。このコントロールを使用することで、お客様はインフラストラクチャの大規模な損傷、生産性の低下、直接的な金額的損失を避けることができます。
- 組織が SOX 法や HIPAA などのプライバシー保護および適合規格の要件を遵守するのに役立ちます。遵守する必要がある法的な要件を満たすことができない組織は、顧客や規制当局との関係を危険にさらすことになります。

Cisco NAC アプライアンスのコンポーネント

- **Clean Access Server** - エンド ポイントがポリシーに適合しているかどうかに基づいて、評価を開始し、アクセス権限を決定するデバイスです。
- **Clean Access Manager** - ユーザのロール、チェック、ルール、およびポリシーを確立するための Web ベースの集中管理コンソールです。
- **Clean Access Agent（オプション）** - 脆弱性評価機能の一部を拡張し、修復を効率化するコンパクトな読み取り専用のエージェントです。

Cisco NAC アプライアンス（Clean Access）概要



Cisco NAC アプライアンスの機能

シングル サインオンを可能にする認証との統合

Cisco NAC アプライアンスは、ほとんどの認証方式で認証プロキシとして機能します。Kerberos、Lightweight Directory Access Protocol（LDAP）、RADIUS、Active Directory、S/Ident などの認証方式と統合可能です。エンド ユーザの手間を最小限に抑えるために、Cisco NAC アプライアンスは VPN クライアント、ワイヤレス クライアント、および Windows Active Directory ドメインに対してシングル サインオンをサポートしています。ロールベースのアクセス制御がサポートされているため、管理者はさまざまなアクセス レベルの複数のユーザ プロファイルを維持できます。

脆弱性の評価

Cisco NAC アプライアンスは、すべての Windows ベースの OS、Mac OS、Linux マシンのほか、ゲーム機のコンソール、PDA、プリンタ、IP フォンなど、ネットワークに接続された PC 以外のデバイスのスキャニングをサポートしています。Cisco NAC アプライアンスではネットワークベースのスキャンを実施しますが、必要に応じてカスタムビルトのスキャンを実施することもできます。Cisco NAC アプライアンスは、レジストリ キー設定、実行中のサービス、またはシステム ファイルによって任意のアプリケーションを識別することができます。

デバイスの検疫

Cisco NAC アプライアンスは、ポリシーに適合していないマシンを検疫エリアに接続させます。これによって、修復のためのリソースにはアクセスできるようにしながら、感染の拡大を防ぐことができます。検疫には、/30 程度のサイズの小さいサブネットを使用するか、検疫 VLAN を使用します。

セキュリティ ポリシーの自動更新

標準的なソフトウェアのメンテナンス パッケージに組み込まれているシスコシステムズが提供するセキュリティ ポリシーの自動更新機能では、重要な OS の更新や一般的なアンチウイルス ソフトウェアのウイルス定義の更新、一般的なアンチスパイウェア ソフトウェアの定義の更新をチェックするポリシーをはじめ、一般的なネットワーク アクセス条件に関するポリシーを事前に設定しています。これにより、ネットワーク管理者は Cisco NAC アプライアンスを利用して常に最新のポリシーを維持することができるため、管理コストを軽減できます。

中央集中型の管理

管理者は、Cisco NAC アプライアンスの Web ベースの管理コンソールを使用して、ロールごとに必要なスキャンのタイプと、リカバリに必要な関連する修復パッケージを定義することができます。1つの管理コンソールから複数のサーバを管理できます。

修復

Cisco NAC アプライアンスの検疫機能によって隔離されたデバイスには、修復サーバへのアクセス権が与えられます。修復サーバは、OS のパッチとアップデート、ウイルス定義ファイル、または Cisco Security Agent などのエンドポイント セキュリティ ソリューションを提供することができます。管理者は、Cisco NAC アプライアンス エージェントによる自己修復を有効化するか、Windows アップデートの自動起動を行うか、修復手順を記載した一連の Web ページを指定できます。

柔軟な導入モード

Cisco NAC アプライアンスは、きわめて広範な導入モードを備えているため、あらゆるお客様のネットワークに適合させることができます。お客様は導入時に、仮想 IP または物理 IP のゲートウェイ、末端または中央、レイヤ 2 またはレイヤ 3 のクライアント アクセス、およびインバンドまたはアウトオブバンドのネットワーク トラフィックを選択できます。

関連情報

詳細については、シスコの営業担当者にご連絡いただくか、http://www.cisco.com/jp/go/nac/appliance をご覧ください。

06.12