AN ADAPTIVE APPROACH TO NETWORK SECURITY

Evolve your network security strategy to meet new threats and simplify IT security operations

Frank Andrus
CTO, Bradford Networks

- Executive Summary................................................................. 1
- Network Security Today......................................................... 1
- Evolving Network Security Requirements............................ 2
- The Evolution of Network Security and NAC’s Role............... 3
- An Adaptive Approach to Network Security......................... 4
  › Platform.................................................................................. 5
  › Functional Elements............................................................. 5
  › Architectural Elements....................................................... 6
  › Use Cases.............................................................................. 7
- Conclusion............................................................................... 8
- About Bradford Networks..................................................... 8
An Adaptive Approach to Network Security

EXECUTIVE SUMMARY

Network threats, and effective security solutions to cope with them, are evolving rapidly. In addition, new business imperatives, including the need for more internal and external collaboration, the growth of the Bring Your Own Device (BYOD) phenomenon and expanded regulatory requirements, are forcing networks to be more accessible, placing even greater demands on network security and on IT operations.

Today, network security solutions are often fragmented, with a number of best-of-breed technologies deployed independently in silos to address different problems. This silo approach to security is insufficient to deal with a changing landscape of increasingly mobile users, a highly heterogeneous device mix, and dynamic threats posed by more sophisticated attackers. A tightly integrated and adaptable approach to security is needed.

Network Access Control (NAC) solutions represent an important first step for integrated security solutions by joining the capabilities of endpoint security software with security features of the network infrastructure to manage network access. To meet emerging network security requirements, today's solutions must evolve into an adaptive approach to network security. This approach is based on a security policy engine that breaks the silos between previously distinct and non-integrated security solutions. It leverages all facets of existing network security by integrating the network infrastructure, desktop security, and security infrastructure solutions, without requiring significant redesign of the network or extensive replacement of existing network components.

The benefits of an adaptive network security approach include integration of multiple security technologies, extensive visibility into the network, correlation and sharing of information, as well as the ability to adapt dynamically to network changes and automate day-to-day IT tasks. It also facilitates compliance with industry and government regulations pertaining to information security. Ultimately, an approach to network security that is flexible and able to adapt to an existing environment redefines the nature of today's networks, making them both more secure and more accessible. It enables existing network and security investments to be utilized more effectively, while reducing the operational burden placed on IT organizations by an ever-evolving security landscape. The time for a flexible approach to securing networks is now, and Bradford Networks is the only vendor that can deliver it today.

NETWORK SECURITY TODAY

As networks have grown, changed, and evolved over the years, so too have the threats to network security. With each new type of threat came increased awareness of the need for new security solutions. As a result, today’s network security landscape is scattered with isolated solutions that operate within their own silos. These static solutions each resolve a portion of an organization’s overall security objective to protect corporate assets from the outside world or the wide area network (WAN).

FIGURE 1: TODAY’S FRAGMENTED APPROACH TO NETWORK SECURITY

Network security today is comprised of disparate “silos” of security solutions functioning independently.

1 Source: “Magic Quadrant for Network Access Control,” Gartner, December 8, 2011
An Adaptive Approach to Network Security

Network Infrastructure

Network infrastructure devices such as switches, routers, wireless controllers, firewalls and VPN concentrators all have inherent security features. Virtual LANs (VLANs) are used to physically segment the network and restrict access. Firewalls and access control lists (ACLs) are used to deny access to unauthorized users attempting to access restricted resources. These and other security features in use today are typically implemented manually by IT staff and have to be updated manually when changes are needed.

Desktop Security Solutions

Desktop security solutions help to safeguard investments in desktop and laptop systems by detecting and blocking malware, hackers and other potential vulnerabilities. Anti-virus, anti-spyware, application control, and data encryption solutions are invaluable in terms of keeping systems and data secure, but these technologies operate independently from other security systems in the network environment.

Security Infrastructure Systems

Security systems including Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS) and other Deep Packet Inspection (DPI) systems are typically in-line devices placed close to the external firewall to monitor network traffic for suspicious activity or signs of attack. While useful, these devices do not incorporate information from other areas of the network environment to determine the “full picture.” For example, an IPS may conclude that a suspicious pattern of network traffic is an attack without having knowledge of the identity of the user or device associated with the traffic. In order to avoid potential “false positives”, knowledgeable IT staff must often intervene to determine whether the network activity is in fact a threat.

Access Control

Access control is often a manual process for which IT staff has responsibility to provision network access for authorized users and devices. Acceptable Use Policies are written to outline terms and conditions for use of network resources – however, IT departments often lack the staff and/or the technology required to effectively enforce these policies.

Many of today’s security solutions are deployed as disparate systems with limited or no integration to other network or security systems. Without integration, these solutions are not able to apply security measures in context with factors such as who is on the network, what is on the network, or when or where. In addition, these solutions often require a great deal of manual intervention to be implemented and maintained, further exacerbating this fragmented approach to securing heterogeneous networks.

Evolving Network Security Requirements

With the explosion of new endpoint device technology, and the ever increasing mobile user population and 'Bring Your Own Device' (BYOD) initiatives, the need to understand who and what is connecting to a corporate network has become critical.

IT departments struggle with how to ensure that mission-critical network resources are both operational and secure, while allowing network access for endpoint devices, mobile devices, biomedical devices, security cameras, etc. IT departments are also responsible for ensuring that mobile users, employees, partners, guests and contractors do not misuse network resources, wrongly distribute intellectual assets or otherwise violate usage policies. In addition, IT is ultimately responsible for making sure that network users can accomplish valid tasks with minimal interruptions. This requires IT to be able to dynamically identify, manage and secure a wider variety of devices and users on the network.

At one time, security threats came from outside the corporate network. Today's security threats come from the WAN, outside the firewall, inside the firewall, in the DMZ, and inside the corporate network. In the past, threats were targeted to bring the network down. Security threats now come from hackers wanting to keep the network up and running as they attempt to steal valuable information without detection. Whereas security infrastructure used to be deployed along the perimeter of the network, now it is required throughout the network. IT must therefore be able to more effectively utilize security features inherent within the network infrastructure itself.

Guest access has also become a crucial enabler of business on today's network. At the same time, the distinction between guests and employees has become more difficult to define. Guests might include customers or clients, business partners, outside vendors, contractors, and others -- each with unique access requirements. The growing need for guest access has put yet another strain on an already over-tasked IT department, driving the need for IT to be able to automate and/or delegate the process of provisioning guest access.

Organizational boundaries between business units are becoming less defined. Which department owns which resources? What employee belongs to what department? As organizational silos start to fade, the static silos of security policies become less effective and harder to maintain. Ideally, a security solution that will adapt along with the organization's changing needs is required.

This combination of factors means that today’s approach to security must evolve.
THE EVOLUTION OF NETWORK SECURITY AND NAC’S ROLE

In the face of rapidly changing, and more demanding, business and technical requirements, IT needs an adaptive security solution that integrates with existing technologies, shares information and dynamically adjusts as the security environment changes. In addition, automation of IT tasks along with dynamic policy monitoring and enforcement would significantly ease the demands on the IT department.

Network Access Control (NAC) represents an important first step for integrated security solutions. NAC allows authorized users to gain access to the network based on a number of administrator-controlled factors, and it can dynamically provision the network and the access provided to the user. Most NAC solutions are based on validating user identity and the security posture of the devices they use before allowing access to the network. Areas typically controlled by NAC solutions include:

**User Identity**

This entails validation of user identity through authentication. Advanced NAC solutions can also associate identity-based (or role-based) policies to each user, associate a user to specific network devices, and track the location of a user on the network.

**Endpoint Compliance**

Endpoint compliance involves validation of the security posture of a user’s device; most often with respect to the operating system (OS) version, security patches, and the presence of anti-virus and/or anti-spyware software applications on the device. Advanced NAC solutions can perform more comprehensive posture assessment of applications, processes, and/or files present on endpoint devices.

**Remediation**

Remediation refers to the ability to allow the user to fix compliance problems without impacting the IT staff. Advanced NAC solutions accomplish this with auto-remediation tools or by walking users through a set of web pages that detail the compliance issues and allow access to appropriate web sites for resolution.

**Policy Enforcement**

Policy enforcement may entail simple “on/off” network access based on whether a user and their device are determined to be compliant. Advanced NAC solutions can enforce more granular controls based on user identity, endpoint compliance, and/or other information.

---

**FIGURE 2: NETWORK ACCESS CONTROL (NAC)**

Network Access Control (NAC) solutions address part of the challenge, but still leave several security "silos"
Today’s NAC solutions are generally standalone systems – often in-line devices – that have limited integration with existing network security solutions. NAC adoption has been relatively slow because the traditional definition of NAC focuses mainly on control, acting essentially as a big “ON/OFF” switch for network access. Critical business users may not be allowed on the network when endpoint policies fail, which then can bring productivity to a halt. IT personnel often have to manually “white list” printers, IP Phones, HVAC equipment, and various other devices on the network, further complicating how mixed-device networks are secured (see Figure 2).

THE EMERGENCE OF ADAPTIVE NETWORK SECURITY

To meet evolving network security requirements, traditional NAC solutions must evolve to become more flexible and adaptive. An adaptive network security platform is enabled by a robust security policy engine that breaks the silos isolating today’s disparate, non-integrated security solutions. It leverages all facets of existing network security by integrating the network infrastructure, desktop security, and security infrastructure solutions.

An adaptive security approach integrates all security solutions, from the desktop (endpoint) to network and security infrastructure. This integration allows these disparate systems to correlate and share information. A central policy engine allows administrators to create and deploy highly-effective security policies that leverage all possible enforcement points, while allowing policies to adapt dynamically based on network changes.

FIGURE 3: AN ADAPTIVE NETWORK SECURITY APPROACH
Leveraging the entire network environment – from endpoint to network infrastructure to security infrastructure – to deliver complete visibility and comprehensive security
BRADFORD NETWORK SENTRY™: AN ADAPTIVE SECURITY PLATFORM

Bradford’s Network Sentry(TM) platform is built upon an adaptive network security architecture, which enables Network Sentry to be deployed in any network environment, and to leverage the many other elements in a typical network to deliver a comprehensive security solution.

While Figure 4 depicts Bradford’s Network Sentry platform at the center of the network environment, it is not necessary that it be physically deployed “in the middle” or “inline” between other elements. Network Sentry can be deployed anywhere in the network while still providing network-wide visibility, management, and control functionality.

FUNCTIONAL ELEMENTS

As shown in Figure 4, Bradford’s Network Sentry delivers integration, correlation, and automation, as well as visibility and control, across the entire network. Each of these functions is discussed briefly below.

Integration

Many security features exist in today’s networks that are rarely if ever utilized. Security features built into existing network and security infrastructure should be highly leveraged, as each provides a valuable contribution to a comprehensive system of security. For example, multiple points of policy enforcement can be enabled by leveraging security features inherent in desktop security software, network infrastructure devices (e.g. switches and wireless controllers), and traditional security infrastructure devices (e.g. firewalls and IPS). This not only allows for more effective security, but also allows both existing and new technologies to be more effectively utilized.
Correlation
A wealth of information is gathered as a result of this integration, and correlation allows the information to be put into a proper security context. For example, an IPS typically assesses security threats based on traffic patterns between source and destination IP addresses, but provides no knowledge of what endpoint device is represented by a particular IP address. Is it a printer? A server? The CEO’s laptop? This is important information, and it exists on other systems within the network. Network Sentry enables the correlation of information from various sources so that the “big picture” can be seen.

Automation
One of the greatest challenges facing today’s IT organization is that of trying to keep up with evolving network security challenges with very limited staff resources. Network Sentry enables automation of various configuration and management tasks performed by IT staff today, such as provisioning network access for different users and devices. This not only frees IT staff to be able to focus on more important things, but also enhances security and efficiency with the ability to dynamically adapt to network threats and changes.

Visibility and Control
By integrating with and leveraging the entire network environment, Network Sentry is able to deliver end-to-end visibility of all users and devices on the network in real-time, as well as monitor and log all network activity over time for historical views and detailed reporting capability. Utilizing this information, Network Sentry then enables network-wide management and control for enforcement of security policies throughout the network – from switch, to wireless access point, to router, to firewall, to VPN controller, etc. – to secure and protect the network and the organization’s critical information.

The combination of these powerful functions enables Bradford’s Network Sentry to dynamically manage security policy across the entire network.

ARCHITECTURAL ELEMENTS
Architecturally, Network Sentry consists of a number of core engines that drive its key functions, including a Device Engine, State Engine, Policy Engine, and Enforcement Engine. A logical map of the network is created to represent every network and security infrastructure device, as well as every user and endpoint device that connects to the network. The network map and user/device map provide the who, what, where and when information that is the basis for network-wide visibility, and the starting point for managing network security policies.

Device Engine
The Device Engine builds a network map representing every network infrastructure device (switch, router, wireless controller, etc.) and every security infrastructure device (IDS, IPS, firewall, etc.) in the network, along with vendor-specific security features and enforcement options for each device. The Device Engine provides the intelligence about the existing infrastructure and its capabilities that can be leveraged for security policy enforcement.

State Engine
Information on the current status, or state, of users and endpoint devices on the network allows Network Sentry to make real-time policy decisions and to perform dynamic policy enforcement based on current conditions. The State Engine develops a model representing every user and endpoint device in the network. It associates user information including identity, role, and state (i.e., is this a known user? an authorized user? a user who has been flagged as being “at risk” or non-compliant with security policy?). It also associates device information including device type, role, and state (i.e., is this a known device or a rogue? is it currently online or offline? has it been flagged as being “at risk” or non-compliant with security policy?). State data is maintained in the central database of Network Sentry to be leveraged by the Policy Engine and Enforcement Engine.

Policy Engine
The Policy Engine enables the creation of security policies tailored to individual users and endpoint devices based upon a rich set of information residing in the central database of Network Sentry. The Policy Engine also functions as a centralized policy decision point responsible for making real-time policy decisions.

Enforcement Engine
Once a policy decision has been made, an automated response action is typically executed at one or more points of enforcement in the network. The Enforcement Engine leverages information from the Device Engine, State Engine, and Policy Engine to initiate policy enforcement actions. For example, access policy might be enforced by dynamically changing the state of a switch port from enabled to disabled, or by setting Access Control Lists (ACLs) on a router or firewall, to isolate an endpoint device that is determined to be in an “at risk” state.

The true strength of Network Sentry is derived from a combination of these powerful engines functioning together. Next, we explore a few example use cases to show how Network Sentry addresses real business challenges.
USE CASES

Bradford's Network Sentry has been deployed in a number of real-world environments to address specific security requirements. Below are examples of some of those use case scenarios.

Example #1 - Dynamic Enforcement of Endpoint Security Policy

| PROBLEM | Due to the sensitive nature of its data, a large bank requires all employees to have data encryption enabled on their computers when transferring information across the network. However, the bank does not have a way to proactively enforce this policy. |
| SOLUTION | Network Sentry enables dynamic policy enforcement by integrating a number of security functions |
| 1. An employee attempts to connect to the network using a laptop |
| 2. Before network access is allowed, the following process takes place |
| • Employee is required to authenticate (log in) using valid credentials |
| • Laptop is automatically profiled to determine what type of device it is |
| • Laptop is automatically scanned to verify that data encryption is enabled (other policies may be verified as well) |
| • Information about the employee and laptop are correlated in the Network Sentry policy database |
| 3. Network access is dynamically provisioned based on appropriate policy (if the employee logs in successfully and the laptop has encryption enabled, network access will be granted; otherwise access may be denied or restricted) |
| 4. Employee logs into an application on a network server |
| 5. Application queries Network Sentry policy database to validate policy compliance (in this case that data encryption is enabled) |
| 6. Network Sentry policy database validates policy compliance and grants access to application server |
| BENEFIT | Network Sentry automates policy enforcement by integrating a number of disparate security functions, most of which already exist within the network environment. Policy compliance can now be ensured without burdening IT staff, and sensitive data on the network will be protected via encryption. |

Example #2 - Mitigation of Denial of Service (DoS) Attack

| PROBLEM | An employee of a large corporation is working on his laptop while connected to the company’s network. Unknown to the employee, malware on the laptop generates a denial of service attack on a network server which could take the server down and lead to costly productivity losses for the company. |
| SOLUTION | Network Sentry enables dynamic detection, response, and notification in the event of an attack |
| 1. A laptop on the network suddenly starts a denial of service (DoS) attack on a network server |
| 2. An IPS in the network detects anomalous traffic from the DoS attack and communicates information about the attack to the Network Sentry policy database |
| 3. Network Sentry policy database identifies the offending laptop by correlating IP address, MAC address, device profile, and location data, as well as the associated employee's identity and role |
| 4. The offending laptop is dynamically isolated from the network to stop the DoS attack |
| 5. IT personnel are automatically alerted of the attack |
| BENEFIT | Network Sentry leverages a number of disparate security functions within the network environment to detect the DoS attack, confirm the validity of the attack, stop the attack and notify IT personnel. The offending laptop is quickly isolated to minimize impact to the network and the organization. |

Example #3 - Dynamic Provisioning of Network Access

| PROBLEM | A county hospital is in the midst of rolling out a variety of new medical equipment, including hundreds of new devices that must attach to its network. The CIO is expected to complete the rollout in just days with existing IT staff that are already over-tasked with other responsibilities. |
| SOLUTION | Network Sentry enables dynamic provisioning of network access based on device identity and profile |
| 1. A technician plugs a new medical device into a port on the hospital’s network |
| 2. Before network access is allowed, the following process takes place |
| • Medical device is automatically profiled to determine what type of device it is and if it belongs on the network |
| • Information about the device is correlated in the Network Sentry policy database |
| 3. Network access is dynamically provisioned based on appropriate policy (access rights will be determined based on the identity and profile of the device) |
| BENEFIT | Network Sentry automates the process of provisioning network access for new medical devices, which minimizes the burden on IT staff for moves/adds/changes, while at the same time protecting against unauthorized access by unknown devices. |
CONCLUSION

Today’s networks – and the challenge of securing them – continue to evolve at a fast pace, and disparate silos of security technologies are not sufficient to meet this challenge. With today’s security model, organizations remain at risk and IT staffs are stretched to the limit trying to keep pace in a changing environment.

Existing security solutions must evolve to a flexible and adaptive approach to network security that integrates with numerous security technologies, correlates a vast array of information for complete network visibility, and automates network control and security policy enforcement.

Bradford’s Network Sentry is the only adaptive network security platform to meet evolving security challenges – evidenced by the many real-world solutions Network Sentry delivers to Bradford customers today.

Call InNet at 888-80-InNet to schedule a meeting today. Visit our website at innetworktech.com,