Meeting Government Security and Regulatory Goals through Network Access Control

A Frost & Sullivan White Paper
Prepared by Chris Rodriguez, Research Analyst
# TABLE OF CONTENTS

**INTRODUCTION** ................................................................................................................. 2

Evolving Networking Environments in Government ................................................................. 2

**CHALLENGES IN THE FEDERAL, STATE, AND LOCAL GOVERNMENT** .................. 3

Regulatory Compliance – A Global Issue................................................................................. 3

Agency Specific Security Initiatives ......................................................................................... 5

Consultant/Contractor Access and Remote Employees ......................................................... 5

Internal Threats ....................................................................................................................... 5

External Threats ...................................................................................................................... 5

Complex IT Environments ...................................................................................................... 6

**HOW NAC SOLVES THESE MANAGEMENT, SECURITY, AND REGULATORY COMPLIANCE CHALLENGES** ........................................................................... 7

Regulatory Compliance ........................................................................................................ 7

Agency Specific Initiatives ..................................................................................................... 8

Consultants/Contractors and Remote Employees ................................................................. 8

Internal Threats ..................................................................................................................... 9

External Threats ................................................................................................................... 9

Complex Environments ......................................................................................................... 9

**COMPARISON OF CUSTOMER OPTIONS FOR IMPLEMENTING NAC** ............. 10

**CALCULATING THE IMPACT OF A NAC SOLUTION ON COST (ROI)** ............ 11

Help Desk Requests ............................................................................................................. 11

The Number of Routine Network Tasks ................................................................................ 11

Reduction in Risk to the Organization ................................................................................... 11

Costs and Consequences of Inadequate Security Measures ............................................. 12

**ADDRESSING GOVERNMENT SECURITY CHALLENGES WITH CISCO NAC** . 12

A Closer Look at Cisco NAC ................................................................................................. 12

Cisco NAC Profiler ............................................................................................................... 13

Cisco Guest Server ............................................................................................................. 14

**CONCLUSION** .................................................................................................................... 14

**ABOUT FROST & SULLIVAN** ......................................................................................... 15
INTRODUCTION

The dynamic nature of enterprise networks continually opens up new attack vectors for would-be intruders. The days of network penetration as an intellectual pursuit has long passed and has been replaced by attacks perpetrated by financially-motivated criminal syndicates. Government organizations are not exempt from these attacks and in some cases are considered high-value targets. Increasingly, utilities, public records, and critical components of national telecommunications infrastructure are controlled, stored, or transmitted digitally. As a result, attackers are not strictly financially motivated, but may also be committing acts of espionage, terrorism, and warfare. With so much more at risk, government agencies must be vigilant in their efforts to protect sensitive network resources and data.

Consequently, world governments have a renewed focus on cyber security through the implementation of laws and regulations. These regulations are always a top concern for government agencies because of limited budgets that force Chief Security Officers (CSO) to carefully select which security systems to implement. Due to these budgetary constraints, organizations should invest in solutions that will not only help them to achieve compliance now, but will also enable them to achieve and demonstrate regulatory compliance in the future.

For example, in the U.S. there are already numerous laws, standards, regulations, and governing bodies concerning IT security best practices. Yet in 2008, the Bush Administration announced an initiative to review and improve the nation’s cyber security capabilities. Clearly, cyber security has become a top priority for the U.S. and the focus has continued with the Obama Administration which directed the National Security Council and the Homeland Security Council to conduct comprehensive reviews and assessments of the nation’s cyber security systems and policies.

Government agencies must implement a solution that is flexible enough to achieve compliance with existing and future regulations through policy-based control mechanisms. In June 2009, the Government Accountability Office (GAO) reported that standards bodies such as National Institute of Standards and Technology (NIST) and the Department of Homeland Security (DHS) have not sufficiently fulfilled their cyber security responsibilities. Considering the government’s rededication towards cyber security, NIST and DHS will update or replace existing security regulations soon.

Evolving Networking Environments in Government

In addition to an evolving threat and regulatory landscape, network infrastructure has evolved as well to incorporate new technology and to support 21st century business practices. These networks must now support technology such as numerous mobile devices (including PDAs and smart phones), remote access, VoIP, and other IP-enabled network equipment.

These new technologies have enabled greater flexibility in employee schedules and practices. Government employees are allowed to telecommute and may be issued a specific laptop or may access network resources via a home computer. Smartphones and PDAs provide instant network access from anywhere, at any time. In addition, employees and contractors may require access based on any combination of time, location, or role.

These new devices and work trends have introduced new threats and attack vectors into government networks. In addition, mobile devices are off the network for undefined periods of time and are not as closely regulated as desktop computers, thereby increasing the risk that these devices will be compromised by malware or an attacker.

"Protecting this infrastructure will be a national security priority. We will ensure that these networks are secure, trustworthy and resilient. We will deter, prevent, detect, and defend against attacks and recover quickly from any disruptions or damage."

Barack Obama, President of the United States of America
Government agencies rely heavily upon technology systems to transmit, store, and compute data, and even to control critical systems. As a result, attackers do not need to take control of these systems to wreak havoc; instead, they can simply deny legitimate users access to these systems. Securing these systems can be challenging since these networks include numerous third party applications, legacy systems, and may include non-traditional systems such as Supervisory Control and Data Acquisition (SCADA).

CHALLENGES IN THE FEDERAL, STATE, AND LOCAL GOVERNMENT

Regulatory Compliance – A Global Issue

Countries around the world seek to protect sensitive data from intruders through regulations. These laws require government agencies to create policies and implement security technologies that can provide a minimum level of security. The U.K. government has developed a set of security controls called the Code of Connection (CoCo). CoCo is designed to secure connections to the Government Secure Intranet (GSi) network. In the U.K., the GSi is a private network for all U.K. government agencies. Many other countries already have or are developing similar laws to address the threats posed by cyber attackers.

In the U.S. there are multiple regulatory bodies such as the Department of Homeland Security (DHS) and the National Institute of Standards and Technology (NIST) that are tasked with creating security guidelines, standards, and laws. Some of the regulations and guidelines that these entities have produced include SCAP, FIPS, FDCC, and NIST Special Publication 800-53. These mandates have different objectives and will often have both varying and overlapping requirements. This array of requirements has resulted in a complex regulatory environment that can prove difficult for government organizations to navigate.

The Federal Information Security Management Act of 2002 (FISMA) is the most important law focused on U.S. government IT security. FISMA requires government agencies to develop and implement information security systems that protect information systems owned or used by the government (including computers owned by contractors and consultants).

Already, Congress is reviewing the weaknesses of FISMA and government agencies should be expecting a more comprehensive FISMA 2.0 by 2010. Information Technology Association of America (ITAA) President and CEO, Phil Bond testified before Congress about the importance of updating regulations. According to Bond, “FISMA focused unprecedented attention on our government’s responsibility to protect the information entrusted to it by the American people and now it is time for FISMA 2.0. Federal information security can be stronger if we refine and improve the metrics as they are today; focus on results rather than compliance; embrace the public-private partnership that information security requires; and take steps that improve both the policy and the practice of IT security.”

In 2008, the U.S. government spent $68 billion on information & communication technology. Of this, government agencies spent nearly $2 billion on IT security technologies as shown in the following chart. In January 2008, President Bush introduced the Comprehensive National Cybersecurity Initiative in an attempt to bolster the nation’s ability to anticipate future threats and defend against intrusion attempts. In February 2009, President Obama directed the National Security Council and the Homeland Security Council to conduct comprehensive reviews and assessments of the nation’s cyber security systems and policies. This dedication to IT security will help protect government
operations, but will also serve to further complicate the regulatory environment and challenge organizations to stay current with security updates.

**Figure 1 - Government Cybersecurity Market Overview Spending Forecast**

![Government Cybersecurity Market Overview: Spending Forecast (U.S.), 2008-2013](image)

State and local governments are not exempt from these concerns. Government agencies at these levels must still protect sensitive data from criminals, disgruntled employees, and hackers. In 2009, state and local government agencies accounted for 10.8 percent of total U.S. cyber security spending.

**Figure 2 - Government Cybersecurity Market Overview – Market Share by Government End-User**

![Government Cybersecurity Market Overview: Market Share by Government End-User (U.S.), 2009](image)

Note: All figures are rounded; the base year is 2008. Source: Frost & Sullivan
Agency Specific Security Initiatives

The military and other high security government agencies will often have higher security requirements than what the law dictates because the continually changing threat landscape requires new policies to meet new and immediate threats. For example, in November 2008, due to an outbreak of malware, the Department of Defense (DoD) banned the use of USB removable storage devices until the devices could be scanned. Since USB drives are easy to conceal and use, this policy required additional security technology to enforce in order to secure data from a technology not accounted for in current laws. As a result of this policy, agencies sought a solution that would enable them to detect and scan USB drives, and close other security gaps not covered by existing laws.

Consultant/Contractor Access and Remote Employees

Even high security clearance agencies must provide access for consultants and contractors. This requires time and effort from system administrators to create temporary accounts with restricted access. Since government agencies work with tight budgets and limited IT staff, it becomes critically important to implement solutions that allow IT staff to be more productive, without increasing headcount.

According to FBI statistics, remote employees represent a fast growing segment of network users. Certain government agencies such as Defense Information Systems Agency (DISA), now allow employees to telecommute 2 to 3 days per week. Even though remote access is the exception rather than the rule for high security agencies, the fact remains that there are still users that must be able to access network resources remotely.

Internal Threats

Internal threats have been a priority for network administrators since 2005. According to a FBI computer crime survey, 44 percent of the 2,000 organizations surveyed reported insider attacks in 2005\(^1\). This implies that some employees may deliberately leak data or sabotage systems. However, employees may also unknowingly pose a threat. For this reason, security policies must be developed that ensure that employees will only access the information and network resources they need to in order to complete their duties. As seen in the 2006 Veterans Administration data breach, employees may disregard security policies in order to complete their assigned tasks, as a result, technology must be implemented to automatically enforce these policies.

External Threats

Cyber crime is one of the most lucrative activities available to criminals. In 2008, computer-based crimes cost the United States $265 million according to the FBI. By comparison, only $61.6 million was stolen in bank-related crime in 2008. What is clear is that hacking activities are viewed by criminals as a high return, low risk activity that is reflected in the growth rate of computer crimes which jumped from $68.1 million in 2004 to $183.1 million in 2005. By 2008, damages from computer crime reached $265 million in 2008\(^2\). While these losses are staggering, the intangible losses from public disclosure of a data breach are difficult to quantify, and can cause permanent damage to an organization’s reputation.


\(^{2}\) http://www.networkworld.com/community/node/40375

“The number of cyber attacks continues to increase as does the sophistication of the tools used for attacks. At the same time, the required knowledge of attackers is decreasing, which makes targeting and responding to attacks challenging.”

Brad Curran, Senior Industry Analyst, Aerospace and Defense, Frost & Sullivan
Furthermore, government networks face specialized threats from terrorists or adversarial countries and are high value targets for sabotage. The FBI is currently watching online activity from twelve different countries that are suspected of cyber warfare or espionage activities\(^3\). Recent distributed denial-of-service attacks against U.S. government websites are believed to have originated in China or North Korea.

The United States is not the only country to be attacked by hackers. In 2008, Georgia, Lithuania, Latvia, and Ukraine all reported cyber attacks against government websites and communications infrastructure. Several pieces of Lithuania’s key Internet infrastructure, including government sites, banking, and telecommunications services were disabled. The 2007 attacks against Estonia were particularly debilitating, and brought one of the most technologically advanced countries in Eastern Europe to its knees. Estonian computer security experts and officials traced these attacks to Russia\(^4\).

**Complex IT Environments**

Although government agencies have much more control over endpoints than their private sector counterparts, the natural advancement of technology has led to new types of IP-enabled devices including VoIP phones, printers, and other devices. Legacy systems and non-traditional systems such as Supervisory Control and Data Acquisition (SCADA) devices further complicate these network topologies. These devices, along with traditional enterprise applications and systems are vulnerable to numerous attacks, but patching these systems can be a time consuming process for network administrators. Figure 3 shows the number of IT vulnerabilities reported from 1995 to 2008.

**Figure 3 - Vulnerabilities Reported by Year**

![Vulnerabilities Reported by Year](Source: Frost & Sullivan)

In addition, these networks are heterogeneous environments that don’t always rely on Microsoft technology. The wide range of applications and operating system environments

\(^3\) [http://www.newscientist.com/article/dn14961-computer-crime-a-growing-threat-warns-fbi-.html]

\(^4\) [http://www.guardian.co.uk/world/2007/may/17/topstories3.russia]
makes the process of auditing and securing these systems extremely challenging in a large government network environment.

Large enterprise networks tend to be deployed slowly and are typically static environments. However, for military organizations, mobility is crucial as the military must be ready to quickly deploy to any theater of operations at a moments notice. As a result, military organizations must be able to quickly set up networks, as well as detect, and configure endpoints rapidly.

HOW NAC SOLVES THESE MANAGEMENT, SECURITY, AND REGULATORY COMPLIANCE CHALLENGES

Regulatory Compliance

The U.S. Government Accountability Office (GAO) released a report in June 2009 that states that the DHS has not met its cyber security responsibilities. The Homeland Security Act of 2002 assigned the DHS the task of protecting the nation’s computer-based critical infrastructures. This includes virtual assets and physical systems such as communications, defense systems, mass transit systems, power systems, nuclear systems, and others. The National Institute of Standards (NIST) was also assigned important responsibilities under the Federal Information Security Act of 2002 (FISMA). NIST was assigned to develop standards, definitions, and guidelines to aid with the categorization of information and information systems. Most importantly, NIST was tasked with developing minimum security requirements for systems across every type of category. As a result, government agencies at all levels can expect updated guidelines, mandatory requirements, and assessment policies in the near future.

While there isn’t a silver bullet solution that will make a network entirely compliant with these regulations, certain technologies fit the role better than others such as Network Access Control (NAC). NAC is a technology that enables customers to meet many of the security requirements that regulations mandate and is particularly strong in the areas of authentication, access control, and policy enforcement.

NAC can enforce many different levels of authentication, such as by user, location, device, time and role – before granting network access. In addition, NAC solutions ensure that only authorized users have access to the network resources they need. Furthermore, enforcement options such as inline, DHCP management, 802.1X, and VLAN, ensure that only healthy endpoints and credentialed users are allowed onto the network. NAC also provides the ability to quarantine and correct issues via automatic remediation, alerts, or notifications. These features satisfy many of the requirements that federal, state, and local governments require for their networks. The following chart shows the full NAC cycle of authentication, assessment, enforcement, remediation, and post-connect monitoring. Figure 4 illustrates the key NAC Functions as defined by Frost & Sullivan.
Although NAC solutions have useful reporting capabilities, integration with third-party log management and reporting software further strengthens the value that NAC offers to government networks. In fact, NAC can provide a large amount of data such as logging requests for access to specific resources, registration logs, endpoint scan results, policy violations, and connection logs with device type, location, time, and duration. The use of NAC can not only help to meet current regulatory requirements, but can also help organizations to better meet the demands of new regulations or updates.

Agency Specific Initiatives

Laws cannot be passed quickly enough to meet the rapidly evolving threat landscape. As a result, agencies create policies that pertain to the imminent threats that they face. One example is the proliferation of USB devices. USB removable storage can be used to spread malware such as the worm outbreak that infected machines in the DoD. USB devices can also facilitate data leakage. Small spy cameras are sold relatively cheaply, or can be easily made with the aid of online guides. These devices make it easier for rogue users to compromise or sabotage sensitive data and systems.

NAC can be used to detect certain configurations, connecting devices, and even the use of certain technologies, including USB devices and other removable media. Network access control is a solution that is capable of scanning endpoints regardless of the device type. A NAC solution is able to detect the connection of a USB device and can scan the device before deciding to grant it access, initiate a remediation process, or deny the device access to the network.

Consultants/Contractors and Remote Employees

Consultant and contractor access has been a key reason for many organizations to invest in NAC. In recognition of the high demand for consultant /contractor services, NAC vendors offer solutions designed to make temporary account management a more efficient and automated process. These solutions allow organizations to offer specialized access for wireless and wired networks in a secure and easy manner.

While the exact features vary by vendor, NAC solutions typically enable IT departments to simplify or automate guest user account creation and account provisioning. More importantly, NAC can do this in a controlled manner by allowing the organization to set the account expiration time and by logging contractors’ network access activities and resource access. Using NAC, customers can realize tangible savings in terms of time and budget, while securely enabling collaboration and productivity with partners and visitors.
As more employees are allowed to work remotely, the need to provide secure access for these users has been recognized by NAC vendors. NAC solutions are capable of detecting and controlling access of any device regardless of whether it connects over the LAN, wirelessly, or over a Virtual Private Network (VPN). As a result, NAC solutions extend protection and control abilities to remote offices and remote users.

Internal Threats
Defending information and network resources from the insider threat remains a top priority for network administrators. There are other solutions besides NAC that may seemingly be able to help with this goal. For example, Data Leakage Prevention (DLP) is a relatively new technology that is designed to help prevent specific information from exiting the network in any manner. However, DLP is a relatively new technology that is still considered to be immature and difficult to implement with full functionality. Further, because attackers only seek to sabotage information or corrupt the integrity of data assets in a government organization, simply preventing the leak of certain information provides inadequate security protection.

The best method of protecting against insider threats is to only grant employees access to the resources that they require to complete their assigned tasks. In addition, insiders may unknowingly represent a threat by introducing malware through an infected mobile device or laptop. As a result, it’s critical that government agencies implement NAC to assess the health of endpoints and validate users’ identities in order to provide the highest level of security possible by mitigating the risk posed by insider threats.

External Threats
The external threats that government agencies face on a daily basis include hackers, botnets, criminals, terrorists, malware, and unfriendly nations. No other organization has more at risk, which is why government organizations have the highest security demands.

As it was originally envisioned, NAC is an effective tool to stop the spread of malware and intrusions into enterprise networks. NAC’s ability to detect, scan, and control all devices and users attempting to connect to the network enables government organizations to effectively mitigate the risk posed by external threats.

Complex Environments
Currently, typical duties such as network additions or changes can be very time consuming and resource intensive. For example, network administrators must manually hard-code ports for specific MAC addresses when setting up VLANs and assigning permissions. These practices are quickly becoming outdated due to an increasingly dynamic and mobile workforce. In addition, these practices are susceptible to MAC address spoofing and similar attacks.

NAC solutions are able to detect connecting devices and determine the correct levels of access. By doing so, customers can accurately and automatically build inventories of network systems. This frees up network staff’s time and budgets for more productive projects. Further, NAC allows the customer to monitor every device’s behavior and notify administrators in case of a change in the endpoint’s behavior. This reduces the threat posed by MAC address spoofing and other forms of network penetration. This also provides levels of protection for legacy or non-traditional endpoints that other security solutions (such as anti-virus) cannot. NAC is an important solution for customers with complexity and mobility issues, because it can help users to quickly set-up and protect their networks.
### Table 1 - Comparison of NAC Approaches

<table>
<thead>
<tr>
<th>NAC Approach</th>
<th>Overview</th>
<th>Strengths</th>
<th>Weaknesses</th>
</tr>
</thead>
</table>
| **Infrastructure-based NAC** | • Composed of a policy server, endpoint client, and may use 802.1X-enabled switches or network protocols such as SNMP or DHCP for enforcement. Integrates with authentication and remediation servers.  
• Typically compliments the vendor’s core competencies, e.g., building NAC functionality into firewalls that the vendor is known for.  
• Integration with other network technologies such as IPS, VPNs, and routers gives NAC a higher value proposition. | • 802.1X-enabled switches are considered to provide the strongest and most granular form of authentication and enforcement.  
• NAC vendors that utilize switches in their NAC solution have extensive experience with the design, manufacturing, and selling of enterprise-grade switching equipment. | • Certain devices do not have supplicant support yet. |
| **Host-based NAC**      | • Primary method for NAC offered by developers of endpoint security software.  
• Requires an installed client on each endpoint. | • Installed client is able to relay more information about the endpoint to the NAC policy decision server, enabling deeper assessments.  
• Leading vendors have managed to integrate their NAC agents with their endpoint security suite agent to minimize the impact on end-users. | |
| **Appliance-based NAC** | • A full NAC system housed in an appliance that is easily deployed and can utilize existing network infrastructure.  
• Designed to sit either out-of-band or inline. | • Considered to be cost effective, easier to implement, and lower risk than an infrastructure or host-based solution.  
• Out-of-band appliances offer strong scalability, flexible enforcement options, and have been embraced by customers. | • NAC vendors that only offer inline appliances have not fared very well. This is because inline appliances represent a performance bottle-neck as well as a single point-of-failure. |
CALCULATING THE IMPACT OF A NAC SOLUTION ON COST (ROI)

As a result of implementing a NAC solution, a variety of gains may be seen for network and security administrators. Three key areas where significant savings in cost and workload are recognized are:

- Help desk requests
- The number of routine network tasks, and
- Reduction in risk to the organization.

Help Desk Requests

Help desks get a wide variety of requests on a daily basis ranging from simple password resets to more complex hardware and software issues. When malware problems arise, the volume of help desk requests increase exponentially, burying help desk personnel under the load and causing the organization significant frustration and embarrassment.

A NAC solution can provide relief on a number of fronts. First, by keeping machines patched and inline with security policy, the chances of an outbreak are reduced significantly. Second, should an outbreak occur, remediation can be triggered automatically, saving hours of manual application of patches and updates for the IT staff.

The Number of Routine Network Tasks

Administrators spend a large amount of time performing routine network duties. Whether it’s conducting inventories, updating machines, setting endpoint policies, or patching vulnerabilities these routine tasks all take time away from other, more important initiatives. All of these tasks cost organizations time and money that could be spent on higher value projects that require the expertise of information security professionals. Simple network additions, moves, or changes involve manually hard-coding ports for specific MAC addresses, VLANs, and ACLs. This time consuming process is compounded by an increasingly dynamic and mobile workforce.

As a result, even routine network tasks are very resource intensive. NAC can eliminate the majority of this work by enforcing security policies and by automating inventory, updates, and remediation. Government agencies can utilize NAC to show significant and tangible savings for IT budgets. The intangible benefits of NAC implementation are reflected in the availability of security personnel to pursue other business critical projects.

Reduction in Risk to the Organization

NAC reduces an organization’s risk profile by forcing updates and remediation before a machine is able to connect to the network and by continuing to check the health of a machine after it is allowed to connect. The importance of forcing remediation for a problem before connecting to the network was highlighted by a large U.S. federal agency that could have been infected by a Trojan designed to log and transmit personally identifiable data.

The Trojan did not affect the operation of the infected laptop, so it went unnoticed by the employee until he returned from a business trip. When he returned and attempted to access the network, his laptop was automatically quarantined, forced to install security updates, and a full-scan was implemented. Once the updates were run the Trojan was discovered and eliminated, averting what could have been an embarrassing and costly incident.
Costs and Consequences of Inadequate Security Measures

Unfortunately, there are many examples of government agencies that have not been well prepared. In 2006, hackers illegally accessed a U.S. Department of Agriculture (USDA) database containing the names, Social Security numbers, and photos of agency employees. Consequently, the USDA had to provide one free year of credit monitoring for the approximately 26,000 employees that were at risk for identity theft.

In 2008, the State Department was breached and several hundred passport applications containing personal information, including Social Security numbers, were illegally accessed and used to open fraudulent credit card accounts.

While these breaches resulted in employee data leakage, governments have much more sensitive data targets. Robert Phillip Hanssen proved that it only takes one rogue user to undermine the security of an entire country. In what is regarded as the worst intelligence breach in U.S. history, Hanssen gained access to nuclear and defense secrets and passed thousands of pages of top secret intelligence to the Soviet Union for most of his 27 year career at the FBI.

Even in cases where no security breach actually occurred, the losses can be very substantial. In 2006, a laptop containing Social Security numbers, names and addresses for more than 26 million veterans was stolen from the Department of Veterans Affairs (VA). The laptop was recovered shortly after and the FBI could not determine conclusively that the data was not accessed. As a result, most veterans invested in credit protection and fraud prevention services. A class action lawsuit was filed against the VA and the agency agreed to a $20 million settlement to reimburse veterans\(^5\). In addition, the leak had pernicious effects on the VA’s reputation and credibility.

The risk varies from organization to organization. Whether it’s a few hundred employee files or defense secrets, government agencies must evaluate the value of their data and systems and devote the necessary resources towards protecting these assets. The millions of dollars of damages caused by security breaches could have been prevented for only a fraction of the cost.

ADDRESSING GOVERNMENT SECURITY CHALLENGES WITH CISCO NAC

Cisco originally offered an architecture-based NAC solution, and then supplemented its portfolio with an appliance-based solution. Today however, Cisco NAC is a single solution that draws on the advantages of both deployment types and allows organizations to bake NAC functionality into their network infrastructure through NAC-ready switches. On the other hand, Cisco NAC can provide full NAC functionality through an easy to deploy network device. Cisco NAC is composed of a Cisco NAC Server, Cisco NAC Agent, and the Cisco NAC Manager.

A Closer Look at Cisco NAC

The Cisco NAC Server may be deployed inline or out-of-band to meet the business needs of any organization. Out-of-band deployment of the Cisco NAC Server provides a non-intrusive, scalable NAC solution. Inline deployment is recommended for VPN traffic and wireless access points. This server is available on three different hardware platforms, in five different sizes, from devices that support 100 or 500 concurrent users, to devices

that support as many as 1,500 or 5,000 concurrent end-users. Multiple Cisco NAC Servers may be deployed to support larger networking environments.

The Cisco NAC Agent is an optional, read-only agent that can be installed on endpoints and has a lightweight 10 MB footprint. Customers have the option to implement network-based scans or custom-built scans, but the installed agent enables customers to offer automated remediation for noncompliant endpoints. This agent is distributed at no charge to Cisco NAC Appliance customers.

Cisco NAC Manager provides a centralized, web-based management console for network administrators. With Cisco NAC Manager, customers can create rules and policies, and establish roles. Cisco NAC Manager is available in three sizes: Cisco NAC Lite Manager, Standard Manager, and Super Manager, capable of managing 3, 20, and 40 Cisco NAC Servers, respectively.

A key benefit of Cisco NAC is that it eases the long standing friction between business-users and network personnel. Cisco NAC integrates with most forms of authentication, enabling single sign-on for clients, thereby simplifying network and application access for business-users. For network administrators, Cisco NAC supports automatic security policy updates and includes predefined policies to ease rapid implementation. In addition, the Cisco NAC Server is inline with the network traffic only during the authentication and assessment process. Unless the endpoint requires remediation services, its network traffic will pass through the switch as it normally would. The optional, ultra-light endpoint agent makes the entire process as seamless as possible for end-users.

Most importantly, Cisco NAC provides complete, end-to-end network protection. Cisco NAC is able to scan and control every single device including nonresponsive devices such as printers, VoIP phones, gaming consoles, and others. Regardless of whether it is a managed or unmanaged device, employee-owned or guest machine, the Cisco NAC Appliance can determine the endpoint’s health and policy compliance. Noncompliant machines can immediately be quarantined to protect other endpoints from infection by malware. These assessment and prevention capabilities enable customers to achieve compliance with government and internal security regulations and standards, while reporting capabilities allow the organization to prove their compliance.

Furthermore, because Cisco NAC enforcement is based on customizable policies, government organizations can quickly adapt to new regulations and guidelines.

While additional modules are not required for Cisco NAC to provide full functionality, Cisco does offer additional solutions to help address specific challenges that enterprise networks face.

Cisco NAC Profiler

Cisco NAC Profiler works in conjunction with Cisco NAC to automate the process of detecting, categorizing, scanning, and monitoring all devices that connect to the network. Cisco NAC offers these abilities natively; however, Cisco NAC Profiler improves on these processes by generating automatic inventories of all endpoints complete with the MAC address, description, and access level.

The Cisco NAC Profiler can detect changes in the endpoint’s behavior on the network, which would indicate a change of device type or the possibility of an attack. Due to these

---

abilities, Cisco NAC Profiler reduces deployment time, increases the ease of network management, and provides an additional layer of security. Cisco NAC Profiler will prove invaluable for organizations requiring quick and easy network deployments, with complex networking environments, or with high security requirements.

Cisco Guest Server

Cisco Guest Server integrates with the Cisco NAC and wireless LAN Controllers to offer temporary or limited user services for government networks. Cisco Guest Server provides numerous methods for customers to assign user account details to contractors and consultants. In one method, the network administrator can assign the task of creating temporary accounts to any employee at his discretion. The internal user is able to easily create and manage these accounts for the consultant or contractor. Details of the guest's network activities are recorded for auditing purposes.

Cisco Guest Server also offers automatic provisioning for temporary accounts, with preset account expiration times. As a result, Cisco Guest Server not only adds another layer of security for government agencies, but also fosters greater collaboration with partners.

CONCLUSION

Government agencies must protect highly sensitive data and critical network infrastructure from a constant barrage of security threats. A single security breach can cost millions of dollars in damages and lawsuits, as well as have an intangible but very costly impact to the agency's reputation. Furthermore, government organizations are challenged to reach compliance with an ever changing range of regulatory requirements. Complex and evolving network environments further increase the strain on the network staff and their security budget.

Cisco NAC can help government agencies to meet many of these security goals, regulatory demands, and network management challenges. Cisco NAC enables state, local, and federal government agencies to improve security by forcing authentication based on user type, location, time, role, and other attributes. Cisco NAC then provides access to only authorized network resources. Cisco NAC guards networks from external and internal threats by enforcing security policies and preventing the spread of malware on the network. With Cisco NAC, government agencies will be able to meet regulatory requirements, report, and record data for compliance audits. Most importantly, because Cisco NAC is a policy-based control mechanism, these policies can easily be updated to help an organization to adapt to changes in government regulations and emerging security threats.
ABOUT FROST & SULLIVAN

Based in Mountain View, California, Frost & Sullivan is a global leader in strategic growth consulting. This white paper is part of Frost & Sullivan’s ongoing strategic research into the Information Technology industries. Frost & Sullivan regularly publishes strategic analyses of the major markets for products that encompass storage, management, and security of data. Frost & Sullivan also provides custom growth consulting to a variety of national and international companies.

The information presented in this publication is based on research and interviews conducted solely by Frost & Sullivan. Frost & Sullivan takes no responsibility for any incorrect information supplied to us by manufacturers or end users. All copyright and other proprietary notices must be retained. No license to publish, communicate, modify, commercialize or alter this document is granted.

For information regarding permission, write:

Frost & Sullivan
331 E. Evelyn Ave. Suite 100
Mountain View, CA 94041