

## **Preparing the network for Cisco's Network Admission Control** *LAN-based NAC deployments are enabled by Endpoint Profiling*

### *The promise of NAC*

Cisco's Network Admission Control delivers a robust and scalable solution to many of the most pressing challenges facing the IT administrator in the realm of secure and trusted computing. Included in these challenges are the reestablishment of a secure perimeter, authentication and verification of the machine and the user attaching to the network, and identifying the state of the machine for use as a credential for that user being granted access to the network.

To date, there have been a number of products and solutions in this space that have addressed these concerns in varying degrees, but none have provided a solution that provides the stability, redundancy, and technological diversity required by commercial and Enterprise companies. These solutions have generally been positioned in small to mid-size higher educational institutions whose challenges regarding the transient nature of their customer base, coupled with a strong philosophical tendency towards open and collaborative systems, have led to an acute challenge that can be largely solved by the products in the market to date. These products have a loose association with other security systems in the network such as Anti-Virus, Anti-SPAM, Anti-Spyware, IDS/IPS, Firewalls, etc., and typically exist on a centralized appliance that controls network access and allows the user base to self-remediate their machines.

The development of NAC represents a significant leap forward on the notion of trusted computing, and delivers the first viable solution to these challenges for large Enterprise networks where a centralized appliance and end user remediation are not acceptable for technological and cultural reasons. NAC leverages 802.1X as a medium for integrating the functions of authentication and authorization into a framework in which the relationship between the user, the machine, the state of the machine, and the aforementioned security components are unified into a cohesive system that protects and enhances the investment in systems ranging from the network infrastructure to directory systems, and all the components in between.

802.1X has been an industry standard for several years, yet its deployment to date has been largely as a mechanism to secure Wireless LANs, more specifically, as a way to allow only known users onto the WLAN, and as a way to frequently change the encryption keys used for communication between the wireless client and the access point. With the development of NAC Phase II, the network administrator now has the opportunity to deploy 802.1X on the wired LAN as a mechanism for unified network-based authentication, and as the foundation for a trusted computing platform to integrate the machine, the user, and the state of the machine as attributes for granting network access and establishing levels of access for different groups within an organization, or to facilitate secure network access for guests, contractors, vendors, etc, without providing them with access to corporate resources.

### *The realities of deploying 802.1X*

Deploying 802.1X in the wireless realm is less complex than in the wired LAN because of two realities: 1) the wireless domain has a small ratio of ports to users, generally 10-30 per "port", where an Access Point represents either a single port or a small number of ports with regard to interface configuration; and 2) most, if not all, of the nodes attached to the wireless medium are laptops or PDAs, meaning they possess an 802.1X client and are capable of authenticating using 802.1X. The wired network, meanwhile, does not share these characteristics. There are more ports than attached endpoints in the wired LAN, and the diversity of endpoint types is dramatically greater than the Wireless LAN. These devices do not yet support 802.1X clients, but their secure connectivity to the network must be provided. Non-802.1X endpoints include printers, Voice over IP Phones, Uninterruptible Power Supplies, HVAC systems, medical imaging machines, etc.

The settings for 802.1X are configured per port, which means the network must be configured to challenge a user to authenticate while provisioning secure connectivity for a printer on the next, and providing secure access for VoIP phone on the third. The deployment of NAC, therefore, requires that the location and type of these non-802.1X endpoints (as well as the 802.1X capable devices) be ascertained prior to the deployment of 802.1X in the wired network. The work of locating all of the attached endpoints using brute force is not only costly in terms time and resources, but it also suffers from inaccuracies related to the cabling plant, the realities of endpoints continuously moving within the Enterprise LAN, and human error. It's notable that adds, moves, and changes are a challenge that resurfaces in the authentication-enabled network because network attached devices cannot move freely within the LAN. This is the desired result from a security perspective, but must be managed effectively to mitigate the possibility of the administrative costs of the feature overwhelming the benefits of implementation.

### *The Solution - Endpoint Profiling*

Great Bay Software has developed a solution to this challenge called Beacon which introduces the concept of Endpoint Profiling as a mechanism to facilitate the deployment of 802.1X and NAC by providing a system for discovering and managing the location and type of all the attached endpoints in the LAN. Beacon allows the network administrator to quickly deploy port settings for 802.1X without having to visit every closet and trace every cable in order to discover what is attached to each port. Beacon understands which device types are attached to which ports making this unnecessary. This provides a dramatic time savings to the IT staff and relieves them from the exceptionally time consuming task of tracking the exact location and type of all attached network endpoints.

The Beacon System gives the network administrator the opportunity to realistically deploy NAC, as well as providing a system to facilitate several administrative tasks in the NAC-enabled network including Adds, Moves, and Changes, location of non-compliant devices, discovering unmanaged endpoints, and quickly locating endpoints in situations such as helpdesk calls, security events, policy violations, and asset tracking.

Endpoint profiling works by aggregating information from a number of sources including Inference-based Discovery, traffic analysis, and the network topology in order to develop an understanding of the types of the devices. The type of the endpoint is aligned with the location of the device to provide a complete picture of the network attached endpoints. In addition, because the system is cognizant of the authentication process, Beacon additionally provides visibility into the machines and people that have authenticated to the network, their location, and their history of network usage.

As mentioned, data sources for Endpoint Profiling include network traffic analysis, Inference-based Discovery, and information available from the network infrastructure such as the Source Address Tables, ARP Cache information, and numerous MIBs. Network Traffic analysis is customized through the creation of Profiles, which consist of rules that can include attributes extending from Layer 2 through Layer 7 of the OSI model. These rules can be combined to create a more detailed picture of the endpoint types, and decipher very slight differences between different endpoint types. Inference-based discovery is a technology that uses information about a single network device to ascertain the relationship between it and all of its associated endpoints. A simple example would be the print server; knowing the IP address of the print server(s) allows Beacon to discover all of the printers associated with that print server. Another common scenario is the Voice gateway, where simply knowing the voice gateway's IP address can be leveraged to quickly and effectively discover all of the IP phones associated to that gateway.

In addition to network traffic analysis and inference-based discovery, Beacon also communicates with the network infrastructure to gather information about the network attached endpoints as well as to better understand the attributes of the network configuration such as inter-switch links, VLAN usage, backplane ports, etc.

#### *Other applications*

The combination of the data sources described (traffic analysis, Inference-based, and network infrastructure communications) allows Beacon to provide real-time and historical information about the network attached endpoints at a very granular level and allows the network administrator to gain a strong understanding about what exactly is attached to the network, where it is, and where it's been. This information is useful for a myriad of things beyond the enabling of network authentication including asset tracking, rogue user detection, and change management functions. In addition, the contextual information provided by Beacon provides systems such as IDS/IPS and vulnerability scanning systems with a level of understanding about what kind of device has been seen in these products, creating a more educated understanding of the event seen, in the case of an IDS/IPS, or the results seen via a vulnerability scanner.

#### *Conclusion*

Endpoint Profiling is an important aspect of preparing the network for the deployment of Network Admission Control. Great Bay Software provides a solution that allows the network administrator to gain a complete understanding of what is attached to the LAN edge. In addition to the provisioning of 802.1X settings, Beacon provides a framework

for Identity and Location management, facilitates the cost effective administration of 802.1X and the authenticated network, and provides complimentary functions to compliance efforts, asset tracking systems, vulnerability scanners, and security systems.