

THE CITY OF GASTONIA

True multivendor RADIUS that works



When IT officials for the city of Gastonia, North Carolina got word that its network access control (NAC) provider was exiting the market, they seized the opportunity to evaluate newer, more improved alternatives that could overcome some longstanding technical limitations.

AN UNWIELDY CHALLENGE

According to Robert Loveland, network engineer for the city of Gastonia, various city and county government organizations were authenticating against three different Active Directory servers and multiple RADIUS servers.

The new network access solution had to condense this problem by bringing centralized control on one management console for all city and county groups, including:

- Gaston County Public Safety
- Two police departments
- The sheriff's office
- The 911 center
- An ambulance service
- City administration

The goal was to improve network security, visibility, control and troubleshooting, but city IT officials also wanted to fix current problems that users were encountering while introducing new features.

"Our domains were split between a Cisco access control server (ACS) and Juniper Steel Belted RADIUS, and we needed a product that could talk to all domains," said Loveland.

"Our RADIUS servers would not talk to one of my Active Directory domains and we could never get county laptop users to authenticate to their mobile data applications, such as the county police reporting system," he added. "When we tried to work with other vendors to solve this problem, they all said it was an Active Directory issue, and would not help us."



It was imperative to allow public safety officers to authenticate and access their server resources. Anything less was unacceptable. And Loveland faced an even bigger challenge with the planned rollout of wireless email access.

In addition to authentication and access issues, the ability to manage and troubleshoot multiple domains proved to be a formidable issue for the small IT staff, which supports more than 1,000 users.

"Managing multiple directories made troubleshooting issues very time consuming," Loveland said. "Unless you knew exactly what the problem was, it was a like a shot in the dark figuring out how to resolve it."

THE MOVE TO A NEW SOLUTION

With the requirements for a new solution clearly defined, Loveland and his team came across the Aruba ClearPass Policy Manager™.

"We needed our new solution to provide the same functionality as our previous solution, but with greater visibility for troubleshooting," said Loveland. "After considering many different alternatives, we determined that Aruba was the best choice."



"In addition to extensive control and visibility features, the ability to natively support 802.1X authentication was a major factor in our selection of the ClearPass Policy Manager," he added. "Aruba supports all of our client devices – from Dell Windows laptops to guest users with iPhones and Android mobile devices."

SECURE NETWORK ACCESS

The Aruba ClearPass Policy Manager consists of a hardened network appliance, a flexible policy platform, and built-in AAA services. It is the only solution that centrally manages policies for multivendor equipment across all access methods while supporting bring-your-own-device (BYOD) initiatives and identity stores of any type.

According to Loveland, the system setup was up and running in one day. City IT officials used a phased approach to rollout the ClearPass Policy Manager appliances, which initially supported 300 users.

Clustering capabilities allowed the IT staff to add a second ClearPass Policy Manager appliance to ensure high availability and scalability to support additional users.

"We really liked the web interface, which is very intuitive and provides clear, guided steps for each part of the configuration process," Loveland said. "The previous solution was hit or miss. You had to know exactly what you wanted to do beforehand to make it work. Aruba is intuitive enough to help you get going, which makes it a lot easier to build out policies and rules that work the first time."

Aruba provides authentication via the right directory as network access is requested, and employs roles to match users to appropriate access policies. ClearPass Policy Manager then provides enforcement instructions to network switches and VPN devices, which grant network access based on appropriate user privileges.

For example, city code enforcement employees and public works building inspectors rely on wireless and VPN to access departmental servers. ClearPass Policy Manager uses the appropriate Active Directory server to determine group

membership and sends associated rules to network devices to ensure proper access to resources.

PUTTING IT ALL TOGETHER

With Active Directory authentication now working properly, the city began using 802.1X authentication for all laptops in public safety and public works vehicles.

"The ClearPass Policy Manager lets us view all attributes that were sent to a device and what is returned, making it easier to troubleshoot problem," said Loveland. "The ClearPass Policy Manager is a time saver that cut our troubleshooting efforts in half."

According to Loveland, the previous solution had a cumbersome interface with limited search fields and no easy way to pinpoint specific transaction data. Consequently, the IT staff had to parse through numerous logs to find what it needed.

"Now we can search with multiple criteria and parameters to get results right away," he said. "What previously took 30 minutes now requires only a few seconds."

To illustrate the ClearPass Policy Manager's ease of use, Loveland recalled returning to his office after an offsite training event to find that users could not authenticate wirelessly.

"I logged into the ClearPass Policy Manager, and found that our certificates expired," he said. "ClearPass identified the problem so I could fix it quickly, which I was not able to do previously."



RESULTS ARE KEY

ClearPass Policy Manager allows Gastonia to centrally manage and differentiate network access policies for city and non-city organizations like the county public safety agency. Additionally, users and their endpoint devices are now authenticated via existing and distributed Active Directory stores.

Today, the Gastonia City administration and fire and police departments access the network using role-based authentication. Other employees can only access network resources based on their roles. And computers in police department patrol cars are checked against a database during each login for added security.

“The Aruba platform is very important to us,” said Loveland. “It controls all of our remote and wireless access. It is a critical part of our operation.”

A CITY ON THE MOVE

Moving forward, Aruba’s ClearPass Policy Manager will remain the central point of identity-based access management for Gastonia. The IT group plans to roll out wired 802.1X after an infrastructure upgrade, and Aruba will play a critical role in that deployment, according to Loveland.

“Support for 802.1X over the wired network is vital because we have buildings all over the county,” he said. “Aruba helps us protect our systems better. We now have the visibility to see the people and devices that connect to our network and the ability to unify policies for wired and wireless access. We’ve never had that before.”

GASTONIA, NORTH CAROLINA

Gastonia is the largest city and county seat of Gaston County, North Carolina. It is also the third largest suburb of the Charlotte area. With a population of 71,226, Gastonia is the 13th largest city in North Carolina. The city has experienced steady growth, with a population change over the past decade of more than 10 percent, according to the U.S. Census Bureau.



www.arubanetworks.com

1344 Crossman Avenue. Sunnyvale, CA 94089
1-866-55-ARUBA | Tel. +1 408.227.4500 | Fax. +1 408.227.4550 | info@arubanetworks.com