



Ranking the Top 5 Quarantine Approaches

Getting the most from your quarantine method

By Grant Hartline

This paper surveys the various quarantining methods offered by NAC solution vendors, grading each on several characteristics. The five methods we consider are:

- Flow Interruption
- Access Control Lists
- VLAN Switching
- Switch Port Shutting
- Address Resolution Protocols

We conclude that, on balance, quarantining methods based on address resolution protocols provide the best overall solutions to companies who are looking for remediation and visibility as well as network protection.

Introduction

As the quarantine requirements for NAC continue to evolve, three key requirements begin to emerge. The first is the ability to interactively lead the endpoint user through a series of remediation steps. Indeed, the oft-noted example of authentication is, at a high level, just another remediation step—something the endpoint user must do to bring her endpoint into compliance. The second and third surround the protection and visibility models for endpoints contained within a quarantine. As malware continues to morph into specifically targeted zero-day exploits that look to leak information as opposed to spread, visibility into traffic from a quarantined endpoint becomes critical for organizations looking to assess their exposure post infection; and as propagation vectors change from aggressive IP scanning to lightweight reconnaissance methods, holistic protection of and from quarantined endpoints is vital. Before delving into quarantine methods, a closer look at user-led remediation and protection and visibility models is in order.

An endpoint is quarantined when it is removed from a network. Endpoints are quarantined if they exhibit threatening behavior or violate a network policy.

User-Led Remediation

As is often the case with buzzwords, ask 10 people in a survey what remediation means within the context of NAC and you're likely to get 11 different answers. For the purposes of this paper, remediation is simply a set of steps needed to bring a non-compliant endpoint back into the

compliance required to gain (or – and this is important – regain) network access. At least at a high level, this can be as simple as the acceptance of an Acceptable Use Policy, or the submission of valid credentials. And it can be as complex as a notification to security staff that a managed endpoint's OS patch level is below the level of compliance, followed by the delivery of the required updates to the endpoint, followed by the inevitably required endpoint reboot. Many use cases exist in between.

An endpoint can violate a policy or become infected at any point in its lifecycle on a network.

That's a great deal of ground to cover, and there is a bewildering array of options. Two common threads exist, however. The first is that these steps can arise at any time during the endpoint's lifecycle on the network, from the moment of connection to the moment of disconnection. From authentication (think token based schemes), to policy compliance, to malware removal, every NAC solution should envision and provide for a means of remediation post-connect.

The second is that *some* form of user interaction is required. Even in the case of a fully automated software push, the NAC solution still needs to determine what happens in the meantime. Since no update can be downloaded and installed instantaneously, what level of network access is granted to the endpoint during the push? What is the user told during this process? Answering “nothing” to the second question and anything other than “everything” to the first is likely to result in a rash of help-desk calls.

Protection and Visibility Models

As opposed to the predominant threats seen, say, four years ago, today's threats are driven more by financial gain than rapid propagation. This difference places two demands on NAC solutions. The first is to provide a protection method for quarantined endpoints that envisions a true and complete quarantine. The network must be protected from the endpoint; the endpoint must be protected from the network; other endpoints (including those in the same segment) must be protected from the endpoint; and the endpoint must be protected from other endpoints, including those in its segment. Simply throwing quarantining bulkheads around the segment, or even the switch, may have been adequate for things like the Slammer infection. For lightly spreading, long-term threats, however, the quarantine needs to be

An incomplete quarantine is no quarantine at all. Quarantined endpoints must be completely isolated to prevent further contamination to the network or the already infected endpoint.

complete if administrators can hope to actually eliminate the malware from their environment.

The second demand is, at a minimum, ongoing flow-level visibility into the traffic bound to and emitting from the quarantined endpoint. A zero-day exploit that begins with a web page hit, followed by a post to a botnet controller, followed by an IRC backdoor poses significant issues for products in the NAC space. The first is that this type of infection is not just possible but the most likely once an endpoint has successfully authorized its initial connection, which means that any connect-time check fails to help. The second is that the zero-day characteristic allows for infection of an otherwise fully compliant endpoint, so no amount of compliance checking helps. The third is that the blended nature of the exploit demands that the NAC solution in place must be capable of providing relevant information post-infection.

5 Quarantine Methods Go Head to Head

1. Flow Interruption

Traditionally in the domain of IDS and early IPS products, flow interruption techniques, namely TCP Resets and ICMP Unreachables, saw some early adoption as mitigation methods for LAN based security products. From a network protection perspective, flow disruption has considerable issues to overcome, not the least of which are (a) the requirement of interrupting every flow from a quarantined device and (b) the reliance that the quarantined host will accept the disruption and discontinue the flow. From a remediation perspective, flow disruption not only doesn't help but also actually hurts. While other quarantining methods provide at least an improvised method of effecting notification and remediation, flow disruption is likely to interfere with these techniques as the disrupting device attempts to hold the endpoint in some kind of holistic quarantine.

Neither ACL engineering nor flow interruption techniques provide support for remediation.

2. Access Control Lists

In general, Access Control Lists are a critically important component of any in-depth security strategy. In the NAC context, dynamically generated ACLs run the risk of being either too broad or too specific, particularly given the blended and always-morphing face of exploits. From a visibility perspective, a log of hits presumably can be part of

the generated ACL; but it's often cumbersome to pull that log data into a larger management framework. Finally, dynamic ACLs are designed to either drop packets or not; they are not designed to interface with users and redirect them from what they were going to do to what they now need to do, so from a remediation perspective ACLs are no help at all.

3. VLAN Switching

Whether accomplished via vendor-specific protocols (such as VMPS on Cisco gear), vendor-specific integration with standard protocols (such as SNMP integration) or standard protocols such as 802.1x, VLAN switching appears to be the most-discussed quarantine method for NAC products. Taken on its own, VLAN switching is exactly as the name implies: the placement of an endpoint into a VLAN. There is certainly a place for this in any defense-in-depth strategy, and actions such as identity-based VLAN assignment are likely long-term components of an overall NAC strategy. However, by its nature, VLAN assignment of an endpoint is simply a single component of a much larger framework. Want actual protection from the traffic? Better have an ACL in place. Want visibility into the endpoint's traffic? Better have a sniffer in the VLAN ready to go. Want user-led remediation? Perhaps cobbling together transparent redirection with some sort of proxy can get you there. While identity or property based VLAN assignment can be an effective policy statement, for the purposes of effecting a short-term quarantine, providing remediation, and letting the user get back to work, VLAN switching hardly fits the bill.

This method, also referred to as the "VLAN of Death" scheme, can create a pod of endpoints that share their infections, which complicates remediation.

4. Switch Port Shutting

Since the process of changing VLAN membership of a particular switch port is considered above, this section focuses on the act of shutting a switch port as part of an enforcement scheme, whether explicitly, via RSH or SNMP, or by forcing the port into a NOAUTH 802.1x state. From a protection perspective, this technique is obviously highly effective. Indeed, it is difficult to provide more protection to either the network or the endpoint except by simply removing connectivity altogether. This protection model comes at a cost, however, that makes it unworkable for anything other than the most basic of NAC implementations. Visibility into ongoing traffic from the endpoint is null, as is any network-based remediation. Additionally, shutting switch ports has consequences for overall network architecture, since it

Shutting a switch port is like closing a dam; contaminants can't travel downstream, but when the creek dries up, all the fish die anyway.

disrupts everything downstream. In IP Telephony environments, to name only one, this may well prove unsupportable. For extreme cases, the Slammer infection for example, these trade-offs may be acceptable. For garden-variety NAC remediation (captive portal authentication, informational pages while pushing an update, etc), however, this falls well short.

5. Address Resolution

Even assuming that most Ethernet networks are running TCP/IP as the upper layer protocol suite, the opportunity to leverage address resolution protocols exists at a couple of layers of the OSI model. Translating DNS names to IP addresses and translating IP addresses to MAC addresses are the two best examples. At a high level, the primary benefit of using address resolution as an enforcement methodology is that it provides the best balance across all three requirements of protection, visibility, and remediation without sacrificing one for the others. When done correctly, address resolution based quarantining combines the ease of an out-of-band deployment model with a protection model that is often even more effective than inline solutions, since it applies to all traffic originating from or sent to the endpoint. From a visibility perspective, address resolution based quarantining is also highly effective, since all traffic emitting from and headed towards the endpoint is captured. Finally, by being in the endpoint's path at a protocol level, appliances leveraging address resolution for quarantine can provide end-user notification and remediation in a way that assures a consistent user experience. The primary disadvantage to address resolution-based quarantine is that it depends upon the quarantining device's visibility into the resolution path. Leveraging DNS for quarantine, for example, depends upon having the quarantining device either act as the DNS server or spoof replies back to the client. Likewise, leveraging IP-MAC lookups (ARP in IP version 4 and Neighbor Discovery in IP version 6) for quarantine relies on layer 2 visibility of the endpoints by the quarantining device.

Address resolution can create the best of both worlds—an out-of-band NAC solution that deploys easily, yet precision quarantines like an inline agent.

Summary: Why Address Resolution Is Best

Much has been said about how NAC is a framework. If it is going to be successful, NAC must be a solution. NAC products can and should provide integration into other existing components of IT infrastructure. NAC products can and should work within defined standards to provide interoperability across organizational and operational

boundaries and provide investment protection for customers. But in the end, NAC products should install and function as a solution. Certainly, the degree of the solution encompasses many factors (post-admission as well as pre-admission compliance, manageability, reporting, etc.) in addition to quarantine method; however, how offending users are quarantined, remediated, and admitted back onto the network is the single most visible component of the NAC solution across the organization. Recent reports (Forrester) on the NAC industry generally indicate that end-user acceptance of the NAC solution has been an impediment to wide-scale NAC implementations, and remains a gating factor. In order to gain the acceptance of their end-user base, organizations looking for a NAC solution should ask themselves, and the prospective vendors, questions such as:

- Does the protection model protect same-segment endpoints from each other?
- Does the protection model allow for continued visibility into dropped traffic?
- When an endpoint is denied network access at connect time, how is this communicated to the user of the endpoint and what methods are provided to gain access?
- When an otherwise fully compliant—and already connected—endpoint violates usage policy, gets infected, or is otherwise deemed a threat, how completely is the endpoint quarantined? What is communicated to the endpoint user and operations staff?
- How do end users request assistance or provide feedback while in quarantine?

Questions such as these can allow evaluating network staffs to begin to separate the wheat of NAC solutions from the chaff of products that simply provide components that can only function within a much larger overall framework. A NAC implementation that, under any circumstances, restricts end-user access without communication to the end user about that restriction or the means to get unrestricted is unlikely to pass the user-acceptance test. Likewise, just dropping undesirable traffic without giving security operations staff visibility into the traffic—and therefore visibility into the organization's exposure—is unlikely to meet the ultimate statutory compliance requirements many organizations face

today. Finally, a protection and quarantining model that protects same-segment endpoints from each other, as well as protecting the network from the endpoints, is vital given the malware active in today's landscape.

Grant Hartline is Chief Technical Officer for Mirage Networks, a leader in NAC solutions. For more information, visit www.miragenetworks.com.

Address Resolution	<ul style="list-style-type: none"> • Deploys easily and without network disruption • Provides continuous visibility into traffic flow from quarantined endpoints • Precision quarantines, eliminating cross contamination • Provides continuous protection, both pre- and post-admission
Switch Port Shutting	<ul style="list-style-type: none"> • No visibility into traffic from quarantined endpoint • Destabilizes network architecture by disrupting all traffic downstream of the closed switch port
VLAN Switching	<ul style="list-style-type: none"> • Cannot protect a network from threatening traffic without an ACL • Provides no visibility into traffic flow without a sniffer • Does not natively support user-led remediation
ACL Engineering	<ul style="list-style-type: none"> • No support for remediation • Log data can be difficult to integrate into a management console • Dynamically generated ACLs tend to be either too broad or too specific
Flow Interruption Techniques	<ul style="list-style-type: none"> • No support for remediation • Depends on the quarantined endpoints' acceptance of the disruption and discontinue flow on their own