CONFIGURATION GUIDE

3Com® Solutions: QUARANTINE

UTILIZING IPS, SMS AND EMS

3com®

3Com Solutions: QUARANTINE

UTILIZING IPS, SMS AND EMS

CONTENTS

INTRODUCTION

Our customers need to tightly couple network visibility and control into their network without disrupting day-to-day business operations and incurring huge capital and operational expenses. They are looking for end point protection, scalability from tens to thousands of end points, efficiency and compatibility among systems from multiple vendors.

Quarantine is an important building block in meeting these needs.

Quarantine is a powerful tool and its usage can be as varied in the networking and security world as the vendors who give it different meanings and definitions. However, the general purpose of Quarantine – common to all vendors' solutions – is to separate a target from the rest of the network environment.

There are other security solution areas that invoke this phrase. For instance, vendors of IPS (Intrusion Prevention Systems) and end-point focused Network Access Control/Network Access Protection (NAC/NAP) tools also cite "quarantine" as a capability.

For NAC/NAP vendors, Quarantine is separation from normal network access. Here, Quarantine takes place from the first attempt to join the network; a device is in Quarantine until it can prove it has met some criteria before it is allowed on the network. For IPS, the Quarantine action will be triggered by the IPS. As contrasts to the NAC/NAP solution, in an IPS-driven environment the end point is free until it initiates malicious or undesirable activity.

WHAT IS QUARANTINE?

For 3Com, Quarantine is the state at which the IPS and/or the Security Management System (SMS) have initiated an action against a device because of its activities. The typical scenario is that the IPS detects problematic traffic coming from a device and initiates action to Quarantine.

In general, Quarantine actions are:

- IPS Quarantine – block all traffic and redirect HTTP traffic to a web page
- Write to a syslog
- Send an email
- Send a Simple Network Management Protocol (SNMP) trap
- Invoke a Network Management System (NMS) action
- Remove a device from the network – initiated at the access switch
- Place a device into a VLAN – initiated at the access switch

ABOUT THIS GUIDE

This Quarantine Configuration Guide describes best practices for any technical pre- or post-sales engineer wanting to deploy enhanced security into a network using 3Com equipment. The guide specifically focuses on deploying network Quarantine with the 3Com Enterprise Management Suite (EMS), TippingPoint IPS system and SMS system. It is organized into five sections:

- Best Practices – What to Quarantine and Not
- Deployment Configuration and Topology
- Step-by-Step Configuration
- Running and Verifying a Quarantine Example
- Troubleshooting

A listing of used terms appears at the back.

BEST PRACTICES – WHAT TO QUARANTINE AND NOT

QUARANTINE END USERS

It is important to identify what you wish to protect your network resources from. This is the process of risk mitigation by which you determine what is likely to be your greatest source of risk and then the type of risk.

A common scenario arises from mobile or non-employee access points. Mobile sources do not just mean wireless, but the device of any user that is likely to be taken out of the internal network and used in accessing other network environments outside the customer's control. Another source is non-employees who are not under the direct control of the company. Both of these end-user groups are valid foci as potential sources of problematic network traffic.

While Windows-based PCs are the typical target for threat mitigation, remember that unlike most NAC/NAP solutions, the Quarantine will operate on any type of device; any device that can be a vector for a threat can be placed under Quarantine control.

It is also important to note that another part of the overall Quarantine process is what to omit from Quarantine actions. Identify key processes that one would not want to Quarantine. Business-critical devices or inter-switch connections are strong candidates for omission.

Once a list of Quarantined hosts has been selected, a Quarantine deployment configuration must be selected, as noted in the next section. When deploying any Quarantine mode, it is advisable to take 'baby steps' in the process. That is, before denying or removing hosts or clients from the network, a first step is to identify the misuse and report it as an SNMP trap, email or a syslog message. Once comfortable with the Quarantining process, only then enable switch-level Quarantine actions, such as moving a device to a Quarantine network or even disabling the port on the switch to which the device is connected.

DEPLOYMENT CONFIGURATION AND TOPOLOGY

DEPLOYMENT OPTIONS

There are several options or modes of deploying a Quarantine solution, depending on the 3Com product being used in the customer network, as follows:

- IPS
- SMS + IPS
- SMS + IPS + EMS
- SMS + IPS + 3Com Network Director

All of these options have advantages and disadvantages depending on whether the Quarantine solution is being built upon a 3Com or a non-3Com infrastructure. The advantages and disadvantages are outlined below.

IPS Quarantine Standalone

This deployment option calls for a standalone TippingPoint IPS or several standalone IPS systems throughout the network. The TippingPoint IPS systems can Quarantine independently.

Advantages

- Easy to deploy
- Requires no integration with any other infrastructure
- Fast responsiveness to a Quarantine action
- Switch-independent: works regardless of network manufacturer

Disadvantages

- Still requires a network management solution for bulk configuration of the infrastructure devices
- Increased management overhead with use of more than one IPS system

Compatible Products

All

SMS + IPS Quarantine

This solution uses a TippingPoint SMS with one or more TippingPoint IPS systems.

The SMS offering can manage several IPS systems at the same time. This solution can provide more Quarantine choices than the standalone IPS.

Advantages

- Easy to deploy
- Works in heterogeneous network environments
- Requires no integration with any other infrastructure
- Fast responsiveness to a Quarantine action

Disadvantages

- Limited functionality with non-3Com switches
- Still requires a network management solution for bulk configuration of the infrastructure devices

Compatible Products

All

SMS + IPS + EMS

This integrated solution uses a TippingPoint SMS with one or more TippingPoint IPS systems and 3Com Enterprise Management Suite (EMS). The SMS acts as the security policy system, the IPS handles traffic identification and EMS manages the network, isolating the hosts using RADIUS Authentication Device Access (RADA).

Advantages

- Customizable and flexible – possible for Professional Services to add 3rd-party device support
- Works in heterogeneous network environments
- Provides all Quarantine actions, including removing a device and placing it into another VLAN
- Integrated approach – Network Change and Configuration Management (NCCM) Tool ensures no duplication of network inventory

Disadvantages

- Requires a higher level of integration and configuration

Compatible Products

3Com Switch 4400

3Com Switch 5500

3Com Switch 7750 (planned)

Non-3Com switch products

SMS + IPS + 3Com Network Director

3Com Network Director (3ND) version 2.5 supports automatic Quarantine with SMS + IPS, in a way similar to the EMS method. However, the significant difference is that 3ND will update Network Access Manager (NAM) with the required Quarantine action so that SMS does not need to act as a RADIUS proxy. 3ND also supports a basic, manual Quarantine function, called "Find and Remove", which is integrated closely with 3Com NAM.

Advantages

- Self-contained solution (SMS not needed as proxy) works with Microsoft Active Directory via the 3Com Network Access Manager
- Provides all Quarantine actions, including removing a device and placing it into another VLAN
- Topology-aware – no need for user to distinguish between edge ports and inter-switch links
- Eases configurability of switches through bulk configuration functionality
- Confirmation mode – users asked to confirm automated actions before turning it fully automatic

Disadvantages

- 3Com-only solution – doesn't support 3rd-party devices

Compatible Products

3Com Switch 4400

3Com Switch 5500

FUNCTIONAL OVERVIEW

General

This section provides a technical overview of how an integrated IPS + SMS + EMS system functions to provide a Quarantine solution.

Placing a device into Quarantine

Once requested by the SMS, the EMS can Quarantine an infected device in any of three different ways, as follows:

> Quarantine via RADA (MAC address) – EMS locates the device and forces a RADA re-authentication on the device's port (this is the fastest mechanism to Quarantine a user or host device).

> Quarantine via VLAN modification – EMS changes the port's VLAN membership by acting directly on the switch.

> Quarantine via disabling a port on a switch – EMS disables the port on the switch, where the infected device is connected.

Removing a device from Quarantine

After the Quarantine action, the EMS sends SMS a trap with the configuration data for the port as it existed prior to quarantining. This "undo" data is used in removing the device from Quarantine. The removal process is the reverse of that used to place the device into Quarantine.

> De-Quarantine via RADA – EMS locates the device and forces a RADA re-authentication on the device's port.

> De-Quarantine from VLAN modification – EMS reconfigures the port back to the previous VLAN configuration.

> De-Quarantine from disconnection – EMS locates the port the device is connected to and enables that port.

Scenario configured in this guide

The following Quarantine scenario uses the RADA method. (The detailed steps of configuration for this scenario are found in the next section of the guide.)

Rules

> Supported network devices: 3Com Switch 4400 / 5500 / 7750*

> Required kit: 1 X IPS (min), 1 X SMS, 1 X RADIUS Server, 1 X EMS

> Required configuration:

- Quarantine VLAN created on all LAN switches
- RADA enabled on Switch 4400 / 5500 / 7750*
- Switches configured to send RADIUS requests to SMS. SMS acts as a proxy between the switch and RADIUS server

*Support for Switch 7750 is planned for late-2006 availability

Expected Quarantine behavior

Devices are automatically moved into the Quarantine network

Quarantine scenario functionality

The diagram and order of system interactions show a scenario deploying a Quarantine solution using an IPS + SMS + EMS and a RADIUS server.

FIGURE 1: Quarantine functionality (IPS + SMS + EMS)

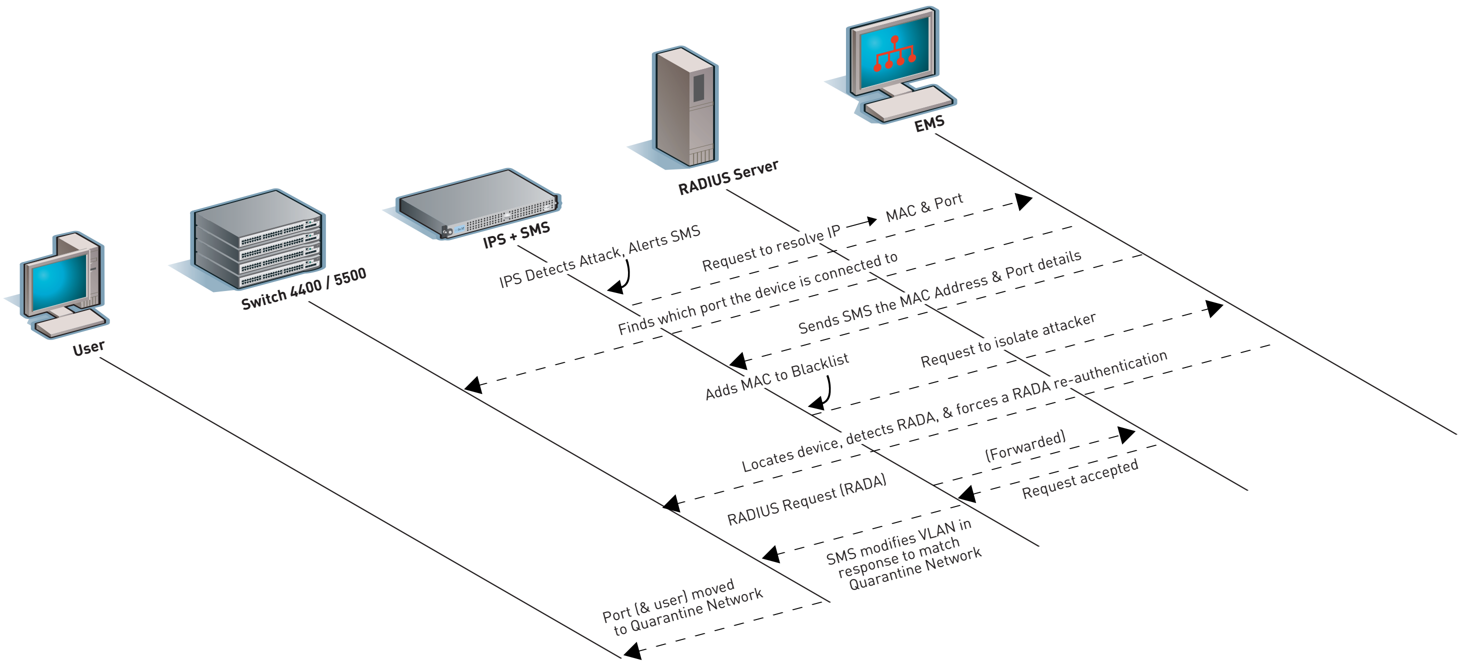
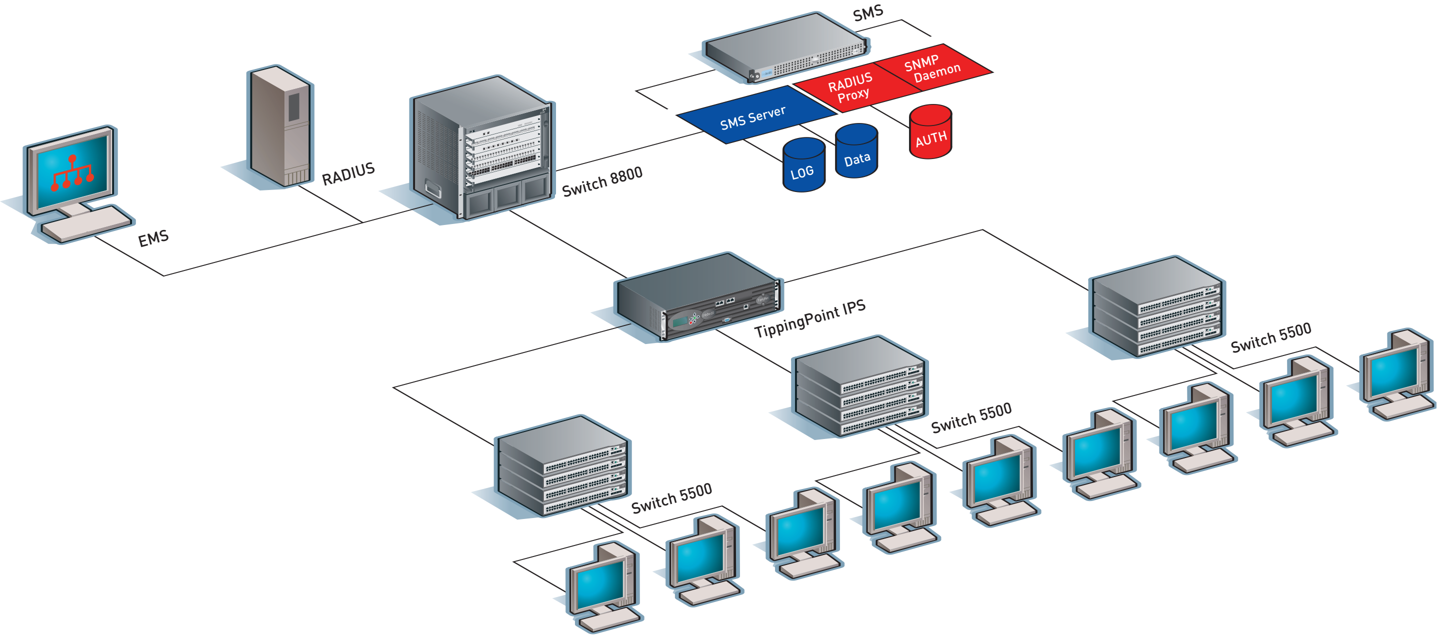

User
Switch 4400 / 5500
IPS + SMS
RADIUS Server
EMS
IPS Detects Attack, Alerts SMS
Request to resolve IP
MAC & Port
Finds which port the device is connected to
Sends SMS the MAC Address & Port details
Adds MAC to Blacklist
Request to isolate attacker
Locates device, detects RADA, & forces a RADA re-authentication
RADIUS Request (RADA)
(Forwarded)
Request accepted
SMS modifies VLAN in response to match Quarantine Network
Port (& user) moved to Quarantine Network

FIGURE 2: Typical network topology



Quarantining using RADA method

1. IPS detects suspicious or undesired activities from a specific client on the network and notifies the SMS of the device's IP address and the suspicious activity.
2. SMS sends a trap that includes the IP address of the target device to the EMS station.
3. The next stage depends on the policy configured in the SMS for the method of quarantining: RADA re-authentication, VLAN isolation, or disabling of the port on the switch. In this scenario, the policy dictates SMS will request EMS use the RADA re-authentication method.
4. The EMS searches for the offending device location and forces the action requested by SMS. EMS searches the devices to find the IP-to-MAC mapping and port location. The EMS sends the MAC address of the infected device to the SMS.
5. The EMS tells the switch to re-authenticate the offending device MAC, i.e., forces a RADA re-authentication on the device.
6. When the infected device re-authenticates, the SMS, acting as a RADIUS server proxy, modifies the RADIUS response using Auto-VLAN to place the infected device into the Quarantine network.
7. The EMS sends the SMS all the data necessary for the SMS to later instruct the EMS to undo the Quarantine; SMS persists the undo data.

De-Quarantining using RADA method

The reverse order of the method that placed the device into Quarantine is followed.

The EMS uses this de-quarantining trap to remove the device from Quarantine using the reverse order of the method that placed the device in Quarantine.

1. The SMS sends a Quarantine release trap to the EMS.
2. The EMS uses the data in the Quarantine release trap to re-authenticate the port.
3. The SMS forwards the RADA re-authentication packets to the switch without modifying the RADIUS response.

STEP-BY-STEP CONFIGURATION GUIDE

This section is a step-by-step configuration guide for RADA-based Quarantine. The steps are proven for the configuration example shown below and at the beginning of the next section, Running Quarantine. The overall configuration time will vary depending on the pre-existing infrastructure. Running Quarantine, to verify the application, will take from 15 minutes to an hour. The configuration is organized into four groupings as follows:

1. Configure 3Com switches for MAC authentication (RADA)
2. Configure Windows IAS/RADIUS server
3. Setup EMS
4. Configure SMS to Quarantine devices

Configuration Components

> RADA-enabled switches (Switch 5500, 4400) (1)

> Server running IAS/RADIUS Server, (Windows 2000 or Windows 2003 Server) (2)

> Workstation for EMS (Windows, Solaris or Linux) (3)

> SMS management appliance, software version 2.2 Build 4409 (4)

> IPS device, running software version 2.2 Build 6493 (4)

> Switch 77xx/8800 used for routing (configuration not shown)

> End station

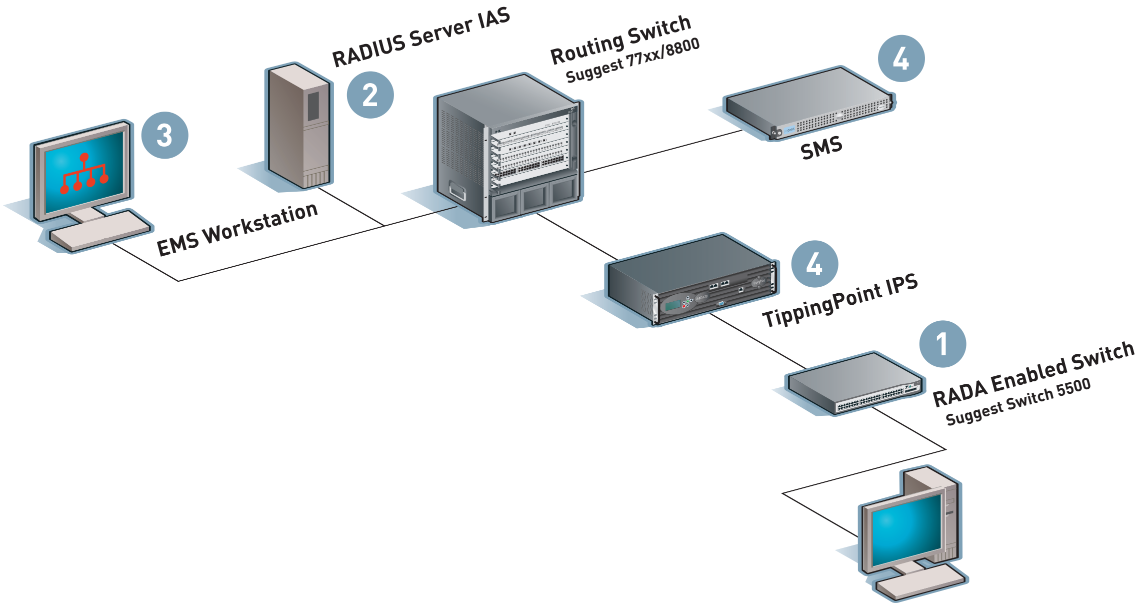
Note

In any field configuration, attention should be paid to product version throughout the configuration. The NMS and Switch 5500 code have the following compatibility requirements:

> 2.2 EMS with 3.01.00 Switch 5500

> 2.3 EMS with 3.02.00 Switch 5500

FIGURE 3: Used configuration



1. CONFIGURE 3COM SWITCHES FOR MAC AUTHENTICATION (RADA)

General

- For this Quarantine solution to work, the RADIUS authentication server configuration on each switch must be pointing at the IP address of the SMS as the RADIUS server.
- For the RADIUS accounting, the switch should point at the actual RADIUS accounting server, i.e., not the IP address of the SMS.

1.1 – Configure MAC authentication (RADA) on the Switch 4400

The detailed installations are made according to the *3Com SuperStack 3 Switch 4400 Getting Started Guide*.

Note

- It is recommended to configure only a single port as a test port. Once the system has been proven to work, repeat the steps and enable security on the remaining ports.

TABLE 1: Switch 4400 Configuration Tasks

Task	Commands	Parameters
1. Connect & Login	Default login: admin	No password (default)
2. Initialize	system control initialize	No parameters
3. Set IP Address	protocol ip interface modify 1 manual	IP address, subnet mask & management VLAN (accept the default of 1)
4. Set Default Gateway	protocol ip route default	IP address of gateway
5. Check RADIUS connectivity	protocol ip ping ipaddr	IP address of (actual) RADIUS server
6. Create needed VLANs	bridge vlan create	VLAN ID & Name
7. Enable RADIUS Authentication with IAS	security radius setup	1. IP address of RADIUS server (the IP address of the SMS, which is acting as a proxy) 2. UDP socket (1812) 3. Ignore secondary RADIUS server – just press CR 4. Shared secret (minimum 8 characters) 5. Ignore accounting server settings – just press CR
8. Enable security	security network access systemMode enable	No parameters
9. Configure ports with RADA	security network access portSecurity	1. List of port(s) - press ? for format options 2. Mode: rada 3. RADIUS failure: maintainSecurity 4. Addresses: 1 5. Unauthorized Action: blockMACAddress 6. VLAN/QoS: RADIUS
10. Enable fixed username mode for RADA	system management snmp set	Repeat set command 3 times: 1. OID: 1.3.6.1.4.1.43.10.22.7.4.0 2. Type: num 3. Value: 2 1. OID: 1.3.6.1.4.1.43.10.22.7.5.0 2. Type: str 3. Value: *username* 1. OID: 1.3.6.1.4.1.43.10.22.7.6.0 2. Type: str 3. Value: *password* **Note: The same username and password need to be configured on the RADIUS server (IAS) and must be allowed access.**

1.2 – Configure MAC authentication (RADA) on the Switch 5500

The detailed installations are according to the *3Com Switch 5500 Family Getting Started Guide*, also using the *3Com Switch 5500 Family Command Reference Guide*.

Notes

- Use 'user@system' format (e.g., admin@system) when logging in at the console to force the switch to use local user accounts (e.g., admin) and not authenticate via RADIUS.
- Use the command *dir* to display system files.
- Switch 5500 Version 3.01.00 supports either RADA or IEEE 802.1X on the same port; Switch 5500 Version 3.02.00 supports both RADA and IEEE 802.1X on the same port.
- It is recommended to configure only a single port as a test port. Once the system has been proven to work, repeat the steps and enable security on the remaining ports.
- To disable RADA on port(s), use the command *undo mac-authentication interface portlist*.
- When in a 'view', you can see the status of that view with the command *display this*.

TABLE 2: 3Com 5500 Switch Configuration Tasks

Task	Commands	Parameters
1. Connect & Login	Default login: admin@system	No password (default)
2. Initialize	1. delete /unreserved 3comoscfg.cfg 2. reboot	 No parameters – need to login again after reboot
3. Enter system mode	system-view	No parameters
4. Set IP Address	1. interface vlan-interface 1 2. ip address ipaddr subnet 3.quit	 IP address Subnet mask
5. Set Default Gateway	ip route-static 0.0.0.0 0 gateway	Default Gateway
6. Check connectivity with IAS	ping ipaddr	RADIUS IP Address
7. Create the necessary VLANs	1. vlan vlan-id 2. description name 3. quit	 VLAN ID & Name
8. Enable MAC Auto-VLAN	private-group-id mode standard	No parameters
9. Create a RADIUS schema (i.e. a group of settings)	1. radius scheme iasScheme 2. primary authentication ipaddr 3. key authentication sharedsecret 4. accounting optional 5. user-name-format without-domain 6. display this (& check configuration displayed) 7. quit	IP Address of RADIUS Server Shared Secret The RADIUS IP address must be the address of the SMS, which acts as RADIUS proxy
10. Create a RADIUS domain & make it the default	1. domain iasDomain 2. scheme radius-scheme iasScheme local 3. display this (& check configuration displayed) 4. quit 5. domain default enable iasDomain	 No parameters
11. Configure MAC-based authentication	1. mac-authentication domain iasDomain 2. mac-authentication authmode username fixed 3. mac-authentication authusername username 4. mac-authentication authpassword password	 The Username & Password for MAC-based Authentication
12. Configure the ports	1. mac-authentication interface portlist	MAC authentication
13. Enable authentication globally	1. mac-authentication	No parameters
14. Exit system mode & save	1. [Ctrl-Z] 2. save	 No parameters

2. CONFIGURE WINDOWS IAS/RADIUS SERVER

Notes

> You need to create an Internet Authentication Service (IAS) Remote Access Policy to direct all RADIUS requests from a 3Com device.

> Correct configuration of this policy is critical because any mismatch in parameters (such as authentication types) will result in the RADIUS request not being processed.

2.1 – Launch IAS

> *Start > All Programs > Administrative Tools > Internet Authentication Service*

2.2 – Create a remote access policy

> Select "Remote Access Policies" from the tree

> Action > New > Remote Access Policy

- Select the new Remote Access Policy from the list in the right-hand pane
- Right-click and select "Properties"
- Click "Edit Profile …"
- Select the "Authentication" tab
- Make sure that 'Encrypted Authentication (CHAP)' and 'Unencrypted Authentication (PAP, SPAP)' are both selected

2.3 – Add the SMS as a client into the IAS RADIUS server

> Select "RADIUS Clients" from the tree

> Action > New > RADIUS Client

> For each SMS in the network, enter the name & IP address

> Click Next

> Select Client-Vendor = "RADIUS Standard", Enter and Confirm the switch's Shared Secret (between the IAS RADIUS server and the SMS as proxy)

> **Do not** click the "Request must contain the Message Authenticator attribute"

> Click Finish

2.4 – Configure Active Directory users and computers

1. Launch Active Directory users and computers

> Start > All Programs > Administrative Tools > Active Directory Users and Computers

2. Create an entry in the Active Directory for the username and password

Note

The username and password must match those configured on the switch in the section, *Step 1. Configure 3Com Switches*.

> Select "Users" from the tree.

> For the RADA User Account:

- Action > New > User
- Enter First Name, Last Name and User Logon Name.
- Enter & confirm password.
- Un-tick the "User must change password at next logon".

3. Enable Dial-in access for RADA user

> Select "Users" from the tree.

> On the list of users in the right-hand pane, double-click on each new User in turn.

> Select the tab "Dial-in"

- Tick the box "Allow access" under "Remote Access Permission".

> Select the tab "Account"

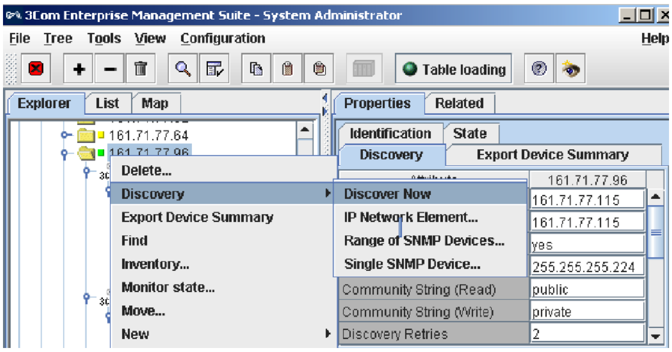
- Tick the box "Store password using reversible encryption" under "Account Options".

4. Set the Network Access permissions for RADA user

3. SET UP EMS

The EMS should be installed according to the *3Com Enterprise Management Suite Getting Started Guide*. Its overall operation is described in the *3Com Enterprise Management Suite User Guide*. The server should be started and a client connected to the server.

FIGURE 4: EMS discovery

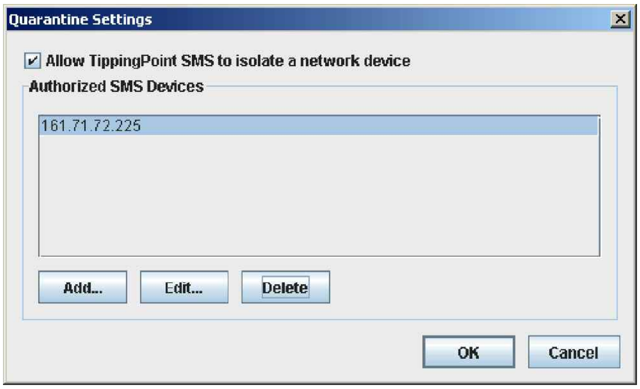


161.71.77.96
161.71.77.115
161.71.77.115
yes
255.255.255.224
Community String (Read) public
Community String (Write) private
Discovery Retries 2

3.1 – Set up EMS to discover switch (figure 4)

1. Right click on Equipment and select New->Equipment Folder
2. Give the folder a name (Tip: it is helpful to name equipment folders after the subnets that it will contain)
3. Select the new folder and click on the Discovery tab in the right pane
4. Enter the IP address range and SNMP options
5. Right click on the new folder and choose Discovery->Discover Now. EMS will discover all SNMP devices within the range specified.
6. Expand the new folder to see all the devices after the discovery report is shown.

FIGURE 5: Switch Quarantine Tab on EMS



☑ Allow TippingPoint SMS to isolate a network device

Authorized SMS Devices

161.71.72.225

3.2 – Set up EMS to allow SMS to Quarantine switch (figure 5)

1. Right click on Equipment near the top level of the tree. Choose Quarantine->Quarantine Settings…
2. Check the box "Allow TippingPoint SMS to isolate a network device"
3. Add the IP Address of the SMS using the Add button.
4. Click OK.

3.3 – Set up the Quarantine parameters

For this step, knowledge of the network's topology is necessary (see explanation below). Take the topology into account when first setting up the network. If the topology is not known, then 3Com Network Director can discover the network and display links between switches.

- For the 4400 family of devices the convention for specifying ports is unit/port (e.g. 1/1)
- For the 5500 and 7750 family of devices the convention is slot/sub-slot/port (e.g. 1/0/1)

For each edge switch in the tree that is part of the Quarantine solution:

1. Expand the device to see the Security folder > Select Security folder.
2. Click on the Quarantine tab (shown in table below).
3. Set Allow Quarantine Actions to *yes*.
4. Enter a port range for Quarantine-enabled Ports.
5. Enter a port range for Switch to Switch Ports. In this case it is better to specify *all* on item 5 and specify the switch-to-switch ports individually.
6. Press *Save all*

TABLE 3: Guide for specifying ports

Quarantine-enabled ports are all the ports that can be quarantined. These ports should be those that are connected to end stations only, and not to other switches or business critical devices. Only ports that appear in this list will be subject to Quarantine actions.

Switch-to-switch ports only connect switches to switches. If a port is specified as "switch-to-switch" it will not be quarantined, even if it also is specified as a Quarantine-enabled port. Switch-to-switch ports also help the 3Com Quarantine feature locate end stations on the network. Any end station seen on a switch-to-switch port will be ignored because all end stations will be seen on switch-to-switch ports if they are sending traffic. Incorrectly specifying switch-to-switch ports will result in incorrect Quarantine operations.

- Specify Quarantine-enabled ports as "all" and switch-to-switch ports as "1/0/1" (where the first port is connected to another switch).
- Ranges can only be specified over ports, not stacks.

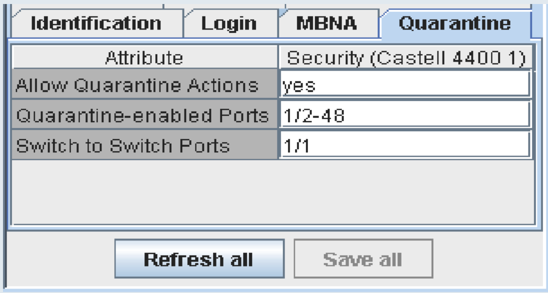
Note:

Commas are used for non-contiguous port ranges; spaces separate units/slots.

Switch 5500/7750
Single Port: 1/0/1
Simple Range: 1/0/1-20
Stack Range: 1/0/1-20 2/0/1-20 3/0/1-20

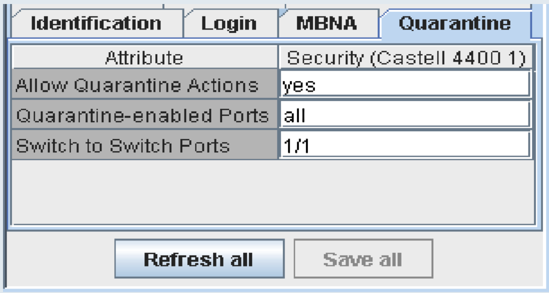
Switch 4400
Single Port: 1/1
Simple Range: 1/1-20
Stack Range: 1/1-20 2/1-20 3/1-20

FIGURE 6: Range of Quarantine-enabled ports (4400)



Attribute	Security (Castell 4400 1)
Allow Quarantine Actions	yes
Quarantine-enabled Ports	1/2-48
Switch to Switch Ports	1/1

FIGURE 7: Specifying all for Quarantine-enabled ports (4400)



Attribute	Security (Castell 4400 1)
Allow Quarantine Actions	yes
Quarantine-enabled Ports	all
Switch to Switch Ports	1/1

4. SET UP SMS TO QUARANTINE DEVICES

Note:

SMS version 2.2.0.4420 was used for the example configuration.

Installations

- Install the IPS device according to the *TippingPoint Hardware Installation and Safety Guide*. Once installed, no special setup or configuration is required for this deployment.
- Install the SMS as described in the *TippingPoint Security Management System Installation and Configuration Guide*. Install the client on the management station. Check the SMS client installation as per the *Security Management System User Guide*.

4.1 – Add an IPS client to the SMS station

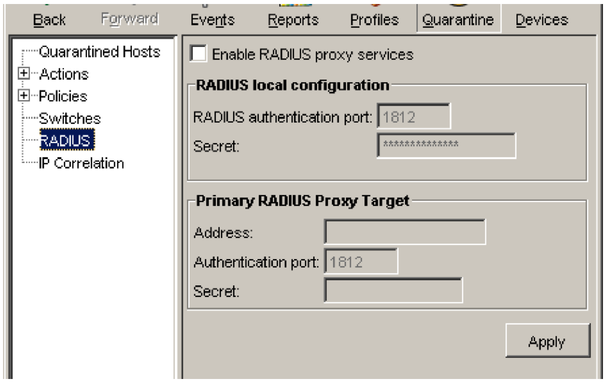
1. Log in as a user to the SMS management station.
2. Click on the Devices icon in the tool bar of SMS.
3. Choose New Device in the bottom right corner.
4. Fill in all the details in the dialog and click Add.

4.2 – Configure SMS as RADIUS proxy

The SMS will be used as a proxy between the switch and the RADIUS server.

1. Click on the Quarantine icon in the SMS tool bar.
2. Select RADIUS in the tree at the left hand side of the client.

FIGURE 8: SMS as RADIUS proxy



□ Enable RADIUS proxy services

RADIUS local configuration

RADIUS authentication port: 1812

Secret: ***************

Primary RADIUS Proxy Target

Address:

Authentication port: 1812

Secret:

3. Click on the Enable RADIUS proxy services check box.
4. Input the same shared secret for the local configuration as is used with the IAS RADIUS server clients.
5. Input the details of the IAS RADIUS server as the Primary RADIUS Target including the shared secret specified in IAS.
6. Click on Apply.

Note

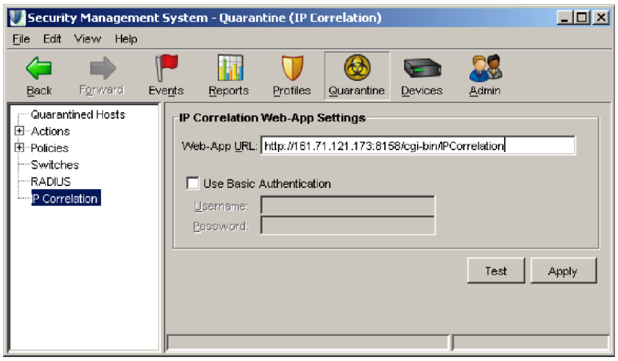
The username and password must match those configured on the switch in the section, *Step 1. Configure 3Com Switches.*

4.3 – Configure the IP correlation on the SMS

The IP correlation tells the SMS where to find the IP-to-MAC address mapping. In this case the EMS will take care of this function.

1. Select IP Correlation in the tree at the left hand side of the client.
2. Input **http://<EMS SERVER IP ADDRESS>:8158/cgi-bin/IPCorrelation** as the Web-App URL. Replace <EMS SERVER IP ADDRESS> with the IP address of the EMS Server (or the server that will be the EMS server if EMS is not yet set up).
3. Click on Apply

FIGURE 9: IP correlation



Security Management System - Quarantine (IP Correlation)

IP Correlation Web-App Settings

Web-App URL: http://161.71.121.173:8158/cgi-bin/IPCorrelation

□ Use Basic Authentication

Username:

Password:

4.4 – Configure SMS actions

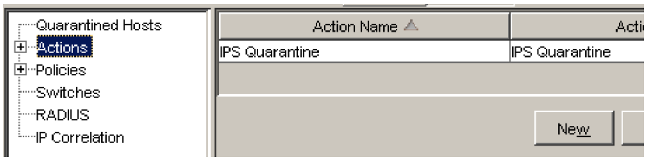
Note

This guide describes configuration and settings for the RADA re-authentication deployment mode only. However, SMS can initiate other modes of Quarantine, such as Quarantine via VLAN isolation and switch disconnection.

Setting an action tells the SMS what to do when the misuse is reported. In this case the action will be to send a trap to the EMS station.

1. Select Actions in the tree at the left hand side of the client.
2. Click on New.

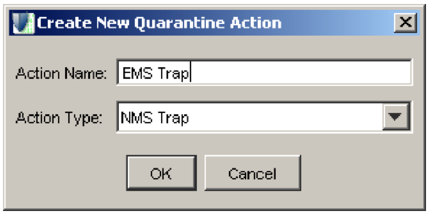
FIGURE 10: Open SMS action



Action Name	Acti
IPS Quarantine	IPS Quarantine

3. Give the new action a name (here given an EMS Trap) and choose NMS Trap from the drop down list
4. Click on OK

FIGURE 11: Create new Quarantine action



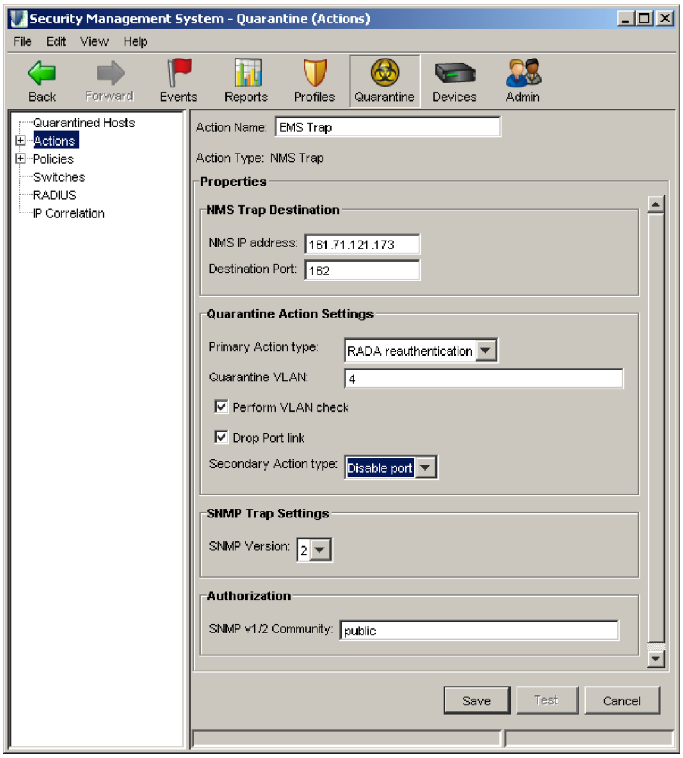
Create New Quarantine Action

Action Name: EMS Trap

Action Type: NMS Trap

5. Set the NMS IP address to be the EMS Server IP address.
6. Set the Primary Action Type to RADA-re-authentication
7. Set the Quarantine VLAN to be the VLAN ID of the VLAN that was previously chosen to be the Quarantine VLAN.
8. Check the Perform VLAN check and the Drop Port link options.
9. Choose Disable Port as the Secondary Action type. This setting tells the EMS to go ahead and disable the port if the VLAN quarantining fails.
10. Click Save.

FIGURE 12: Action item settings



Action Name: EMS Trap

Action Type: NMS Trap

Properties

NMS Trap Destination

NMS IP address: 161.71.121.173

Destination Port: 162

Quarantine Action Settings

Primary Action type: RADA reauthentication

Quarantine VLAN: 4

☑ Perform VLAN check

☑ Drop Port link

Secondary Action type: Disable port

SNMP Trap Settings

SNMP Version: 2

Authorization

SNMP v1/2 Community: public

To change any trap properties, return to this tree item.

4.5 – Configure SMS policies

1. Select Policies in the tree menu at the left.
2. Give the policy a name at the top of the screen next to Policy Name.
3. Select the Default Segment in the Segments and Signatures tab.
4. Find a suitable filter in the available filters list. Using an Instant Messenger login or Ping is recommended (2467, 2519, 2564 and 0079).
5. Add the filter to Selected list by clicking on the > button.
6. Choose the IP Addresses tab.
7. Add all of the IP Addresses that SMS should be able to Quarantine and any IP Addresses not to Quarantine.
8. Choose the Actions tab.
9. Click on EMS Trap and Click on Add.
10. Click on Create to finish.

TABLE 4: Switch 5500 configuration output

```
#
 private-group-id mode standard
#...
MAC-authentication
MAC-authentication domain sms-proxy
MAC-authentication authmode usernamefixed
MAC-authentication authusername testuser
MAC-authentication authpassword testpass
#
radius scheme system
radius scheme sms-proxy
 server-type extended
 primary authentication 192.168.1.12
 primary accounting 202.1.1.146
 accounting optional
 key authentication secret
 key accounting secret
 user-name-format without-domain
 nas-ip 192.168.1.250
#
domain sms-proxy
scheme radius-scheme sms-proxy
domain system
#...
vlan1
Igmp-snooping enable
#
vlan 20
#
vlan 50
#
interface Vlan-interface1
 ip address 192.168.1.250 255.255.255.0
#
interface Vlan-interface50
 ip address 192.168.50.1 255.255.255.0
#...
interface Ethernet1/0/19
stp edged-port enable
broadcast-suppression PPS 3000
priority trust
port access vlan 50
undo jumboframe enable
MAC-authentication
apply qos-profile default
#...
ip route-static 0.0.0.0 0.0.0.0 192.168.1.1 preference 60
# ...
```

QUARANTINE EXAMPLE

This section describes the set-up (A) and verification (B) for a specific Quarantine scenario. The configuration screens and verification outputs are shown below.

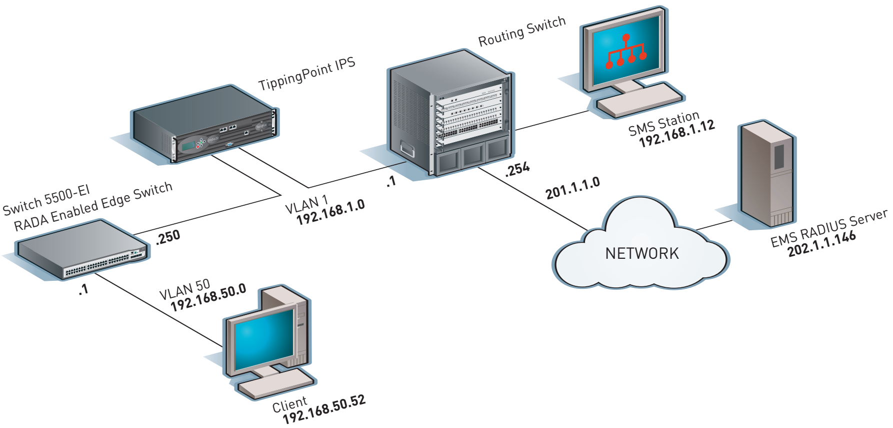
SET UP TOPOLOGY

The configuration is organized into three step groupings, as follows:

1. Configure Switch 5500-EI for MAC authentication (RADA)
2. Configure SMS to Quarantine devices
3. Configure EMS

The following topology was used.

FIGURE 13: Network Topology



1. Switch 5500-EI configuration

For this scenario, the Switch 5500-EI is at the edge of the network with three VLANs, configured as follows:

- VLAN 1 with IP address 192.168.1.250/24 – connects to the core of the network.
- VLAN 50 with IP address 192.168.50.1/24 – clients connect to this network.
- VLAN 20 no IP address – Quarantined devices sent to this VLAN.
- RADA (MAC Authentication) is enabled on port Ethernet 1/0/19.
- RADIUS server configured to be the SMS station IP address 192.168.1.12.
- Client connects to port Ethernet 1/0/19 on 5500-EI switch and is placed on VLAN 50.

Note

The configuration example uses a fixed username and password for MAC authentication.

2. CLI output after RADA is configured on the Switch 5500-EI

The following table summarizes the output from the above switch configuration. Some output is substituted with "…"; the pertinent user commands for the example are shown in bold face.

3. SMS station configuration

Note:

SMS version 2.2.0.4420 was used for the example configuration.

The SMS station requires the following configuration:

- Set up SMS Actions menu
- Set up SMS Policy Summary tree menu
- Set up SMS RADIUS Server Configuration menu
- Set up SMS IP Correlation menu

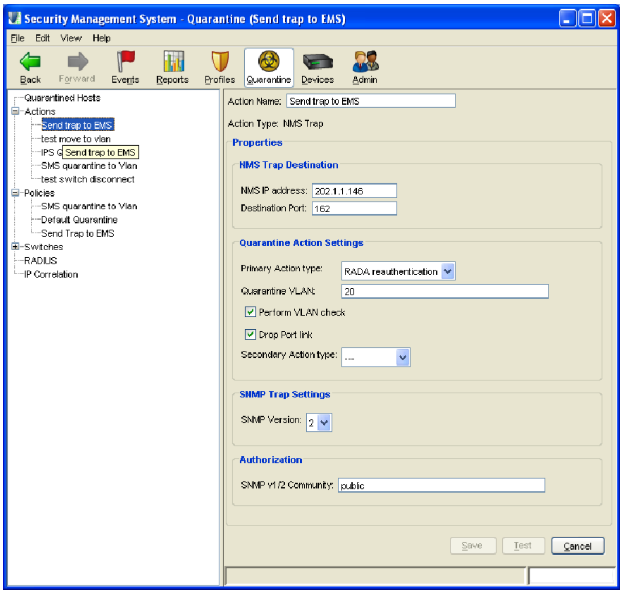
3.1 – Set up the SMS Actions menu

The Actions menu defines the EMS IP address, SNMP values and the action to be taken. In this example the action will be triggered when a UDP scan is encountered. The action will tell the EMS/NMS station to force a RADA re-authentication and place the quarantined device on VLAN 20. If the RADA action fails, the menu offers the choice of a secondary Action type, for example, to disable the port.

This is the Actions tab on the Policies tree with an action to send a trap to the EMS station.

Input the IP address and the other criteria in the appropriate lines. The following example adheres to the Switch 5500-EI Used Configuration shown in the preceding network diagram.

FIGURE 14: Actions menu



Security Management System - Quarantine (Send trap to EMS)

Action Name: Send trap to EMS

Action Type: NMS Trap

Properties

NMS Trap Destination

NMS IP address: 202.1.1.146

Destination Port: 162

Quarantine Action Settings

Primary Action type: RADA reauthentication

Quarantine VLAN: 20

☑ Perform VLAN check

☑ Drop Port link

Secondary Action type: ---

SNMP Trap Settings

SNMP Version: 2

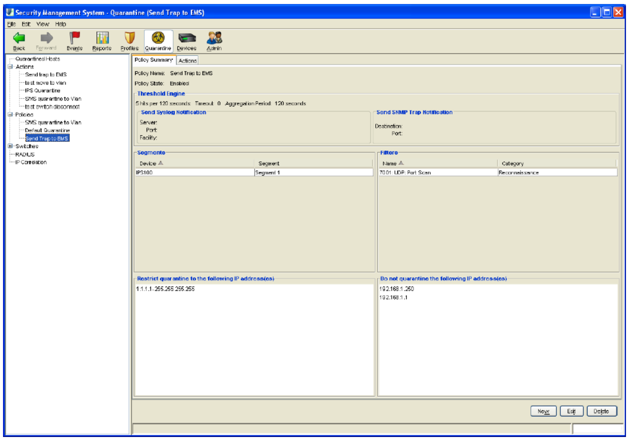
Authorization

SNMP v1/2 Community: public

3.2 – Set up SMS Policy Summary tree menu

The following screen shows the Policy Summary tab. A filter to identify UDP port scan traffic is modified to permit and notify the SMS station. The action taken is to send a trap to the EMS station. The IP addresses not to Quarantine are 192.168.1.250 and 192.168.1.1.

FIGURE 15: Policy Summary tab



Policy Name: Send Trap to EMS

Policy State: Enabled

Threshold Engine

5 hits per 120 seconds Timeout: 0 Aggregation Period: 120 seconds

Send Syslog Notification

Server:
Port:
Facility:

Send SNMP Trap Notification

Destination:
Port:

Segments

Device	Segment
IPS100	Segment 1

Filters

Name	Category
7001: UDP: Port Scan	Reconnaissance

Restrict quarantine to the following IP address(es)

1.1.1.1-255.255.255.255

Do not quarantine the following IP address(es)

192.168.1.250
192.168.1.1

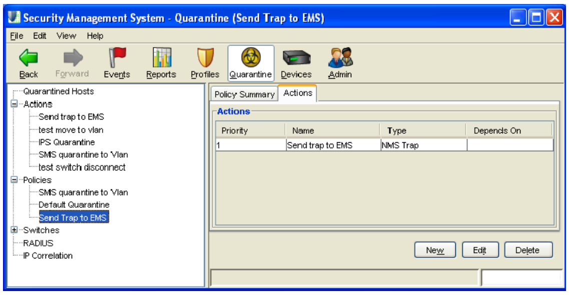
Under the Profiles symbol on the main menu, the filters setting can be modified to:

- permit and notify
- block and notify
- disable filters

The UDP scan filter served as the undesired network traffic to trigger the Quarantine process in this example. The UDP scan filter is disabled by default and must be enabled and set to "permit" and "notify" for this example to work. On the main menu under Profiles, use the following path to find the UDP scan filter:

Profiles>Default>Application Protection>Reconnaissance>Scans/Sweeps

FIGURE 16: Actions tab on Policies tree



Actions

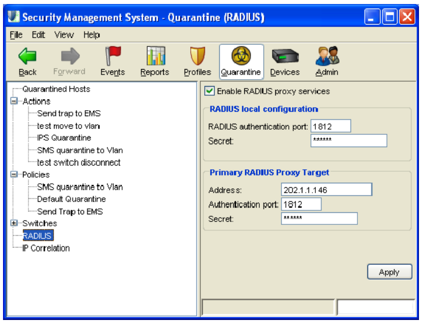
Priority	Name	Type	Depends On
1	Send trap to EMS	NMS Trap	

The Actions tab on the Policies tree shows an action to send a trap to the EMS station.

3.3 – Set up SMS RADIUS server configuration menu

Following is the RADIUS Set-Up menu where the SMS is told where to send RADIUS requests. The SMS is acting as a RADIUS proxy. Fill in the three Primary RADIUS proxy target fields.

FIGURE 17: RADIUS set-up menu



☑ Enable RADIUS proxy services

RADIUS local configuration

RADIUS authentication port: 1812
Secret: ******

Primary RADIUS Proxy Target

Address: 202.1.1.146
Authentication port: 1812
Secret: ******

Note

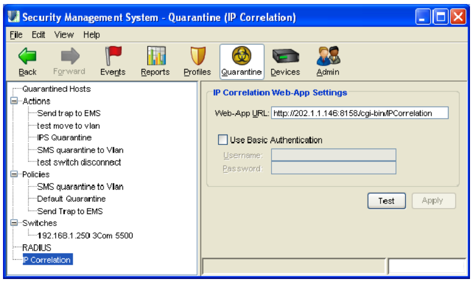
The username and password must match those configured on the switch in the section, *Step 1: Configure 3Com Switches.*

3.4 – Set up SMS IP correlation menu

The IP correlation menu tells the SMS where to go to resolve the IP-to-MAC address. The URL needs to point to the EMS station

Input **http://202.1.1.146:8158/cgi-bin/IPCorrelation**

FIGURE 18: IP correlation menu



IP Correlation Web-App Settings

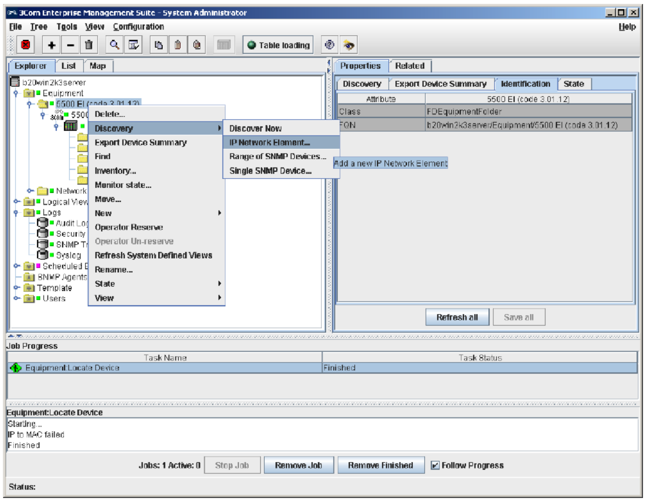
Web-App URL: http://202.1.1.146:8158/cgi-bin/IPCorrelation

☐ Use Basic Authentication
Username:
Password:

4. EMS station configuration

4.1 – Set up EMS to discover Switch 5500-EI:

FIGURE 19: Switch 5500-EI discovery



Attribute	5500 EI (code 3.01.12)
Class	FDEquipmentFolder
FQN	b20win2k3server/Equipment/5500 EI (code 3.01.12)

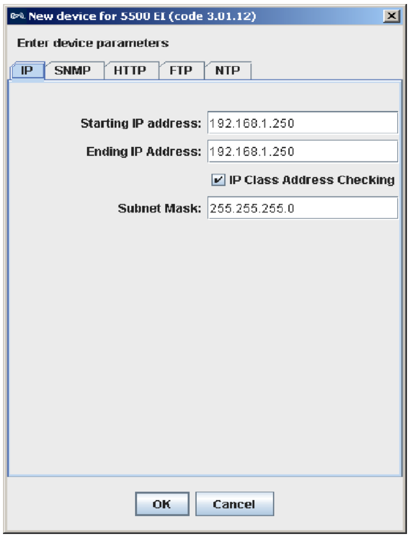
Task Name	Task Status
Equipment:Locate Device	Finished

Equipment:Locate Device

```
Starting...
IP to MAC failed
Finished
```

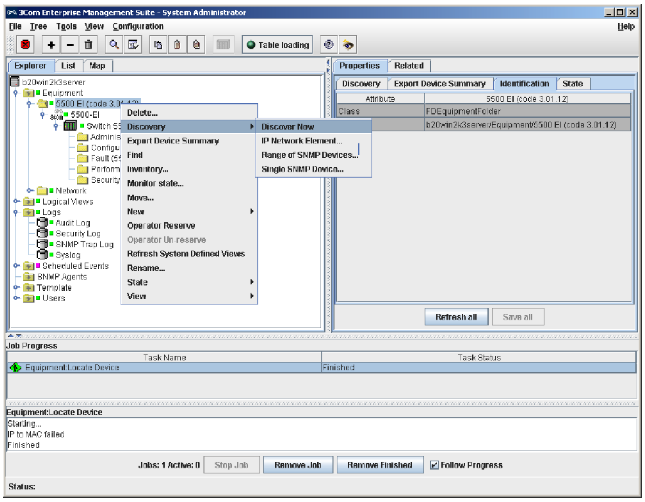
Jobs: 1 Active: 0 ☑ Follow Progress

FIGURE 20: Enter device parameters



Starting IP address: 192.168.1.250
Ending IP Address: 192.168.1.250
☑ IP Class Address Checking
Subnet Mask: 255.255.255.0

FIGURE 21: Discover device



Attribute	5500 EI (code 3.01.12)
Class	FDEquipmentFolder
	b20win2k3server/Equipment/5500 EI (code 3.01.12)

Task Name	Task Status
Equipment:Locate Device	Finished

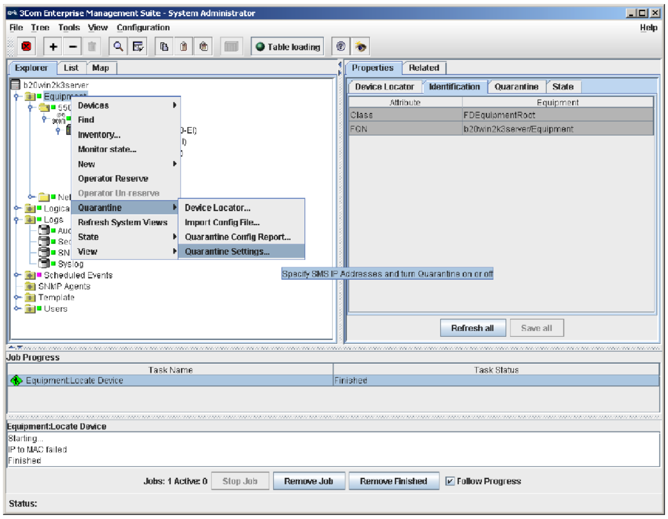
Equipment:Locate Device

```
Starting...
IP to MAC failed
Finished
```

Jobs: 1 Active: 0 ☑ Follow Progress

4.2 – Set up EMS to allow SMS to isolate a network device

FIGURE 22: Configure Quarantine settings



Attribute	Equipment
Class	FDEquipmentRoot
FQN	b20win2k3server/Equipment

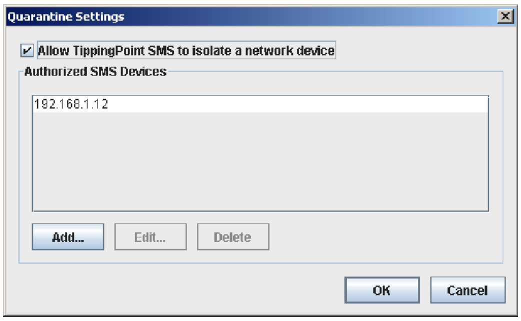
Task Name	Task Status
Equipment:Locate Device	Finished

Equipment:Locate Device

```
Starting...
IP to MAC failed
Finished
```

Jobs: 1 Active: 0 ☑ Follow Progress

FIGURE 23: Specify IP address



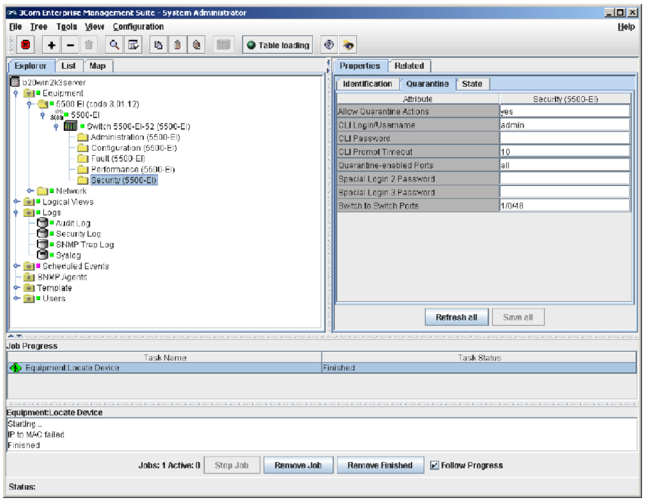
☑ Allow TippingPoint SMS to isolate a network device

Authorized SMS Devices

192.168.1.12

4.3 – Set up the Switch 5500-EI Quarantine tab under the security folder on EMS

FIGURE 24: Configure Quarantine tab



Attribute	Security (5500-EI)
Allow Quarantine Actions	yes
CLI Login/Username	admin
CLI Password	
CLI Prompt Timeout	10
Quarantine-enabled Ports	all
Special Login 2 Password	
Special Login 3 Password	
Switch to Switch Ports	1/0/48

Job Progress

Task Name	Task Status
Equipment:Locate Device	Finished

Equipment:Locate Device

```
Starting...
IP to MAC failed
Finished
```

Jobs: 1 Active: 0

☑ Follow Progress

VERIFY QUARANTINE EXAMPLE

There are five steps to verify Quarantine in this example:

1. The client connects to switch and gets authenticated to RADIUS server.
2. The client starts a UDP port scan; the IPS detects the UDP port scan and sends an alert message to the SMS station.
3. The SMS station sends a Quarantine request trap to the EMS station.
4. The EMS station initiates a RADA re-authentication on the client.
5. The SMS station intercepts the RADA re-authentication and modifies the RADIUS packet to VLAN 20. Client is Quarantined.

1. Client connects to RADA-enabled Switch 5500

The client connects to the Switch 5500. Check to ensure the client gets authenticated on the RADIUS server. Next, check to verify client can connect to the network using port Ethernet 1/0/19 on the Switch 5500-EI, is authenticated via RADA and is granted access and put on VLAN 50.

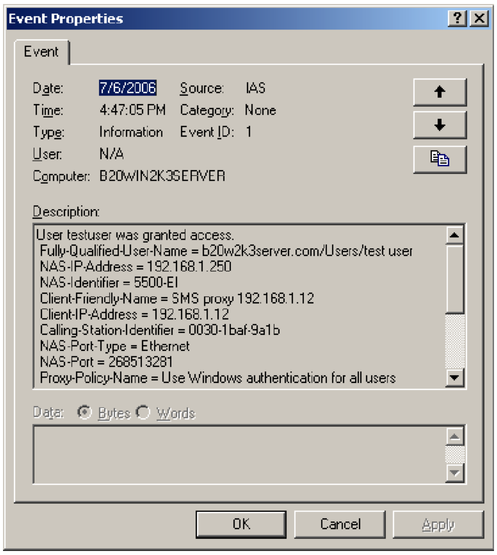
1.1 – On the IAS, view the Event Viewer log.

Verify the client can connect and authenticate to the RADIUS server.

TABLE 5: Client entry verified

```
<5500-EI>display mac-authentication int e1/0/19
Ethernet1/0/19 is link-up
 MAC address authentication is Enabled
 Authenticate success: 1, failed: 0
 Current online user number is 1
    MAC ADDR        Authenticate state              AuthIndex
    0030-1baf-ddc2  MAC_AUTHENTICATOR_SUCCESS       4
<5500-EI>

<5500-EI>display vlan
 The following VLANs exist:
 1(default), 20, 50

<5500-EI>display vlan 50
 VLAN ID: 50
 VLAN Type: static
 Route Interface: configured
 IP Address: 192.168.50.1
 Subnet Mask: 255.255.255.0
 Description: VLAN 0050
 Tagged Ports: none
 Untagged Ports:
    Ethernet1/0/19

<5500-EI>display vlan 20
 VLAN ID: 20
 VLAN Type: static
 Route Interface: not configured
 Description: VLAN 0020
 Tagged Ports: none
 Untagged Ports: none
<5500-EI>display ip interface brief

Interface         IP Address       Physical     Protocol
Aux1/0/0          unassigned       up           down
Vlan-interface1   192.168.1.250    up           up
Vlan-interface50  192.168.50.1     up           up
```

FIGURE 25: Verify client access



Event Properties

Event

Date: 7/6/2006 Source: IAS
Time: 4:47:05 PM Category: None
Type: Information Event ID: 1
User: N/A
Computer: B20WIN2K3SERVER

Description:

User testuser was granted access.
Fully-Qualified-User-Name = b20w2k3server.com/Users/test user
NAS-IP-Address = 192.168.1.250
NAS-Identifier = 5500-EI
Client-Friendly-Name = SMS proxy 192.168.1.12
Client-IP-Address = 192.168.1.12
Calling-Station-Identifier = 0030-1baf-9a1b
NAS-Port-Type = Ethernet
NAS-Port = 268513281
Proxy-Policy-Name = Use Windows authentication for all users

Data: ● Bytes ○ Words

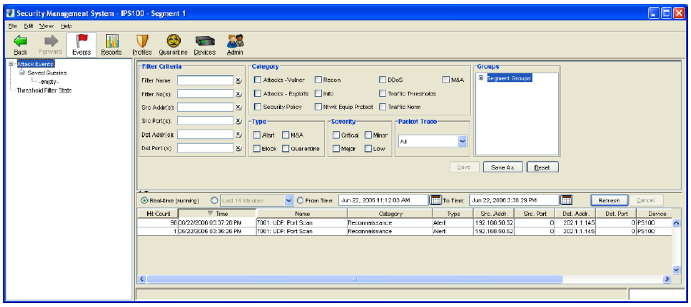
1.2 – View client access to network on VLAN 50.

Open a CLI and verify that the client enters the network on VLAN 50. The commands and results are as follows (pertinent results in bold face):

2. Client starts UDP port scan. The IPS detects the scan and sends an alert to the SMS station.

View from the Events page on the SMS station.

FIGURE 26: Port scan detection



Security Management System - IPS100 - Segment 1

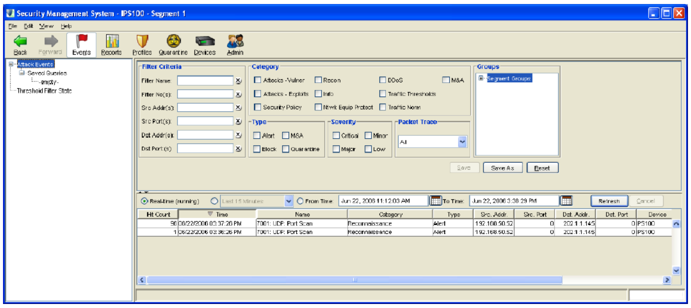
● Real-time (running) ○ Last 15 Minutes ○ From Time: Jun 22, 2006 11:12:03 AM To Time: Jun 22, 2006 3:38:29 PM

Hit Count	Time	Name	Category	Type	Src. Addr.	Src. Port	Dst. Addr.	Dst. Port	Device
96	06/22/2006 03:37:26 PM	7001: UDP: Port Scan	Reconnaissance	Alert	192.168.50.52	0	202.1.1.145	0	IPS100
1	06/22/2006 03:36:26 PM	7001: UDP: Port Scan	Reconnaissance	Alert	192.168.50.52	0	202.1.1.145	0	IPS100

3. SMS sends a Quarantine trap to the EMS station.

At the EMS station, view the EMS SNMP trap log events.

FIGURE 27: Quarantine trap log events



Security Management System - IPS100 - Segment 1

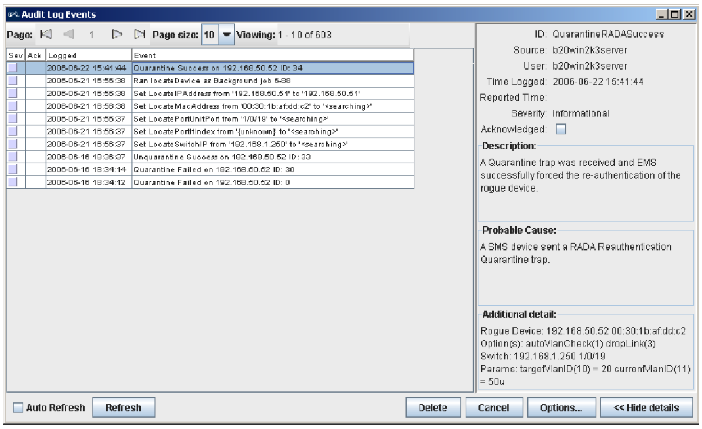
● Real-time (running) ○ Last 15 Minutes ○ From Time: Jun 22, 2006 11:12:03 AM To Time: Jun 22, 2006 3:38:29 PM

Hit Count	Time	Name	Category	Type	Src. Addr.	Src. Port	Dst. Addr.	Dst. Port	Device
96	06/22/2006 03:37:26 PM	7001: UDP: Port Scan	Reconnaissance	Alert	192.168.50.52	0	202.1.1.145	0	IPS100
1	06/22/2006 03:36:26 PM	7001: UDP: Port Scan	Reconnaissance	Alert	192.168.50.52	0	202.1.1.145	0	IPS100

4. The EMS station initiates a RADA re-authentication on the device.

View the EMS Audit log events pages.

FIGURE 28: Quarantine success log



Sev	Ack	Logged	Event
□		2006-06-22 15:41:44	Quarantine Success on 192.168.50.52 ID: 34
□		2006-06-21 16:55:38	Ran locateDevice as Background job 6-88
□		2006-06-21 16:55:38	Set LocateIPAddress from '192.168.50.51' to '192.168.50.51'
□		2006-06-21 16:55:38	Set LocateMacAddress from '00:30:1b:af:dd:c2' to '<searching>'
□		2006-06-21 16:55:37	Set LocatePortUnitPort from '1/0/19' to '<searching>'
□		2006-06-21 16:55:37	Set LocatePortIfIndex from '{unknown}' to '<searching>'
□		2006-06-21 16:55:37	Set LocateSwitchIP from '192.168.1.250' to '<searching>'
□		2006-06-16 18:35:37	Unquarantine Success on 192.168.50.52 ID: 33
□		2006-06-16 18:34:14	Quarantine Failed on 192.168.50.52 ID: 30
□		2006-06-16 18:34:12	Quarantine Failed on 192.168.50.52 ID: 0

ID: QuarantineRADASuccess
Source: b20win2k3server
User: b20win2k3server
Time Logged: 2006-06-22 15:41:44
Reported Time:
Severity: informational
Acknowledged: □

Description:
A Quarantine trap was received and EMS successfully forced the re-authentication of the rogue device.

Probable Cause:
A SMS device sent a RADA Reauthentication Quarantine trap.

Additional detail:
Rogue Device: 192.168.50.52 00:30:1b:af:dd:c2
Option(s): autoVlanCheck(1) dropLink(3)
Switch: 192.168.1.250 1/0/19
Params: targetVlanID(10) = 20 currentVlanID(11) = 50u

5. SMS intercepts RADA re-authentication, changes VLAN ID in RADIUS packet to VLAN 20.

In the CLI, check that Switch 5500, port Ethernet 1/0/19, is now placed under the Quarantine network, VLAN 20. Following are the commands and key results (shown in boldface):

TABLE 6: Quarantine verified

```
<5500-EI>display vlan
 The following VLANs exist:
 1(default), 20, 50

<5500-EI>display vlan 50
 VLAN ID: 50
 VLAN Type: static
 Route Interface: configured
 IP Address: 192.168.50.1
 Subnet Mask: 255.255.255.0
 Description: VLAN 0050
 Tagged Ports: none
 Untagged Ports: none

<5500-EI>display vlan 20
 VLAN ID: 20
 VLAN Type: static
 Route Interface: not configured
 Description: VLAN 0020
 Tagged Ports: none
 Untagged Ports:
    Ethernet1/0/19

<5500-EI>display ip interface brief
Interface           IP Address       Physical       Protocol
Aux1/0/0            unassigned       up             down
Vlan-interface1     192.168.1.250    up             up
Vlan-interface50    192.168.50.1     down           down
```

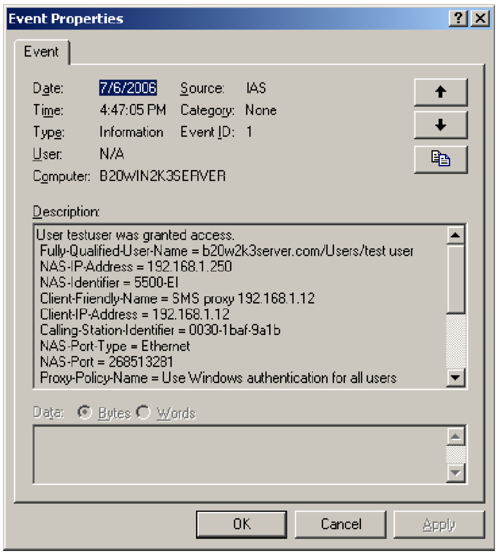
TROUBLESHOOTING

The following are some tips for troubleshooting the main sub-systems used in the RADA Quarantine mode: the RADIUS server, IPS, SMS and EMS.

RADIUS SERVER

- > Check the RADIUS server to ensure RADA authentication is working and the device is authenticated.
- > For IAS, under Windows 2003 server, check under Start > Administrative Tools > Event Viewer > System for a log message confirming the user has been granted access.
- > If no RADA requests are reaching the Radius server then check the Switch 5500 Radius configuration.
- > When using a fixed username and password, make sure the same username and password exist on the RADIUS server, which is case sensitive.
- > When using the MAC address as the username and password, ensure that the username and password on the RADIUS server exist. In the case of the Switch 5500, the username and password are in the form xx-xx-xx-xx-xx-xx all lower case.

FIGURE 29: RADIUS server check



Date: 7/6/2006 Source: IAS
Time: 4:47:05 PM Category: None
Type: Information Event ID: 1
User: N/A
Computer: B20WIN2K3SERVER

Description:

```
User testuser was granted access.
 Fully-Qualified-User-Name = b20w2k3server.com/Users/test user
 NAS-IP-Address = 192.168.1.250
 NAS-Identifier = 5500-EI
 Client-Friendly-Name = SMS proxy 192.168.1.12
 Client-IP-Address = 192.168.1.12
 Calling-Station-Identifier = 0030-1baf-9a1b
 NAS-Port-Type = Ethernet
 NAS-Port = 268513281
 Proxy-Policy-Name = Use Windows authentication for all users
```

Data: ● Bytes ○ Words

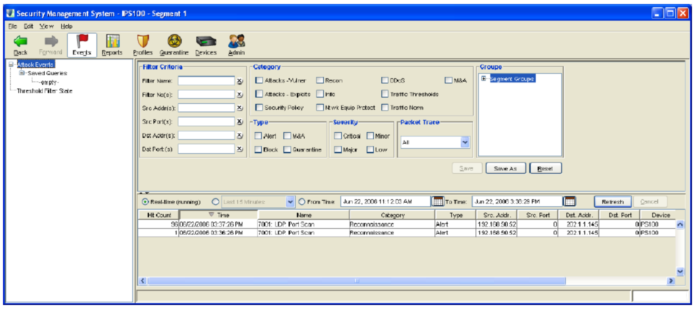
SMS STATION

- > Check the SMS Events page.

Here you should see the event received that causes the SMS to trigger the action configured for the specific attack. If the event is not showing up in the Events page, then the IPS is not notifying the SMS, the filter is disabled on the IPS, or the IPS is not recognizing the traffic pattern.

- > Under Profiles on the SMS, check the filter actions. On the SMS, ensure the filter is enabled and set to Notify. If you modify the filter, you need to redistribute the filter back to the IPS.

FIGURE 30: Attack Events

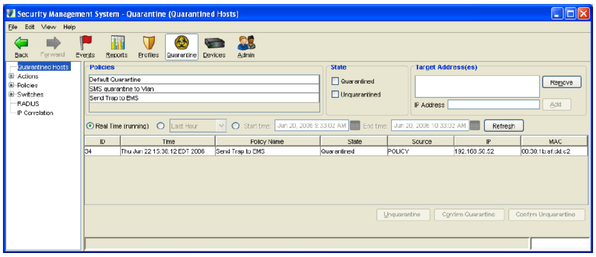


○ Real-time (running) ○ Last 15 Minutes ○ From Time Jun 22, 2006 11:12:03 AM To Time: Jun 22, 2006 3:36:29 PM

Hit Count	Time	Name	Category	Type	Src. Addr.	Src. Port	Dst. Addr.	Dst. Port	Device
96	06/22/2006 03:37:26 PM	7001: UDP Port Scan	Reconnaissance	Alert	192.168.50.52	0	202.1.1.145	0	IPS100
1	06/22/2006 03:36:26 PM	7001: UDP Port Scan	Reconnaissance	Alert	192.168.50.52	0	202.1.1.145	0	IPS100

- > Check SMS Quarantined Hosts to see the Quarantine request and status.

FIGURE 31: SMS Quarantined hosts



Policies: Default Quarantine; SMS quarantine to Vlan; Send Trap to EMS

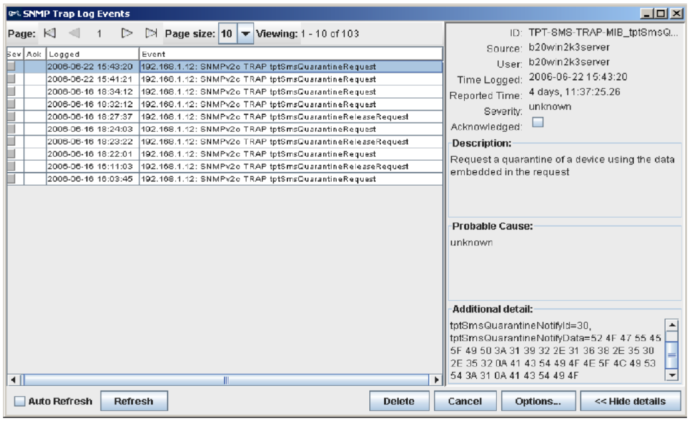
● Real Time (running) ○ Last Hour ○ Start time: Jun 20, 2006 9:33:02 AM End time: Jun 20, 2006 10:33:02 AM

ID	Time	Policy Name	State	Source	IP	MAC
34	Thu Jun 22 15:36:12 EDT 2006	Send Trap to EMS	Quarantined	POLICY	192.168.50.52	00:30:1b:af:dd:c2

EMS STATION

> In the EMS System Administrator window, go to Logs > SNMP Trap Log > View to see SNMP traps the SMS station sent to the EMS station, for Requests and Release Requests.

FIGURE 32: SNMP Trap Log Events



SNMP Trap Log Events

Page: 1 Page size: 10 Viewing: 1 - 10 of 103

Sev	Ack	Logged	Event
□		2006-06-22 15:43:20	192.168.1.12: SNMPv2c TRAP tptSmsQuarantineRequest
□		2006-06-22 15:41:21	192.168.1.12: SNMPv2c TRAP tptSmsQuarantineRequest
□		2006-06-16 18:34:12	192.168.1.12: SNMPv2c TRAP tptSmsQuarantineRequest
□		2006-06-16 18:32:12	192.168.1.12: SNMPv2c TRAP tptSmsQuarantineRequest
□		2006-06-16 18:27:37	192.168.1.12: SNMPv2c TRAP tptSmsQuarantineReleaseRequest
□		2006-06-16 18:24:03	192.168.1.12: SNMPv2c TRAP tptSmsQuarantineRequest
□		2006-06-16 18:23:22	192.168.1.12: SNMPv2c TRAP tptSmsQuarantineReleaseRequest
□		2006-06-16 18:22:01	192.168.1.12: SNMPv2c TRAP tptSmsQuarantineRequest
□		2006-06-16 16:11:03	192.168.1.12: SNMPv2c TRAP tptSmsQuarantineReleaseRequest
□		2006-06-16 16:03:45	192.168.1.12: SNMPv2c TRAP tptSmsQuarantineRequest

ID: TPT-SMS-TRAP-MIB_tptSmsQ...
Source: b20win2k3server
User: b20win2k3server
Time Logged: 2006-06-22 15:43:20
Reported Time: 4 days, 11:37:25.26
Severity: unknown
Acknowledged: □

Description:
Request a quarantine of a device using the data embedded in the request

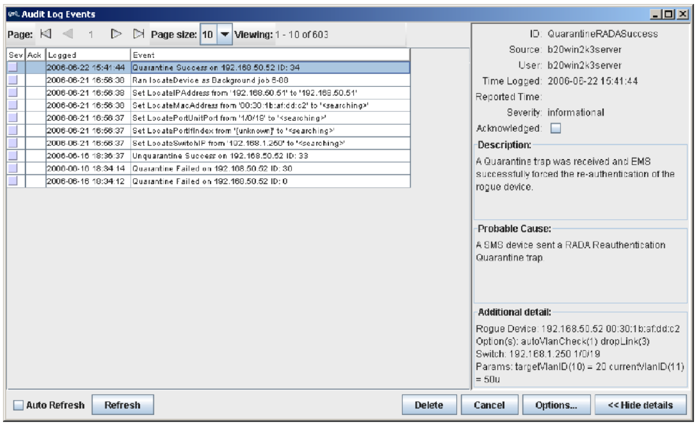
Probable Cause:
unknown

Additional detail:
tptSmsQuarantineNotifyId=30,
tptSmsQuarantineNotifyData=52 4F 47 55 45 5F 49 50 3A 31 39 32 2E 31 36 38 2E 35 30 2E 35 32 0A 41 43 54 49 4F 4E 5F 4C 49 53 54 3A 31 0A 41 43 54 49 4F

□ Auto Refresh

> Also check Logs > Audit Log > View on the EMS for a Quarantine Success or Quarantine Failed messages (and reason).

FIGURE 33: Audit Log Events



Audit Log Events

Page: 1 Page size: 10 Viewing: 1 - 10 of 603

Sev	Ack	Logged	Event
□		2006-06-22 15:41:44	Quarantine Success on 192.168.50.52 ID: 34
□		2006-06-21 16:56:38	Ran locateDevice as Background job 6-68
□		2006-06-21 16:56:38	Set LocateIPAddress from '192.168.50.51' to '192.168.50.51'
□		2006-06-21 16:56:38	Set LocateMacAddress from '00:30:1b:af:dd:c2' to '<searching>'
□		2006-06-21 16:56:37	Set LocatePortUnitPort from '1/0/18' to '<searching>'
□		2006-06-21 16:56:37	Set LocatePortIfIndex from '{unknown}' to '<searching>'
□		2006-06-21 16:56:37	Set LocateSwitchIP from '192.168.1.250' to '<searching>'
□		2006-06-16 18:36:37	Unquarantine Success on 192.168.50.52 ID: 33
□		2006-06-16 18:34:14	Quarantine Failed on 192.168.50.52 ID: 30
□		2006-06-16 18:34:12	Quarantine Failed on 192.168.50.52 ID: 0

ID: QuarantineRADASuccess
Source: b20win2k3server
User: b20win2k3server
Time Logged: 2006-06-22 15:41:44
Reported Time:
Severity: informational
Acknowledged: □

Description:
A Quarantine trap was received and EMS successfully forced the re-authentication of the rogue device.

Probable Cause:
A SMS device sent a RADA Reauthentication Quarantine trap.

Additional detail:
Rogue Device: 192.168.50.52 00:30:1b:af:dd:c2
Option(s): autoVlanCheck(1) dropLink(3)
Switch: 192.168.1.250 1/0/19
Params: targetVlanID(10) = 20 currentVlanID(11) = 50u

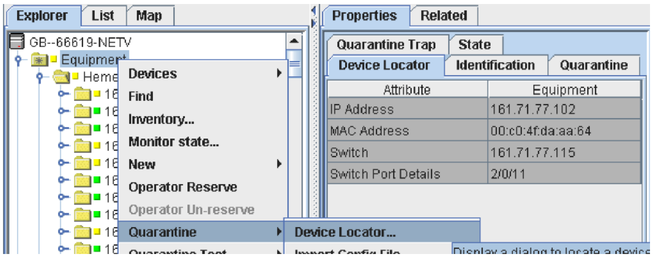
□ Auto Refresh

> Determine EMS is configured correctly to locate a device

The Device Locator feature can be used to test that the EMS can in fact locate a device:

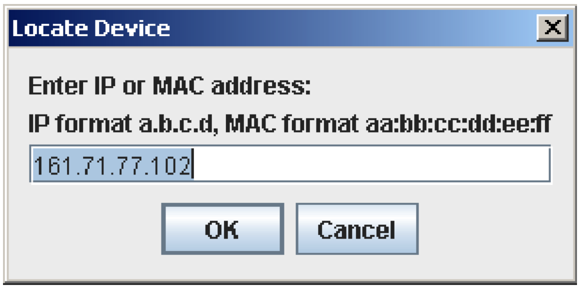
1. Right click on the Equipment root folder and choose Quarantine->Device Locator…
2. Enter the IP address of an end station that can be Quarantined and click on OK.
3. Check the Device Locator tab of the Equipment root that the MAC address and switch information are correctly identified.
4. If they are incorrect check that the end station pings and that the switch-to-switch ports are correctly specified for the switch to which the end station is connected and for the switch/router to which the switch is connected.

FIGURE 34: Quarantine Device Locator menu



Attribute	Equipment
IP Address	161.71.77.102
MAC Address	00:c0:4f:da:aa:64
Switch	161.71.77.115
Switch Port Details	2/0/11

FIGURE 35: Entering device IP address



Locate Device

Enter IP or MAC address:
IP format a.b.c.d, MAC format aa:bb:cc:dd:ee:ff

161.71.77.102

LIST OF FIGURES

LIST OF TERMS

3ND – 3Com Network Director

CHAP – Challenge-Handshake Authentication Protocol

DHCP – Dynamic Host Configuration Protocol

EAP – Extensible Authentication Protocol

EMS – 3Com Enterprise Management Suite

HTTP – HyperText Transfer Protocol

IAS – Internet Authentication Service

IEEE 802 – Institute of Electrical and Electronic Engineers series of LAN standards

IP – Internet Protocol

IPS – TippingPoint Intrusion Prevention System

L3/VPN – Layer 3 Virtual Private Network

LAN – Local Area Network

MAC – Media Access Control

NAC/NAP – Network Access Control/Network Access Protection

NAM – 3Com Network Access Manager

NCCM – Network Change and Configuration Management

NMS – Network Management System

RADA – RADIUS Authentication Device Access

RADIUS – Remote Authentication Dial-In User Service

SMS – TippingPoint Security Management System

SNMP – Simple Network Management Protocol

TELNET/SSH – Terminal-remote host protocol

UDP – User Datagram Protocol

VLAN – Virtual Local Area Network

Visit www.3com.com for more information about 3Com secure converged network solutions.

3Com Corporation, Corporate Headquarters, 350 Campus Drive, Marlborough, MA 01752-3064
3Com is publicly traded on NASDAQ under the symbol COMS.