

JUNIPER NETWORKS UNIFIED ACCESS CONTROL AND GREAT BAY SOFTWARE'S BEACON

Facilitating Network Access for Non-802.1X Endpoints

Challenge

Discovering and documenting all network attached endpoints is a task that can consume a great deal of time at a large cost. This has been a principal cause of many stalled authentication projects.

Solution

Great Bay Software's Beacon Endpoint Profiler provides a comprehensive accounting of all network attached endpoints. The information stored within Beacon is leveraged by Juniper Networks UAC to authenticate endpoints that are not running a client for 802.1X—whether they are incapable of doing so, new to the enterprise or in need of temporary access.

Benefits

The Juniper Networks and Great Bay Software joint solution automates the discovery of all network-attached endpoints, provides real-time and historical views of endpoint data, and unifies the authentication of all network-attached endpoints.

The deployment of Juniper Networks® Unified Access Control (UAC) provides an opportunity for enterprise IT organizations to authenticate, manage and secure user-based endpoints devices, such as laptops and PCs. These systems can be challenged for credentials ranging from username and password to the system's certificate and other two-factor-based authentication techniques that allow corporate users to gain network access.

Today's enterprise network, however, is comprised of a number of other network-attached systems that do not fit into the criteria for authenticated network access. As an example, they may not have a user associated with them to enter the credentials, or they may not be able to run the client software required for authentication. These systems typically include network-attached printers, VoIP handsets, uninterruptible power supplies (UPS) and WLAN access points. They can also include other systems that are often overlooked such as facilities management (HVAC systems), security systems, cash registers, audio-visual equipment, and industry-specific devices such as patient care systems in health care, and robotics in manufacturing.

These devices must be identified, located, documented and tracked in order to successfully deploy network-based authentication and/or network access control (NAC). Once located, these systems must be provisioned with the appropriate level of network access, as well as being monitored to ensure that they behave in a fashion that is acceptable given their known identity. The discovery, location and provisioning for these non-authenticating devices is a core function of Great Bay Software's Beacon Endpoint Profiler. The combination of Beacon and Juniper Networks UAC creates a comprehensive network access control and authentication solution for the enterprise network.

The Challenge

Discovering and documenting all network-attached endpoints can be a time-consuming and costly task. This has been a principal cause of many stalled authentication projects. In addition, the troubleshooting and administration of the authenticated network provide a wealth of information not previously available prior to the deployment of authentication and/or NAC.

The fact that every endpoint must be discovered, located and provisioned regardless of whether or not it will participate in the authenticated network makes this a challenging undertaking: because very few enterprises maintain an up-to-date list of all network-attached endpoints. In addition to the discovery that is required for Day One of the deployment, there are several operational considerations that are served by Beacon's comprehensive database of endpoint, location and behavioral information. These include the provisioning of newly acquired endpoints, facilitating network-based machine imaging, help desk scenarios such as troubleshooting network connectivity in the authenticated network, and defending against media access control (MAC) spoofing and shadow host configurations, both of which are security threats to the authenticated network.

The combination of UAC and Great Bay's Beacon provide a comprehensive solution for facilitating network-based authentication of all devices in the enterprise whether they're running an authentication client or not, and for administering the system in a way that unlocks the efficiencies that are possible, given the instrumentation provided by the Beacon system.

The Juniper Networks – Great Bay Software Joint Solution

Great Bay Software's Beacon Endpoint Profiler provides a comprehensive accounting of all network-attached endpoints. This inventory provides a real-time view of each network-attached device's location, MAC address, IP address, identity and behavior, as well as a historical view of these attributes. This information is used to facilitate the deployment of 802.1X and UAC by relieving the requirement to discover all enterprise endpoints manually. The information stored within Beacon is leveraged by UAC to authenticate endpoints that are not running a client for 802.1X—whether they are incapable of doing so, new to the enterprise or in need of temporary access. In concert, this joint solution provides authentication to the entire enterprise and avoids the costly and unwieldy option of manually configuring all network ports.

Features and Benefits

Automated Discovery of All Network-Attached Endpoints

Beacon leverages its Endpoint Profiling technology to assign an identity to all network-attached endpoints, eliminating the need to manually discover and document endpoints as a precursor to the deployment of 802.1X.

Real-Time and Historical Views of Endpoint Data

Beacon's data repository of information allows the network administrator to understand the state of the network-attached endpoints as well as mining data related to a device's location, previous addressing and behavioral attributes.

Unified Authentication of All Network-Attached Endpoints

Leveraging the Beacon Database, UAC is positioned as the central point for authenticating all network-attached devices, including those that will participate in the UAC environment with a client and those that will not. This comprehensive approach to authenticating all devices attached to the network dramatically reduces the time to deploy network access control, and facilitates the mobility for networked devices and users that today's businesses demand.

Advanced Tools for Managing the Authenticated Network

The deployment of network-based authentication and access control unlocks a number of administrative and operational capabilities that have not been possible before now. In particular, the concepts of identity and location as descriptors that can be used for searching, tracking and managing the network are dramatic improvements when compared to the common mechanisms used today such as MAC address, IP address and Ethernet jack number.

Meeting Compliance Requirements

Recent trends in compliance initiatives and audits have focused on internal communication considerations such as rogue devices, tracking locations, and maintaining a real-time and historical account of all network attached devices. Great Bay's Beacon and Juniper Networks Unified Access Control provide these functions and help support organizations in meeting these requirements.

Solution Components

- Junipers Networks Unified Access Control
- Great Bay Software's Beacon Endpoint Profiler

Summary

The implementation of Juniper Networks Unified Access Control and Great Bay Software's Beacon Endpoint Profiler provides a comprehensive solution for authentication and network access control that delivers the level of security demanded by today's enterprise network administrator. In addition, the implementation of this joint solution unlocks operational efficiencies that will actually reduce the cost of administering and managing the network as well as speeding Mean Time to Repair. Finally, as enterprises continue to implement systems that fortify their efforts in adhering to compliance mandates, the UAC—Beacon Software combination provides many additive benefits to meet these requirements.

Next Steps

To learn more about Juniper Networks Unified Access Control and our joint solutions with Great Bay Software, please visit www.juniper.net/uac.

About Great Bay Software

Great Bay Software, Inc. is the innovator of Endpoint Profiling, a technology designed to rapidly establish and maintain a real time view of all network attached endpoints. The company's Endpoint Profiling technology has applications in enabling the deployment and administration of Network Admission Control and network-based authentication, in addressing compliance concerns related to unauthorized devices attaching to the Enterprise network, and in managing the endpoint lifecycle for all network attached devices.

About Juniper Networks

Juniper Networks, Inc. is the leader in high-performance networking. Juniper offers a high-performance network infrastructure that creates a responsive and trusted environment for accelerating the deployment of services and applications over a single network. This fuels high-performance businesses. Additional information can be found at www.juniper.net.

Corporate and Sales Headquarters

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or 408.745.2000
Fax: 408.745.2100
www.juniper.net

APAC Headquarters

Juniper Networks (Hong Kong)
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

EMEA Headquarters

Juniper Networks Ireland
Airside Business Park
Swords, County Dublin, Ireland
Phone: 35.31.8903.600
EMEA Sales: 00800.4586.4737
Fax: 35.31.8903.601

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at 1-866-298-6428 or authorized reseller.

Copyright 2010 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, Junos, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.