

SOUTH CAROLINA PROBATION AGENTS HAVE SECURE FREEDOM TO MOVE WITH JUNIPER NETWORKS UNIFIED ACCESS CONTROL

Summary

Industry: Government Agency

Challenges:

- Provide secure, wireless LAN service to the HQ staff, 56 field offices, and 46 courtrooms across the state.
- Create virtual restitution centers at Department of Probation locations which other state agencies can use.

Selection Criteria: South Carolina Department of Probation selected Juniper’s Unified Access Control for the department’s enterprise-wide WLAN.

Network Solution: Juniper Networks firewall/IPsec VPN platforms, IC4500 Unified Access Control Appliance and Odyssey Access Client, M7i Multiservice Edge Router, J Series Services Routers, STRM Series Security Threat Response Managers, and IDP800 Intrusion Detection and Prevention Appliance.

Results:

- 680+ staff can better supervise offenders and serve victims with easy and secure wireless access from the HQ, field offices, and courtrooms.
- Vocational Rehabilitation, social services, and other authorized state agencies have the option to cooperatively roll out wireless hotspots at support services for offenders and victims.
- Department’s information security policies are enforced at the endpoint to protect against network attacks and loss of sensitive information.

“Our goal is to manage offenders when they come out of prison and help them become productive members of society. It is our moral and financial obligation,” says David O’Berry, director of IT Systems and Services (ITSS) at the State of South Carolina Department of Probation, Parole and Pardon Services.

The South Carolina Department of Probation is charged with managing more than 32,000 active offenders, and protecting the rights and dignity of the victims. The Department also strives to help offenders achieve positive change in their lives so that they can become productive members of society. The Department has long been a technology innovator in support of this mission, and it relies on advanced technology, such as digital imaging and GPS, to identify and monitor offenders.

Challenges

Much of a parole agent’s work of supervising offenders takes place away from the office and in the community, and the South Carolina Department of Probation was an early adopter of mobile technology. “We have more than 680 employees who can unchain from their offices and go wherever they want,” says O’Berry.

Department parole agents use convertible tablet PCs to access vital information and applications from the office, the field, and the courtroom. Agents traditionally have used a variety of wired and wireless connections, depending on whether they were at headquarters, a field office, courts, or at home, but there wasn’t a consistently easy and secure way to connect.

ITSS wanted to provide secure, enterprise-wide WLAN services so that parole agents and staff, as well as select agencies that often collaborate with the Department to rehabilitate and support offenders, could have convenient access to applications.

“With a ubiquitous wireless infrastructure, our agents won’t have to plug in anymore,” says O’Berry.

In a world of always-on connections, people have come to expect seamless wireless coverage, but delivering secure, reliable WLAN services remains a challenge for IT organizations. The need for secure mobility is even more urgent, given the sophistication of today’s information security attacks and the highly sensitive nature of the Department’s information about active offenders and victims. “It’s hard to manage an environment that’s dynamically changing, and it’s hard to manage a distributed environment. We knew we needed strong identity and access control before we could roll out wireless to our users,” says O’Berry.

Selection Criteria

As a leader in the IT security community, O'Berry has been a strong proponent of industry-standard network access control (NAC) solutions. "Most of my frustration with NAC has been because the progression path was semi-proprietary," he says. "The Trusted Network Connect (TNC) standard is important to us. We don't want to be locked in if we want to make changes."

Grounded by firsthand experience as NAC solutions and standards evolved, O'Berry was familiar with Juniper Networks® Unified Access Control when it came time to roll out enterprise WLAN services. "When I ran my options for NAC solutions, Juniper was in the top three considered. I was impressed with the standards aspects of UAC," says O'Berry.

"Our goal is to provide secure, wireless services to our parole agents and other agencies so they can have the information resources they need to help offenders get a better shot at holding jobs and staying out of prison."

David O'Berry,
Director of IT Systems and Services, State of South Carolina
Department of Probation, Parole and Pardon Services

Juniper Networks is a strong supporter of the standards from Trusted Computing Group's (TCG) TNC Work Group, which ensures interoperability with a host of network and security offerings. Support for the TNC Work Group standard also makes it simple for organizations to gain the benefits of UAC while using their existing Windows Vista and XP clients.

The Department of Probation has long relied on Juniper Networks high-performance networking and security solutions, including routers, integrated firewall/IPsec VPNs, and intrusion prevention. O'Berry adds, "My confidence in the security is what mattered in the NAC buying decision, and Juniper comes from a foundation of security."

Solution

As the South Carolina Department of Probation rolls out its enterprise-wide WLAN service, identity and access control are being secured by Juniper Networks Unified Access Control. "We have the best of both worlds," says O'Berry. "We have distributed wireless and distributed security."

The Department of Probation uses Juniper Networks IC4500 Unified Access Control Appliance, the policy management server at the heart of UAC, as its central policy manager, and Odyssey Access Client 802.1X client software on endpoint computers. Juniper Networks SBR Enterprise Series Steel-Belted Radius Servers are used for backend authentication. Juniper's firewall/IPsec VPN platforms, including the SSG500 line, serve as enforcement points in the network. Once UAC is fully

implemented, no endpoint can access the Department's network without undergoing a thorough pre-connection assessment to verify that the endpoint complies with the predefined ITSS security policies.

The IC4500 UACappliance is an ideal policy manager for mid- to large-size enterprises and remote offices. It uses information gathered by OAC, which acts as the UAC Agent, including authentication, endpoint security state, and device location data, to implement dynamic policies per user and per session that it distributes to enforcement points across the network.

Odyssey Access Client is an 802.1X access client software for wired and wireless users. OAC secures the authentication and connection of wired and wireless users, ensuring that only authorized users can connect to the network, login credentials are not compromised, and data privacy is maintained.

The Department of Probation also uses other Juniper Networks high-performance networking and security solutions. The M7i Multiservice Edge Router serves as the core router that delivers Layer 2 and Layer 3 services. The IDP800 Intrusion Detection and Prevention Appliance provides protection against a wide range of attacks, including zero-day protection against worms, trojans, spyware, keyloggers, and other malware that might penetrate from the network, or spread from already infected users.

The Department uses Juniper's firewall/IPsec VPNs, including SSG550, at the network edge. The purpose-built SSG550 line delivers high performance, security, and LAN/WAN connectivity for regional branch offices. The SSG550 line has a complete set of optimal unified threat management (UTM) security features, including stateful firewall, IPsec VPN, intrusion prevention system (IPS) via Juniper Networks IDP Series Intrusion Detection and Prevention Appliances, antivirus (including anti-spyware, anti-adware, and anti-phishing), anti-spam, and Web filtering. The Department also uses Juniper Networks J4300 Services Routers, migrating to the J4350 Services Router, to provide secure and reliable connectivity to field offices.

Results

The Department of Probation rolled out enterprise WLAN services at its headquarters and is rolling out wireless to its 56 field offices. Once complete, parole agents and staff will be able to access key applications anywhere and at any time, including offender management, parole information, and email, from their wirelessly-enabled laptops. Wireless services provided by South Carolina's Court Administration in the state's 46 courtrooms will allow parole agents to provide real-time updated information to judges and their staff. At the same time, development of a new version of the disconnected mode main business application is currently being finalized. Once it is rolled out, agents will be able to access over 60% of the information related to their job function without a connection to the Department's live network. Instead they will use any secured connection to synchronize, providing greater flexibility and operating efficiency than an always connected model.

The Department of Probation also is in the process of creating wireless hotspots at headquarters and field offices for other agencies' use, such as Vocational Rehabilitation, social services, and county and local law enforcement that work closely with the Department on offender rehabilitation.

"Going forward, it will be mission critical for us to provide secure, wireless access to these other agencies," says O'Berry. "When an offender is out of prison, it takes a lot of effort to support him. Our restitution centers have always in the past had a very good success rate to help offenders get an education, get a job and pay their bills. But, as physical locations, they do not scale as well as we would like in these tough economic times. If we can somehow close the loop and bring real-time relevant data from the various agencies into the county offices, we can provide a virtual restitution center of sorts. These people can then possibly affect the some statistically significant level of change without having to have all of the coordination services handled by one part of the organization. It creates a cooperative environment where we can potentially bring in the necessary services to help offenders succeed, thereby relieving the burden of support from the state and creating a stronger overall economic foundation."

Next Steps and Lessons Learned

The UAC solution is one important layer in the Department of Probation's strong information security defense. "A distributed security infrastructure is so important, because we can't keep up with the attacks right now, but if you overlay various capabilities to cover the challenges in an offset pattern, you stand a better chance of catching the problems in a loose configuration of nets," says O'Berry.

"The digital immune system is so focused on the heart and lungs that you can get an infection in your hand that can kill you," says O'Berry. "You can't look out of your castle, and say 'Here comes the horde.' We have to get security distributed as much as we can, as quickly as we can. That is our goal and has been for a number of years. To have a real chance in this current digital ecosystem, we have to layer security to reduce risks to an acceptable level for our organizations without debilitating our users with so much security that they can't be productive. Security is a constant balancing act."

For More Information

To find out more about Juniper Networks products and solutions, visit www.juniper.net.

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.