Enforcing endpoint security through network-based Quarantine Protection

Business white paper
# Table of contents

**Introduction** ................................................................. 3

**Quarantine in the business** ....................................................... 3
  Quarantine market ................................................................. 3
  The superiority of network-based solutions ........................................ 3
  Clientless architecture ............................................................. 3
  IPS-based solution ......................................................................... 4
  Centralized management ............................................................ 4
  Working with Microsoft NAP .......................................................... 5

**Quarantine concepts and configurations** ............................................. 5
  IPS Quarantine ............................................................................ 5
  SMS Quarantine ........................................................................... 5
  Switch actions .............................................................................. 6
  Quarantine policies ....................................................................... 6
  SMS with NMS ............................................................................ 7

**Deployment considerations** .......................................................... 7
  Time to deploy ............................................................................. 7
  Speed of response ........................................................................ 7
  Minimizing manual intervention ....................................................... 8
  Segment or resource unique business needs ...................................... 8
  Deployment growth ....................................................................... 8

**Summary** ....................................................................................... 9

**Appendix A: SMS MIB examples** ................................................. 9

**Appendix B: SMS HTTP API for network identity management** .............. 10
  Overview .................................................................................... 10
  Customer settings .......................................................................... 10
  Parameters .................................................................................. 10
  Base parameter: method ................................................................. 10
  Return information ........................................................................ 10
Introduction

The most dangerous security threats often emanate from within corporate LANs, and the only true defense is to strictly enforce security policies throughout the entire network.

HP TippingPoint’s Intrusion Prevention System (IPS) incorporates innovative enhancements to prevent the propagation of cyber threats from within the network and quarantine infected devices. This quarantine process prevents the infected device from harming neighboring systems and provides instantaneous redirection to remediation webpages or URLs.

Endpoint security should always include antivirus software and OS patch updates as a base level of security. However, HP TippingPoint’s Quarantine capability complements and goes beyond the simple verification of updated OS and AV signature packs to control the behavior of endpoints that are connected to the LAN. With HP TippingPoint Quarantine, administrators virtually extend sophisticated attack filters from the HP TippingPoint IPS down to the desktop, while maintaining complete control at a central location within the network.

HP TippingPoint offers a standards-based network IPS that will stop the flow of malware and identify the local source of the offending traffic. With the release of Security Management System version (SMS) 2.2, and the HP TippingPoint Operating System version (TOS) 2.2, HP TippingPoint introduced “Quarantine” to take the offending source offline and stop malicious traffic flows proactively. This white paper will provide an overview of the quarantine options and capabilities, providing the reader with an effective technical introduction to this powerful new security tool.

Quarantine in the business

Quarantine market

Many technology vendors have concluded that the best way to enforce LAN security is to make sure that the client is secure before allowing access to the network. Vendors accomplish this by using a host-based client to verify that the host has an updated operating system (OS) and antivirus (AV) signature pack.

HP TippingPoint endorses the enforcement of AV and OS updates as a best practice to network and client security. However, through research in the network security field, HP TippingPoint has concluded that AV and OS updates alone are an insufficient solution to LAN security, for several reasons:

- There is a gap in time between the discovery of new threats and the availability of OS/AV updates, during which malicious traffic will propagate even after an integrity scan
- Denying network access to end users creates help desk calls
- Host integrity checking is inflexible for exceptions or VIPs
- Verification of updated OS/AV systems does not prevent malicious user activities whose endpoints pass a profile check
- The rate of discovery of new threats will cause network administrators to adjust their security policy on a daily basis
- The client-based approach prevents the verification of all endpoints, leaving alternative operating systems, printers, VoIP phones, and wireless devices unchecked

HP TippingPoint has created a superior solution to host integrity checking that is also complementary, by offering a more advanced philosophy in dealing with the LAN-based threat. Instead of making an access decision based on the profile of the endpoint, HP TippingPoint makes an access decision based on the activities of an endpoint. In other words, actions speak louder than profiles. By extending the power of the world’s most advanced IPS down to each endpoint, HP TippingPoint offers a clientless solution that is automatically updated against the latest threats, isolating offending endpoints and propagating security throughout the entire network.

The superiority of network-based solutions

There are three main reasons why a network-based solution can deliver greater value to network and security managers than a host integrity checking solution. A network-based solution is:

- A clientless solution
- An IPS-based solution
- A centrally managed solution

Clientless architecture

The HP TippingPoint Quarantine architecture is a network-based solution, which reduces costs and simplifies deployment. With literally thousands of devices in a typical enterprise environment, the management of each of these individual end-points is
both labor intensive and time consuming; which ultimately reduces the effectiveness of any security solution.

Software distribution solutions require client interoperability testing and agent management. Further, unless the network environment is homogenous, the variety of OS versions and types can drive significant testing investments.

Today’s client-based solutions are designed for Windows® PCs only. The inability of a client to be loaded onto VoIP phones, wireless devices, printers, or PCs with Mac or Linux operating systems leaves a significant portion of the network untouched. The HP TippingPoint Quarantine solution does not rely on a software client; all endpoints on the network are protected without the additional overhead incurred by purchasing, deploying, and maintaining a client.

Many contemporary organizations are dynamic, growing environments where flexibility and responsiveness are keys to success. While having a strict and rigorous network connection policy would certainly be of value, its implementation could require significant investment of both time and money. Often the load of “exception handling” is excessive, making it difficult to keep partners and remote workers connected without interruption. These considerations often lead to evaluate a solution’s TCO.

**IPS-based solution**

Through confirmation from independent analyst firms, the evolution of security vendors’ products, and the fantastic growth of the IPS market, intrusion prevention systems are widely recognized as the next evolution of security technology. HP TippingPoint Quarantine solution harnesses the protective power of the IPS and extends this protection down to the endpoint itself.

With this evolution, the method of detection for the endpoints moves beyond signature-based inspection to leverage behavioral analysis techniques as well. By understanding a baseline of normal traffic behavior, the IPS is able to detect significant deviations from this baseline, which indicate abnormal or malicious network activity levels. HP TippingPoint behavioral recognition technology provides yet another layer of defense against the propagation of worms and viruses in the network.

Another advantage of HP TippingPoint IPS-based solution is its automated nature. As new threats are discovered on a regular basis, HP TippingPoint IPS’s are automatically updated with the latest Digital Vaccine Filters to protect against both disclosed and undisclosed vulnerabilities. In essence, every node on the network instantly benefits from the evergreen protection of the IPS without requiring network administrators to manually change their security policy every time a new Microsoft® vulnerability is disclosed.

One of the most significant advantages of HP TippingPoint’s IPS-based Quarantine solution is that it goes beyond prevention from worms and viruses, to block malicious user activities as well. While a client-based solution’s impact ceases after the decision to allow an endpoint onto the network, the HP TippingPoint solution continues to monitor the activities and behavior of every node on the network to prevent malicious users from launching attacks or performing reconnaissance scanning to either the rest of the LAN or to other external networks.

**Centralized management**

Centralized management is imperative for any network security system. HP TippingPoint centralized management allows for extensive flexibility in the security policy created by a quarantine solution. Many host integrity solutions have a “black-and-white” reaction to an endpoint, which can frustrate VIP users and unintentionally block mission-critical resources from communicating. To address this problem, HP TippingPoint Quarantine solution offers flexible configuration through white lists for IP addresses and address ranges, and flexible policies for internal or external addresses.

Centralized management flexibility is also achieved through the variety of quarantine actions. Thresholds are set by the SMS in order to tune the sensitivity of the quarantine action. Once invoked, several different actions can be taken to inform and remediate the user including redirection to VLANs, redirection to URLs, serving customizable webpages that dynamically display the actions that triggered quarantine, and the configuration of ACL’s.

The SMS can also be configured to work with any third-party network or enterprise management system to invoke quarantine. The SMS can forward event information to a network management system (NMS) where either an automated action or a trusted administrator can initiate the desired action. This configuration allows administrators to create an automated quarantine function via the NMS or to create a manual quarantine function themselves.
Working with Microsoft NAP
As Microsoft’s NAP is introduced on Microsoft’s operating systems, administrators who wish to leverage a host integrity checking solution to verify an updated OS and AV exists before allowing an endpoint to authenticate can leverage integration of HP TippingPoint with Microsoft Network Access Protection (NAP).

When using NAP, if a client attempts to access the network, it must present its system health state. If a client cannot prove it is compliant with system health policy (for example, that it has the latest OS and AV updates installed), its access to the network will be restricted to a special network segment containing remediation server resources so compliancy issues can be remedied. After the updates are installed, the client requests access to the network again. If compliant, the client is granted full access.

Quarantine concepts and configurations
While Quarantine can be implemented seamlessly and quickly into any network infrastructure, implementations can vary in architecture, capability, point of control, and level of automation. HP TippingPoint provides three configurations for Quarantine:

• **IPS Quarantine**—One of the simplest scenarios to stop an infected host’s activities using only an IPS appliance.

• **SMS Quarantine**—This higher level of automation provides a more advanced quarantine action set.

• **NMS Quarantine**—The SMS leverages an existing NMS to provide a flexible level of automation and a different point of control.

IPS Quarantine
In the most basic configuration, the HP TippingPoint IPS acts alone to enforce security and initiate remediation of the infected host. By running in line, the IPS appliance inspects all the activities for malicious traffic. When malicious traffic is encountered, the IPS will block, notify, rate-limit, and/or quarantine based on the security policy defined. With a block/quarantine action set invoked, the IPS can recognize the source of malicious traffic and block all subsequent traffic from the source IP address.

At this point, client Web requests will generate a quarantine notification page. This webpage can be customized based on the trigger that invoked quarantine, to inform the user as to why they have been quarantined. Optionally, users can be automatically redirected to a remediation server or website with repair instructions.

Quarantine is a powerful defense mechanism that automatically blocks malicious traffic on a network segment from traversing the network. This solution also provides instructions for self-remediation. However, even when blocked at the IPS, infected hosts can still communicate with other hosts in a segment, potentially infecting the rest of that portion of the network. In order to prevent intra-segment infections, a more proactive response to malicious traffic is needed. By leveraging HP TippingPoint IPS with an SMS, an offending source can be isolated from the entire network automatically.

SMS Quarantine
SMS Quarantine uses the HP TippingPoint SMS with the IPS. This configuration facilitates automatic isolation of infected hosts. When the IPS sees malicious traffic, that traffic is blocked at the IPS and an alert is sent to the SMS. While the IPS may quarantine a user based on the alert, the SMS can use this event data to invoke more powerful quarantine actions from a central location, including:

• IPS Quarantine (if not already invoked)

• Redirection of Web traffic to a remediation page

• IP/MAC correlation—associates a malicious IP address with a MAC address

• Creation of SNMP trap—enables an industry-standard alert or switch command script

• Disconnect from switch—forces the host to reauthenticate on the access switch and not let them on the network

• Move quarantined host to VLAN—forces the device into an isolated, secure environment

• Creation of Syslog event—sends an event log to external management system or Syslog server

• NMS interaction—works directly with a network management system to alert or take action on the access switch

• Email—sends an email notification to a designated contact
Switch actions
Switch level actions are powerful and provide proactive protection at the access layer. SMS Quarantine offers two critical switch level actions which are closely related: access switch disconnect and placement in a secure VLAN. In order to act on the switch, there must be some means of associating the MAC address known to the access switch and the IP address of the offending device known to the IPS. This can be accomplished with MAC-based authentication mechanisms coupled with queries of Layer 3 devices.

The common use of RADIUS authentication services simplifies the IP/MAC correlation process. During authentication, the SMS can act as a proxy to a RADIUS server and alter the RADIUS response to either deny network access and/or place the device in the secured VLAN. A network employing either 802.1x or 3Com RADA will accelerate the enablement of switch-based Quarantine actions. HP TippingPoint provides a Web service method to enable capture and import of IP and MAC address correlation, described in Appendix B. Requests to an ARP cache may be used to populate the source database, which the SMS will reach via the Web service. This correlation table can then be queried and tested from the SMS environment as needed.

Quarantine policies
While simple quarantine policies for IPS Quarantine can be configured on the IPS locally, the more powerful SMS Quarantine policies are configured from the SMS. These policies specify the conditions that generate quarantine actions. SMS Quarantine policies are created by specifying the following criteria in the SMS:

- Policy name
- IPS devices and segments to apply policy to
- Filters to trigger quarantine
- IP address ranges to monitor (or exclude)
- Quarantine action (switch disconnect, VLAN, Syslog, SNMP trap, NMS trap, email, and/or IPS Quarantine)
- Thresholds

Thresholds allow administrators to control the sensitivity of the quarantine action. Thresholds are particularly valuable for cases where it is important to note the frequency and quantity of suspect behavior. Using the SMS to monitor alerts, the suspect’s activities can be observed over a period of time before triggering quarantine.
Quarantine policies are extremely flexible, facilitating the specification of an IP address range and exceptions for mission-critical IP addresses or VIP users. An auto-unquarantine timeout period can be applied, as well as the ability to manually quarantine or unquarantine a host. This allows for human intervention to take priority over any automated policies and actions as needed.

**SMS with NMS**

SMS-based Quarantine is an extremely powerful solution that brings an exceptional amount of automation to a network. However, some users may wish to leverage their NMS in conjunction with Quarantine in order to track change management, create audit trails, segregate security and networking responsibilities, or maintain a single point of control for network access. For users who prefer to leverage an NMS in conjunction with Quarantine, HP TippingPoint has built extensive interoperability between the SMS and NMS's.

While the SMS is capable of taking direct action in response to threats via quarantine, it can just as easily send that information to an NMS. From the NMS, administrators can optionally configure similar switch disconnects for an automated solution, or simply process the information for manual intervention by IT staff.

Through standard SNMP traps and Syslog event data, the SMS can communicate the same information it uses to make quarantine decisions to the NMS. User location, MAC/IP address, switch IP, and event triggers can be forwarded to an NMS for further automation or manual intervention. By interoperating seamlessly with NMS, HP TippingPoint offers an intermediate level of quarantine automation, allowing administrators to comfortably deploy quarantine in the way that best suits their network and policy.

HP TippingPoint provides several means by which an IT organization can directly integrate the IPS/SMS solution into their management fabric. The simplest and most common approach is to utilize the enterprise Management Information Base (MIB) provided for the SMS. HP TippingPoint has documented how to work with popular systems and network management tools such as Tivoli and HP OpenView provides step-by-step instructions for creating this interface to the SMS MIB. The SMS MIB and its quarantine details are described in Appendix A. The MIB information is also accessible through a Web Services interface for the SMS.

**Deployment considerations**

With an understanding of the available Quarantine options, the attention now turns to best practices in deployment. As with any IT deployment, this requires planning and prioritization. This section discusses some of the issues to be considered.

**Time to deploy**

Quarantine coverage can be extensive with the right amount of time and investment. There are also near term benefits that can be gained quickly. IPS Quarantine actions are the easiest and simplest to deploy. In a matter of minutes, an administrator can cover a wide number of hosts with a basic policy that will both protect the network and inform the host user of the issues detected.

IPS Quarantine actions can be replicated across all IPS’s within the management reach of the SMS. The benefit here is a centralized security enforcement and efficient scale out deployment; but with greater effort a more sophisticated and powerful Quarantine response is possible. For example, threat specific actions and alerts can be enabled, or the DBA on site can receive email alerts of SQL Server exploits. Similarly, popular database monitoring tools such as BMC’s Patrol or Quest’s Foglight can receive SNMP traps on the traffic.

**Speed of response**

Speeding the quarantine action of a malicious source may be more important to an organization than a sophisticated analysis and response. When it is desired to minimize the amount of time to cease an activity, the fastest response will come with the IPS Quarantine configuration. In this scenario, the first detected attack will initiate an IPS level action set to stop malicious traffic and blacklist a user immediately.
This approach can also notify the SMS; which in turn could initiate a network-wide quarantine without any additional thresholds or data processing. Threshold-based policies will introduce a slight delay between detection time and quarantine response. This delay will be driven by the threshold conditions within the policy.

**Minimizing manual intervention**

For some organizations, the priority will be on realizing the benefits of an automated detection and resolution solution. In these cases the ability to propagate rules and actions across a wide portion of the network offers significant value.

With some upfront investment, the HP TippingPoint administrator can determine the appropriate triggers to act upon and specify appropriate actions. Actions of interest could be as simple as telling the user their machine is infected or as sophisticated as directing them to a triggers-specific resolution page on a Web server. Coupled with a service desk solution, a trouble ticket can be automatically generated to initiate proactive resolution for the problematic behavior.

**Segment or resource unique business needs**

Different network areas have different needs based on the services they provide to the business. Individuals responsible for these specific services or segments may customize or append the base Quarantine policies with unique policy/action combinations. A network segment with transient attachments and many individual PC users may require greater focus on items such as spyware and phishing triggers. The resolution activities associated with the triggers can be more aggressive as taking an individual’s PC offline or other restrictive actions will likely impact a minimal part of the business.

Network segments with back office applications require careful handling and will likely have less stringent quarantine actions for the systems involved. A quarantine against the company’s accounting system or email server can have wide ranging impacts to a great number of people. With SMS Quarantine, an administrator can explicitly exempt specific machines and thus remove those from general quarantine actions. There are additional ways to safeguard against negative impacts, such as simply removing the problematic traffic from the network without removing the source from the network itself.

All actions can be coupled with an alert to an application-specific tool. Examples of this coupling include Oracle Enterprise Manager, or an email to the DBAs responsible for those resources. Critical resources are thus protected from malevolent behavior with the IPS, but handled gently to provide for continued business access.

**Deployment growth**

What kind of project plan should be put in place for Quarantine deployment? The answer will likely vary depending on some of the following factors:

- Experience with HP TippingPoint solution
- Time and resources to invest in customization
- Completeness of needs and response understanding
- Corporate policies on compliance and standards

If the HP TippingPoint solutions are already in place and experience is relatively high, the challenge is to simply expand what is already in place. A good first step is to set up IPS quarantine actions and test them over a period of time. As those policies and actions are honed, the decision can be made to deploy them more widely.
If the administrative team is not familiar with the IPS and SMS solutions, then starting with very basic IPS Quarantine is probably the best place to start. Whatever the need for Quarantine in the organization, HP TippingPoint Professional Services Organization can provide both training and consulting services to accelerate a successful deployment.

Summary

Quarantine features in the HP TippingPoint IPS and SMS products will protect network resources while decreasing human investment in the process. HP TippingPoint’s Quarantine facilitates a rapid and cost-effective means of enabling network-based endpoint security. With flexible deployment options, any administrator can make endpoint Quarantine fit within the organization’s policies and work with prior management and hardware investments. Powerful actions give control and awareness to IT teams dealing with an ever-growing security threat. With HP TippingPoint Quarantine, an organization can truly deliver cost-effective, proactive endpoint, and network security.

Appendix A: SMS MIB examples

tptSmsQuarantineRequest NOTIFICATION-TYPE
OBJECTS { tptSmsQuarantineNotifyId,
tptSmsQuarantineNotifyData }
STATUS current
DESCRIPTION
“Request a quarantine of a device using the data embedded in the request”
 ::= { tpt-sms-eventsV2 1 }
tptSmsQuarantineAck NOTIFICATION-TYPE
OBJECTS { tptSmsQuarantineNotifyId,
tptSmsQuarantineNotifyData } STATUS current
DESCRIPTION
“Acknowledge a quarantine of a device using the data embedded in the request”
 ::= { tpt-sms-eventsV2 2 }
tptSmsQuarantineReleaseRequest NOTIFICATION-TYPE
OBJECTS { tptSmsQuarantineNotifyId,
tptSmsQuarantineNotifyData }
STATUS current
DESCRIPTION
“Request the release of a quarantine of a device using the data embedded in the request”
 ::= { tpt-sms-eventsV2 3 }
tptSmsQuarantineReleaseAck NOTIFICATION-TYPE
OBJECTS { tptSmsQuarantineNotifyId,
tptSmsQuarantineNotifyData }
STATUS current
DESCRIPTION
“Acknowledge a release of a quarantine of a device using the data embedded in the request”
 ::= { tpt-sms-eventsV2 4 }
tptSmsQuarantinePolicyNotification NOTIFICATION-TYPE
OBJECTS { tptSmsQuarantinePolicyMatchData }
STATUS current
DESCRIPTION
“Notification of a policy match”
 ::= { tpt-sms-eventsV2 5 }
tptSmsUnQuarantineRequest NOTIFICATION-TYPE
OBJECTS { tptSmsQuarantineDeviceIP,
tptSmsQuarantineDeviceMAC }
STATUS current
DESCRIPTION
“Request SMS to release the quarantine of a device using the data embedded in the request. Either the IP or MAC or both can be specified.”
 ::= { tpt-sms-eventsV2 6 }
Appendix B: SMS HTTP API for network identity management

Overview
This section describes the HTTP protocol that will be used to provide the SMS Quarantine Policy Engine with network identity management. The idea is to expose an API that can be easily implemented using a common, and easy to develop protocol, HTTP.

Customer settings
The user will provide some basic configuration information. This information will be used to build the URL for making correlation queries over HTTP(S).

- Protocol—HTTP or HTTPS
- Server IP
- CGI script
- Basic HTTP authentication—(Y/N)—Credentials

Given this data the SMS will build up a base URL for making HTTP GET requests to query about the network.

Example:
Customer provides:
Protocol = HTTP IP = 10.100.230.111
CGI Script = cgi-bin/myNetLookup
SMS generates the following, and will apply the needed parameters:

Parameters
The following parameters are sent to the CGI program, appended to the URL.

Base parameter: method
- IPLOOKUP—Return everything known about this IP.
  - IP=123.123.123.123
- MACLOOKUP—Return everything known about this MAC.
- SWITCHLOOKUP—Return everything known about switch at IP.
  - IP=123.123.123.123
- NETCONFIG—Retrieve network settings for a MAC or IP
  - IP=123.123.123.123

Example Queries:
HTTP://1.1.1.1/cgi-bin/myLookup?METHOD=IPLOOKUP&IP=10.100.230.111
HTTP://1.1.1.1/cgi-bin/myLookup?METHOD=MACLOOKUP&MAC=00:00:00:00:00

Return information
The SMS will use the HTTP header information to determine success or failure, and the body of the response will result in name-value pair format. A successful response will expect a HTTP 2XX status code. Anything else will be considered an error condition and fail the call.

Each line on the response is in the following format:
Attribute=Value, for example MAC=00:02:fe:ed:ed
Possible return attributes:
• PCIP—IP address in dot notation
• PCMAC—PC MAC in xx:xx:xx:xx:xx format
• USERNAME—The user login associated with the PC IP
• SWITCHIP—SWITCH IP associated with PC IP
• SWITCHMAC—MAC in xx:xx:xx:xx:xx format
• SWITCHPORT—The port on the switch associated with SWITCHIP
• SWITCHLOGIN—Login account for SWITCHIP
• SWITCHPASSWORD—Password for SWITCHLOGIN on SWITCHIP
• NETCFG VLAN—VLAN network configuration
• NETCFG QUARANTINE VLAN—VLAN for assigning quarantine
• NETCFG IP—Configure user with this IP address
• NETCFG GATEWAY If the CGI script will need more than 10 seconds to process response
• RETRY=N—Cause the SMS to retry the operation in N seconds

The use of RETRY is to allow the CGI script to queue up a task that may take a long time. This allows immediate response to SMS. The SMS will then retry the query in N seconds, or as close to that time as possible.

To prevent malicious traffic flows proactively with HP TippingPoint Quarantine solution, visit www.hp.com/networking/security.