

Great Bay Software の Beacon System とシスコ ネットワーク アドミッション コントロール

概要

Great Bay Software の Beacon システムは、Cisco NAC アプライアンスとの統合によってネットワーク アドミッション コントロール (NAC) ソリューションの高度な導入を可能にします。Beacon システムと Cisco NAC アプライアンスの組み合わせにより、すべてのエンドポイント デバイスの検出とプロファイリングが、特定のユーザに関連付けられているかどうかに関係なく簡素化されます。また、Beacon では導入後にデバイスの識別情報、場所、および追加、移動、変更を管理できるため、エンドポイントの高度な管理が可能です。

Cisco NAC アプライアンスの概要

Cisco NAC アプライアンスは、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すべてのデバイスに対して、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 ポリシーを確実に適用します。Cisco NAC アプライアンスを使用することにより、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。ノート PC、IP 電話、ゲーム機のコンソールなどのネットワーク デバイスが組織のセキュリティ ポリシーに適合しているかどうかを識別し、脆弱性があれば、ネットワークへのアクセスを許可する前に修復します。Cisco NAC アプライアンスの管理コンソールは、Cisco Clean Access Manager です。

エンドポイント プロファイリング

すべてのデバイスまたはエンドポイントをすばやくプロファイリングして管理することが NAC の主な目的です。多くのエンドポイントはユーザが使用するデスクトップおよびノート PC ですが、ネットワーク上にはそれ以外にも IP 電話やプリンタなど、ユーザから独立した多くのエンドポイントが存在します。これらは、「非応答ホスト」または「関連付けられていないデバイス」と呼ばれることがあります。

Beacon は、すべてのネットワーク エンドポイントのプロファイリングを行い、ネットワーク エッジの状態を正確に表すことで、強力な認証を実現し、また、その認証に従います。次のような数多くの情報源がオプションとして組み合わせられます。

- ネットワーク トラフィックを集約ポイントで監視した結果
- エンド ステーションの動作
- NetFlow データの取り込み
- ポートの状態 (場所) の継続的な監視
- アクティブなプロファイリング

ネットワーク上のデバイスの 20% から 40% が非応答ホストであることが想定されるため、効果的な NAC ソリューションを実現する上で、この情報の重要性は増しています。

NAC ロールアウトの推進

Cisco NAC アプライアンスは、アクセス許可の手順を標準の Web ブラウザを通じて、またはエンドポイントに常駐する軽量で読み取り専用のクライアントを通じて開始します。ユーザは自分のクレデンシャルを入力します。このクレデンシャルにより、アクセス権およびポリシーの必要条

件が決まります。Cisco NAC アプライアンスは、ユーザによるそのような操作を実行できないデバイスにアクセスを許可する場合、Clean Access Manager の例外リスト（フィルタ リスト）を使用します。ここには、この種の非応答ホストの MAC アドレスがリストされています。フィルタ リスト上のデバイスがネットワークへのアクセスを試みると、NAC アプライアンスはロールベースの VLAN 割り当てによって適切にルーティングします。

フィルタ リストは、MAC アドレスの一括インポートか、手動による MAC アドレスの入力によって作成されます。NAC 全体で使用するためには、コンパイルと組み込みが必要です。さらに、変更の発生に合わせて非応答ホストのリストを最新の状態に保つ必要があります。たとえば、新しく追加したネットワークプリンタを接続できるようにするには、その MAC アドレスをフィルタ リストに追加する必要があります。同様に、デバイスが永久にネットワークから削除される場合、管理者はその MAC アドレスを削除する必要があります。

このプロセスを簡素化するために、Beacon はすべてのエンドポイントについて、MAC アドレスだけでなくデバイス タイプ記述子（プリンタ、IP 電話、無停電電源装置など）および適切なアクセス タイプの値を含む自動インベントリを生成します。アクセス タイプの値は、適切なアクセス レベルを決定します。Beacon は、フィルタ リストを自動的に Clean Access Manager に組み込み、管理ネットワークへのアクセスが許可されたデバイスのリストが有効で正確になるように、そのリストを継続的に管理します。

非応答ホストに対する制御の強化

管理の観点からは、ネットワークに対するデバイスの追加および削除の際、Beacon はエンドポイント環境での変更を動的に検出します。管理者は、フィルタ リストを手動で更新する必要がなくなります。それ以上に重要なことは、この機能によって MAC アドレスのスプーフィングの可能性が排除されることです。

また、Beacon と Cisco NAC アプライアンスを組み合わせたソリューションでは、エンドポイントの動作の変化がデバイス タイプの変更を示している場合、そのことを検出できます。プリンタが Internet Explorer でインターネットにアクセスするなど、デバイスのプロファイルと整合性のないイベントが発生すると、疑わしいエンドポイントをフィルタ リストから削除したり、デバイスの機能変更に対応するためにプロビジョニングを再実行するように、Beacon は Clean Access Manager に通知できます。

全面的に統合されたユーザ インターフェイス

Beacon からのデータは、Cisco Clean Access Manager の Web ベースのインターフェイスに表示されます。これにより、NAC システムの詳しい状態を 1 か所で把握することができます。NAC 管理者はフィルタ リストにあるエンドポイントの現在の状態を一目で見ることができるので、管理の負荷が軽減され、トラブルシューティングが簡単になります。

まとめ

NAC ソリューションを導入する際のコンポーネントとして、エンドポイントのプロファイリングの重要性は高まっています。Great Bay Software の Beacon によるソリューションでは、導入時間が大幅に削減され、継続的なメンテナンスは非応答ホストの場合を中心に簡素化され、動作ベースのサーベイランスによってセキュリティが向上します。Beacon と Cisco NAC アプライアンスの組み合わせは、企業のあらゆる資産に対して信頼できるアクセスを提供するための包括的なソリューションです。

ソリューションの利点

Beacon と Cisco NAC アプライアンスを組み合わせたソリューションは、NAC 管理者にとって主に3つの利点があります。

- エンドポイントを自動的にプロファイリングするため、Cisco NAC アプライアンスの初期導入時の手間と時間が大幅に削減されます。管理者は、データ入力や物理的なインベントリではなく、ポリシーや構成に関する事項に、より多くの時間をかけることができます。
- ネットワークに対するデバイスの追加および削除を検出できるため、NAC 管理者のメンテナンス負荷が軽減されます。
- エンドポイントの動作のサーベイランスによってセキュリティが強化され、非応答ホストが NAC メカニズムに対する攻撃の起点となることを回避できます。

関連情報

Great Bay Software の Beacon の詳細については、<http://www.greatbaysoftware.com> を参照してください。

Cisco NAC アプライアンスの詳細については、<http://www.cisco.com/jp/go/nac/appliance> を参照してください。

©2007 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、および Cisco Systems ロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の一定の国における登録商標または商標です。

本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用は Cisco と他社との間のパートナーシップ関係を意味するものではありません。(0609R)

この資料に記載された仕様は予告なく変更する場合があります。



シスコシステムズ株式会社

〒107-0052 東京都港区赤坂 2-14-27 国際新赤坂ビル東館

<http://www.cisco.com/jp>

お問い合わせ先 (シスコ コンタクト センター)

<http://www.cisco.com/jp/go/contactcenter>

0120-092-255 (通話料無料)

電話受付時間：平日 10:00 ~ 12:00, 13:00 ~ 17:00

お問い合わせ先