



Avaya Solution & Interoperability Test Lab

Application Notes for Enterasys Secure Networks Dynamic Intrusion Response Solution in an Avaya IP Telephony Infrastructure - Issue 1.0

Abstract

These Application Notes describe the procedure for configuring the Enterasys Secure Networks Dynamic Intrusion Response (DIR) Solution to interoperate in an Avaya IP Telephony Infrastructure. Information in these Application Notes has been obtained through compliance testing and additional technical discussions. Testing was conducted via the *DeveloperConnection* Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe a compliance-tested configuration utilizing Avaya S8300 Media Server, Avaya G700 Media Gateway, Avaya IP Softphone, Avaya IP Office, Avaya IP Office Phone Manager Pro and Avaya 4600-series IP Telephones with the Enterasys Secure Networks Dynamic Intrusion Response (DIR).

The information provided in these Application Notes assumes the network configuration as described in the Application Notes in references [1], [2], and [3] has already occurred. Configuration done through the NetSight Atlas Policy Manager supersedes configuration done directly at the Enterasys switch.

Enterasys Dynamic Intrusion Response (DIR) is a Secure Networks Solution that detects abnormal behavior on the enterprise network, and then intervenes to quarantine the offending user or deviant device. Dynamic Intrusion Response isolates and categorizes security vulnerabilities, identifies the source and automatically reconfigures the network to mitigate the threat. The enterprise network can be protected against both known and undocumented security risks.

This compliance test focused on the ability of the Avaya S8300 Media Server with Avaya G700 Media Gateway and Avaya IP Office respectively as well as Avaya 4600-series IP Telephones to successfully operate in a network configured with Enterasys Secure Networks DIR.

The configuration in **Figure 1** shows a network consisting of Avaya S8300 Media Server with G700 Media Gateway, Avaya IP Office, Avaya 4600-series IP Telephones, Infoblox DNSone, and PCs connected to Enterasys Matrix N5, Enterasys SecureStack C2, and Enterasys SecureStack B2. The Enterasys NetSight Atlas Automated Security Manager, Enterasys Dragon Enterasys Manager Server (EMS) Client, and Enterasys Dragon Sensor are connected to the Enterasys Matrix N5. The Enterasys Matrix N5 was used to provide Layer 3 routing. See **Table 1** for detailed port configurations not already addressed in references [1], [2] and [3].

The tested configuration is shown in **Figure 1**.

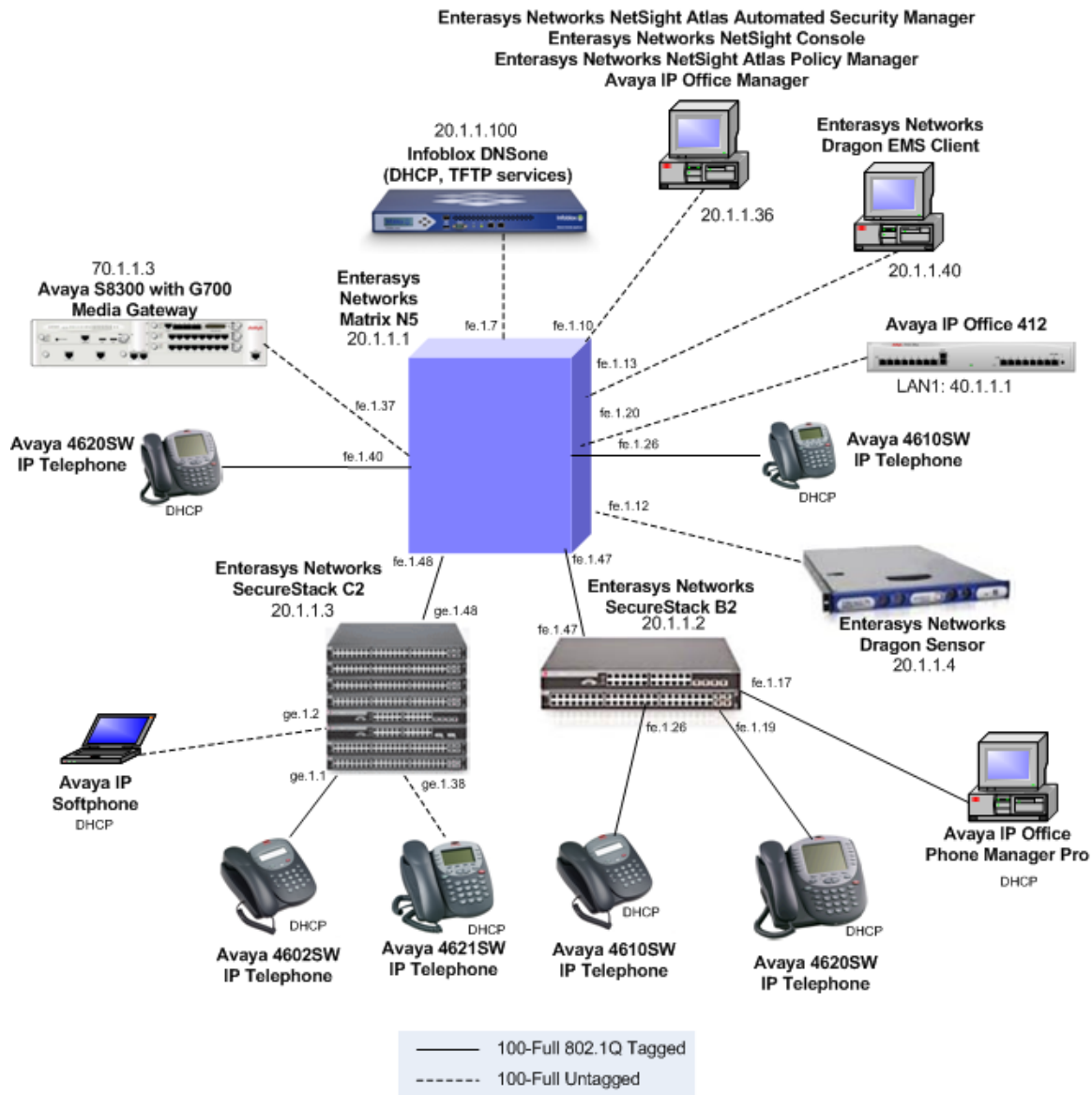


Figure 1 – Sample LAN Configuration

| Device | Port | PVID | Port Priority | Assigned Policy ¹ | Static VLANs | IP Interface |
|---|------|------|---------------|------------------------------|--------------|--------------|
| Enterasys Networks NetSight Atlas Automated Security Manager PC | NIC | | | | | 20.1.1.36/24 |
| Enterasys Networks Dragon Sensor | NIC | | | | | 20.1.1.4/24 |

¹ Please refer to **Table 3** in reference [1] for a description of the policies used in **Table 1** of these Application Notes.

| Device | Port | PVID | Port Priority | Assigned Policy ¹ | Static VLANs | IP Interface |
|--------------------------------------|---------|------|---------------|------------------------------|--------------|-----------------------|
| Enterasys Networks Dragon EMS Client | NIC | | | | | 20.1.1.40/24 |
| Enterasys Matrix N5 ² | fe.1.10 | 2 | | <i>policy1</i> | | vlan2 – 20.1.1.254/24 |
| Enterasys Matrix N5 ² | fe.1.12 | 2 | | <i>policy1</i> | | vlan2 – 20.1.1.254/24 |
| Enterasys Matrix N5 ² | fe.1.13 | 2 | | <i>policy1</i> | | vlan2 – 20.1.1.254/24 |

Table 1 – Connectivity Matrix

2. Equipment and Software Validated

The following equipment and software/firmware were used for the sample configuration provided:

| Equipment | Software/Firmware |
|--|---|
| Avaya S8300 Media Server with G700 Media Gateway | Avaya Communication Manager 3.01 (R013x.00.1.346.0) |
| Avaya IP Office 412 | 3.2(17) |
| Avaya IP400 Digital Module | 3.2(17) |
| Avaya IP Office Manager | 5.2(17) |
| Avaya IP Softphone | 5.2.4.20 |
| Avaya IP Office Phone Manager Pro | 3.2(12) |
| Avaya 4600-series IP Telephones | 2.3 |
| Enterasys Networks NetSight Atlas Automated Security Manager | 2.1 |
| Enterasys Networks Dragon Sensor | 7.1.1 |
| Enterasys Networks Dragon EMS Client | 7.1.1 |
| Enterasys Networks NetSight Atlas Policy Manager | 1.8.2 |
| Enterasys Networks NetSight Console | 2.1 |
| Enterasys Networks Matrix N5 | 05.14.04 |
| Enterasys Networks SecureStack C2 | 03.01.52 |
| Enterasys Networks SecureStack B2 | 01.01.41 |
| Infoblox DNSone | 3.2r1-1 |

Table 2 – Equipment and Software / Firmware Versions Validated

² The port's VLAN was not configured in reference [2] and [3], it should be configured as indicated in **Table 1**.

3. Configure Enterasys Networks Matrix N5 Switch

The Enterasys Networks Matrix N5 switch provides a web interface, a Command Line Interface (CLI) as well as the Enterasys Networks NetSight Console for administration. These Application Notes present administration via the CLI for configuring the Enterasys Networks Matrix N5 for this solution. The information provided in this section describes the modifications to the Enterasys Networks Matrix N5 switch configuration for this solution.


For all other provisioning information such as installation and configuration, please refer to the product documentation in reference [9].

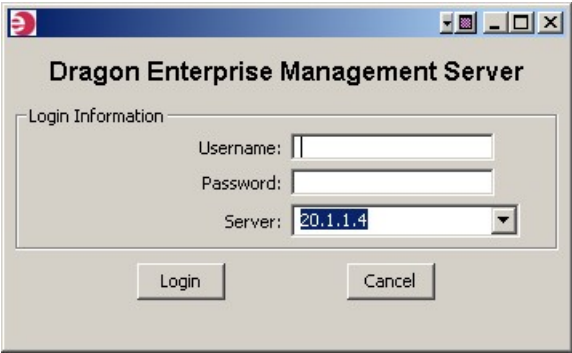

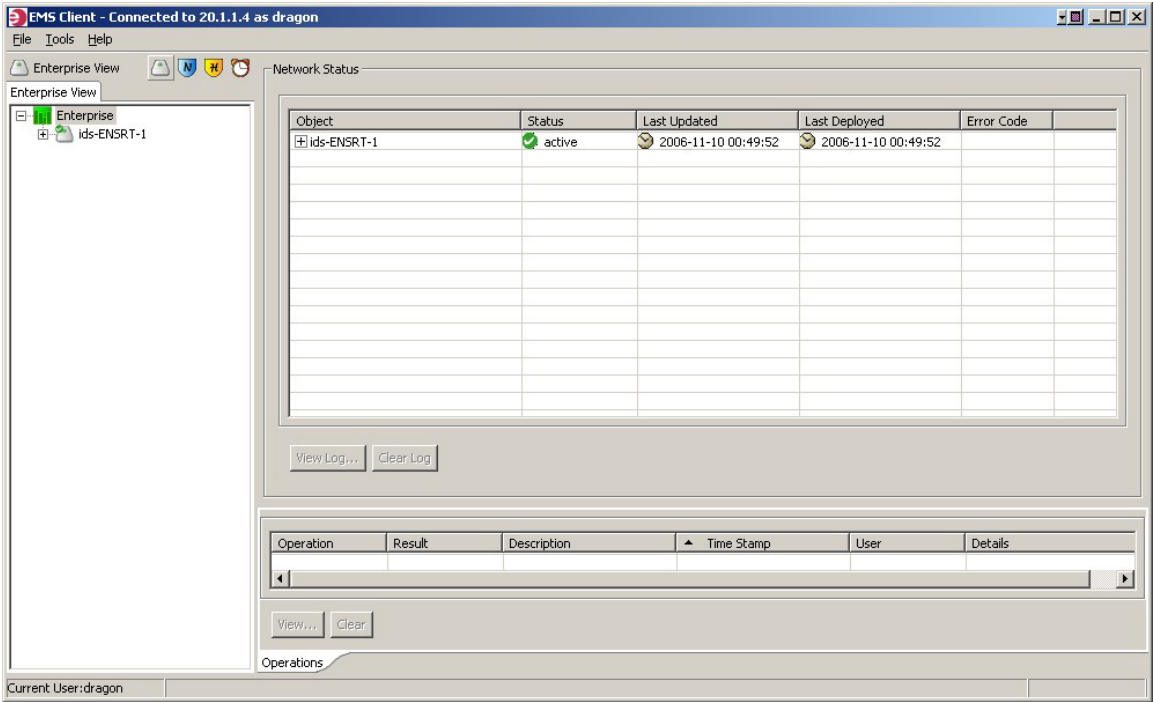
| Step | Description |
|------|--|
| 1. | Configure port mirroring of Matrix N5 trunk ports to Dragon Sensor port. Matrix>Router1# set port mirroring create fe.1.47 fe.1.12 both Matrix>Router1# set port mirroring create fe.1.48 fe.1.12 both |
| 2. | Save the configuration. This completes configuration of the Matrix N5. Matrix>Router1# show config outfile slot1/n5config |

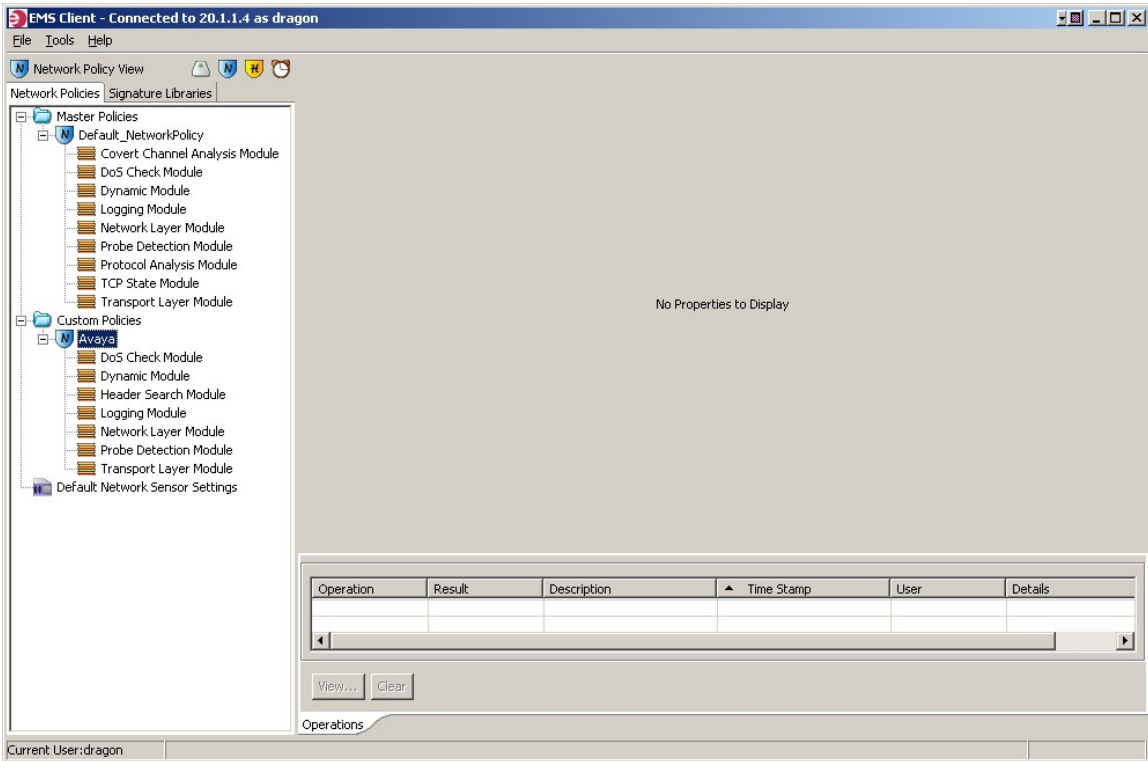
4. Configure Enterasys Networks Dragon EMS Client

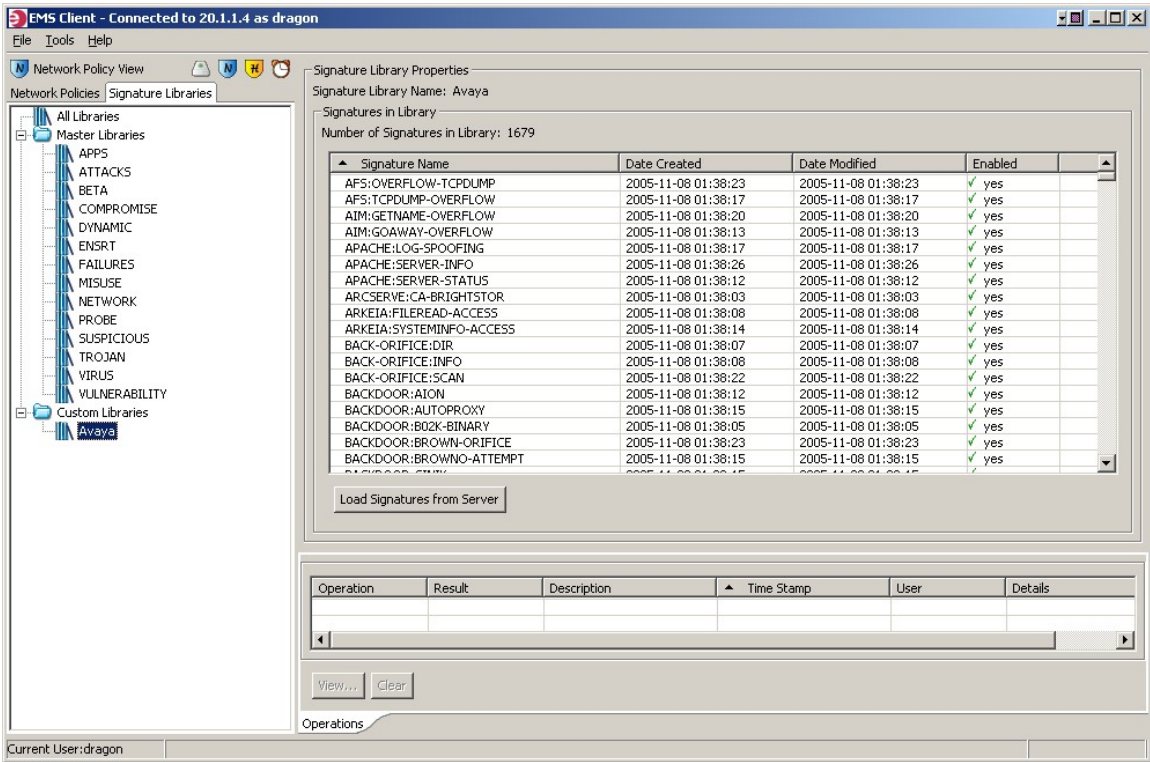
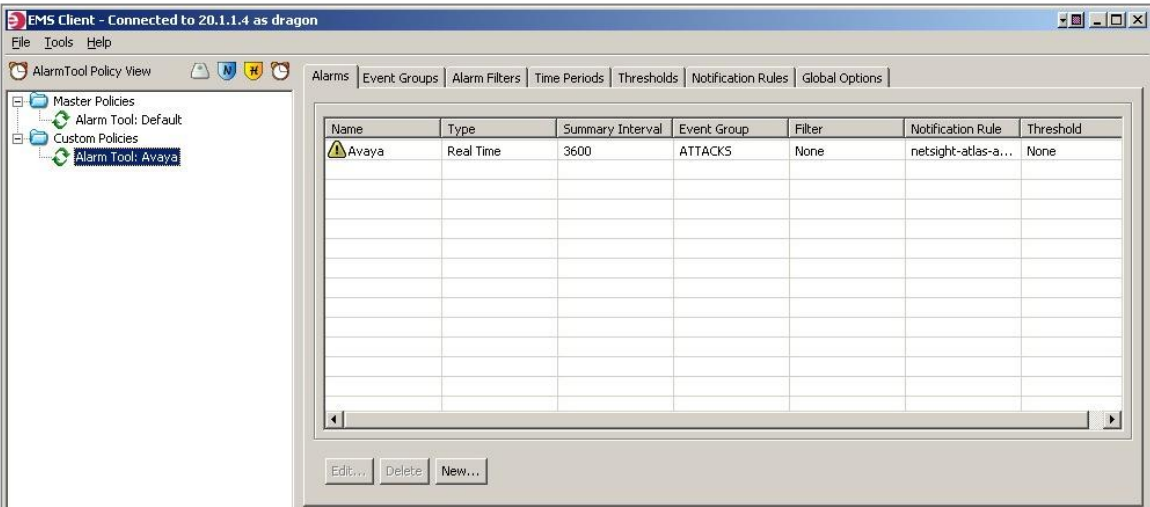
The information provided in this section describes the configuration set up with the Enterasys Networks EMS client for this solution.

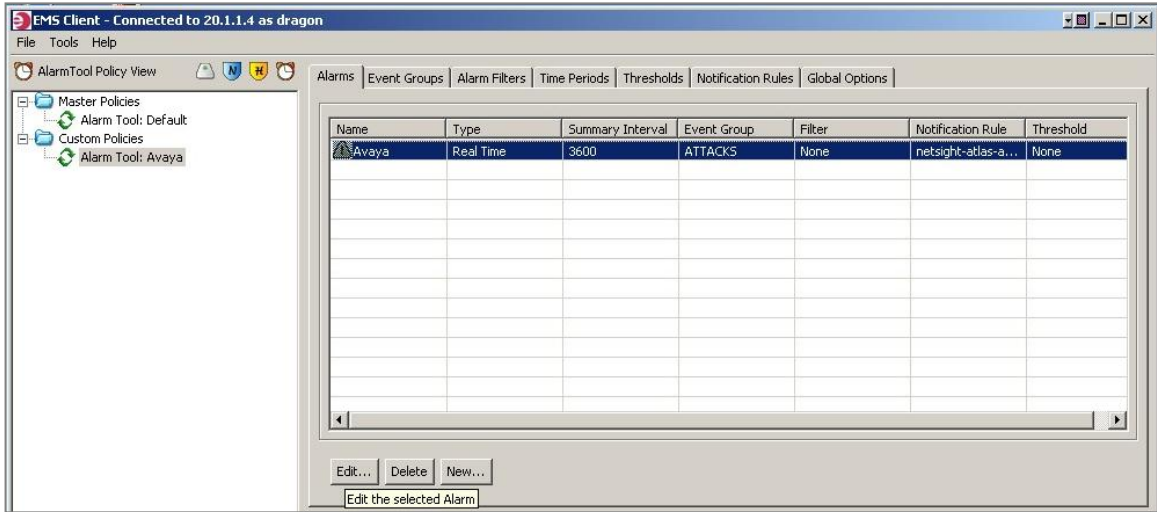
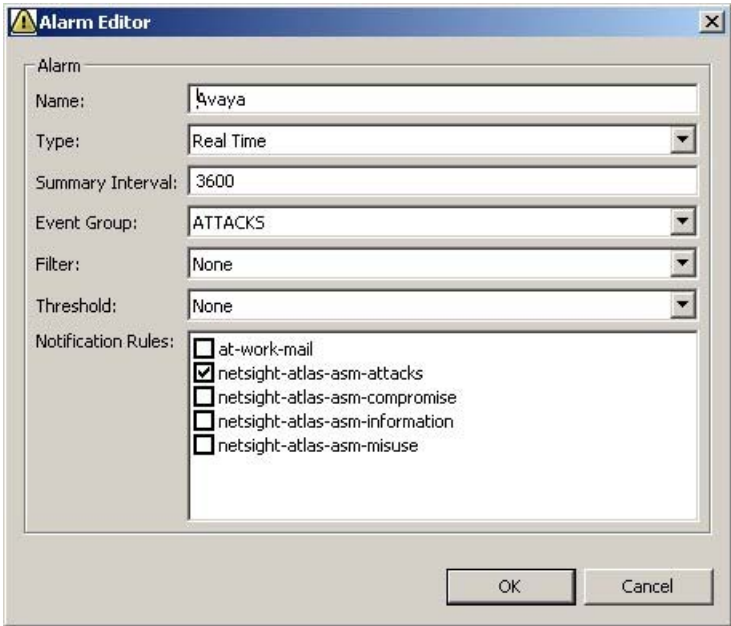
For all other provisioning information such as installation and configuration, please refer to the product documentation in reference [7].

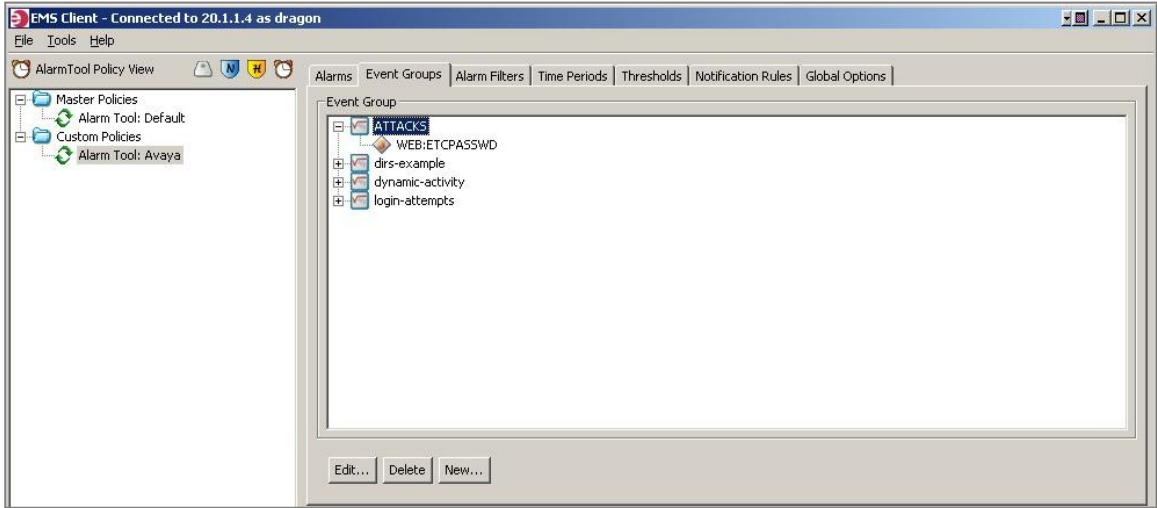
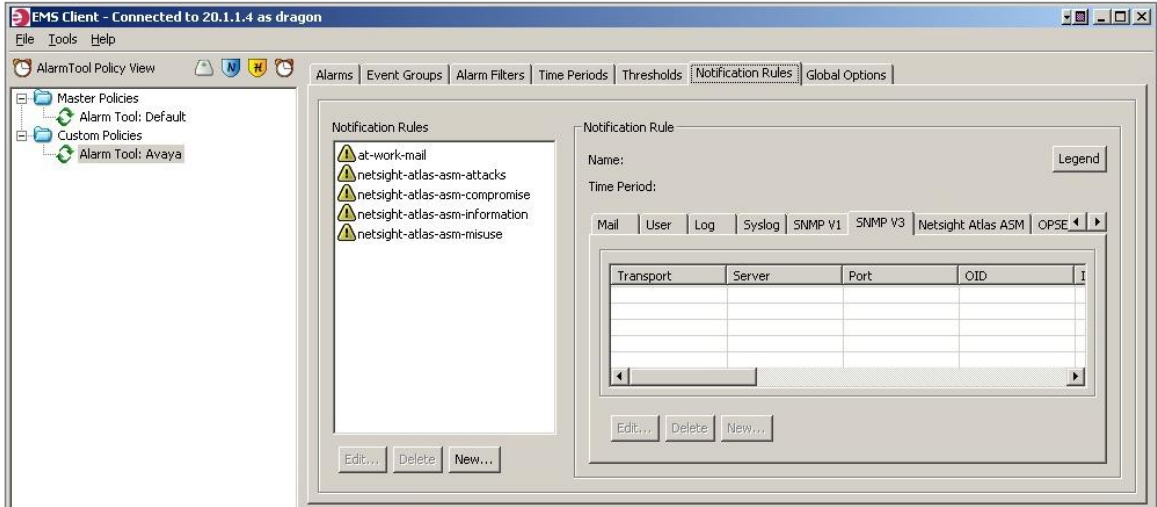
| Step | Description |
|------|---|
| 1. | Log into the Enterasys Dragon EMS client PC with administrative privileges. Double-click the EMSClientWindow icon located on the desktop.  |

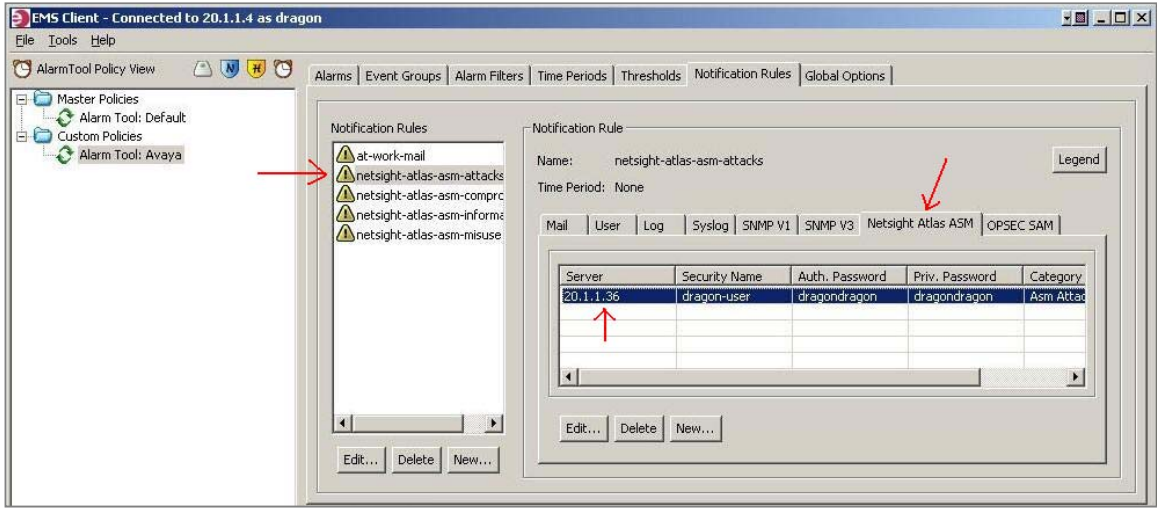
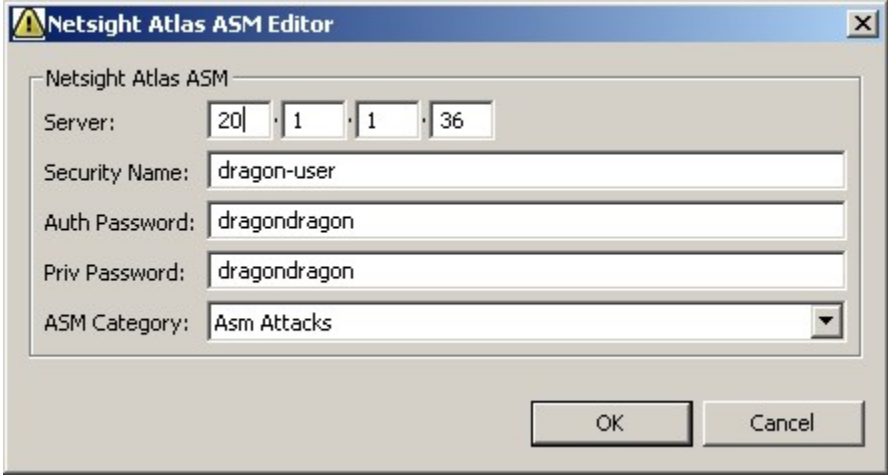
| Step | Description |
|------|--|
| 2. | <p>The screen shots in the remainder of this section were taken after the compliance test.</p> <p>In the Dragon Enterprise Management Server popup that appears, login using the appropriate credentials. Click Login.</p>  |
| 3. | <p>In the EMS Client window that appears, click the Network Policy View and Signature Libraries icon ().</p>  |


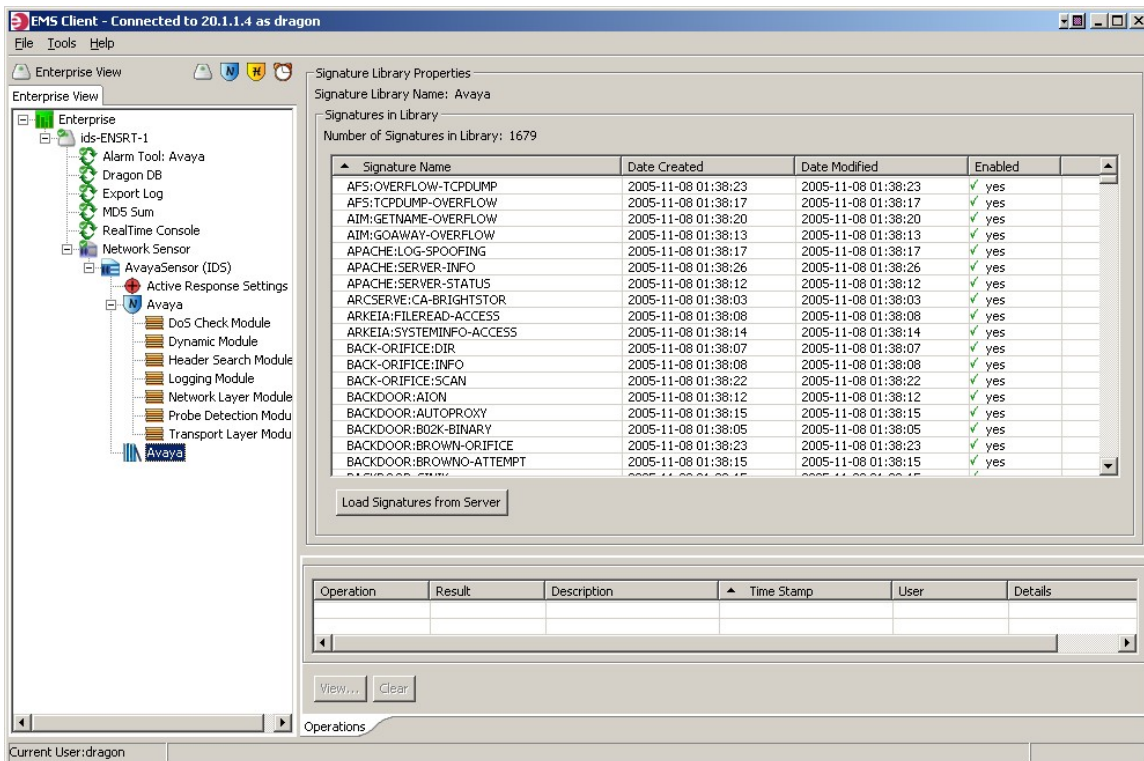
| Step | Description |
|------|---|
| 4. | <p>In the Network Policies tab of the Network Policy View window that appears, go to Custom Policies → Avaya to view the list of the Network Policies defined for this configuration.</p>  |

| Step | Description |
|------|--|
| 5. | <p>In the Signature Libraries tab of the Network Policy View window, go to Custom Libraries → Avaya to view the list of signatures placed in the library for this configuration.</p>  |
| 6. | <p>In the EMS Client window, click the AlarmTool Policy View icon (🕒) and go to Custom Policies → Alarm Tool: Avaya.</p>  |

| Step | Description |
|------|--|
| 7. | <p>In the Alarms tab on the right pane, select the only entry that appears and click the Edit... button.</p>  |
| 8. | <p>The Alarm settings used for this configuration are listed in the Alarm Editor popup that appears. For this configuration, an alarm was set to occur if an event from Event Group ATTACKS was detected. Notifications occur as defined in the netsight-atlas-asm-attacks Notification Rule. Click OK to close the popup.</p>  |

| Step | Description |
|------|--|
| 9. | <p>Click the Event Groups tab to view the list of attacks defined for this alarm.</p>  |
| 10. | <p>Click the Notification Rules tab to view the list of available notification rules.</p>  |

| Step | Description |
|------|--|
| 11. | <p>Click netsight-atlas-asm-attacks in the Notification Rules pane, click the Netsight Atlas ASM tab, select the entry that appears and click the Edit... button.</p>  |
| 12. | <p>In the Netsight Atlas ASM Editor popup that appears, Server is set to the IP address of the Netsight Atlas Security Manager as depicted in Figure 1. ASM Category is set to Asm Attacks. The values of the remaining fields, Security Name, Auth Password, and Priv Password must match the values used for username, MD5 passphrase, and DES passphrase respectively in Section 5, Step 10 for alarm notification to properly work. Click OK to exit the popup.</p>  |

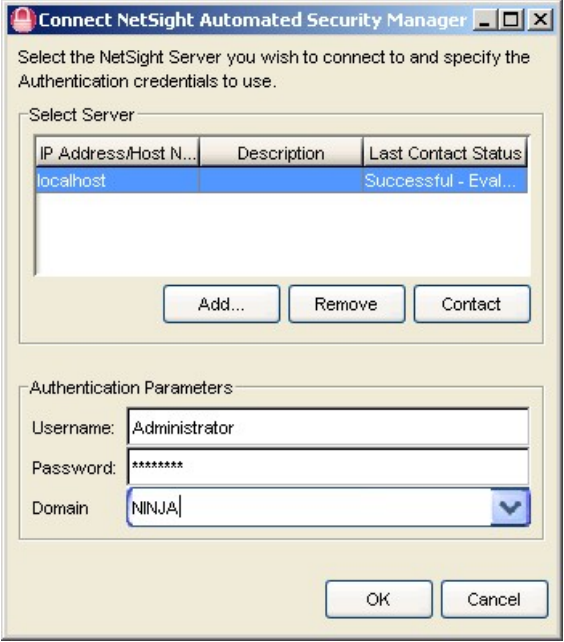
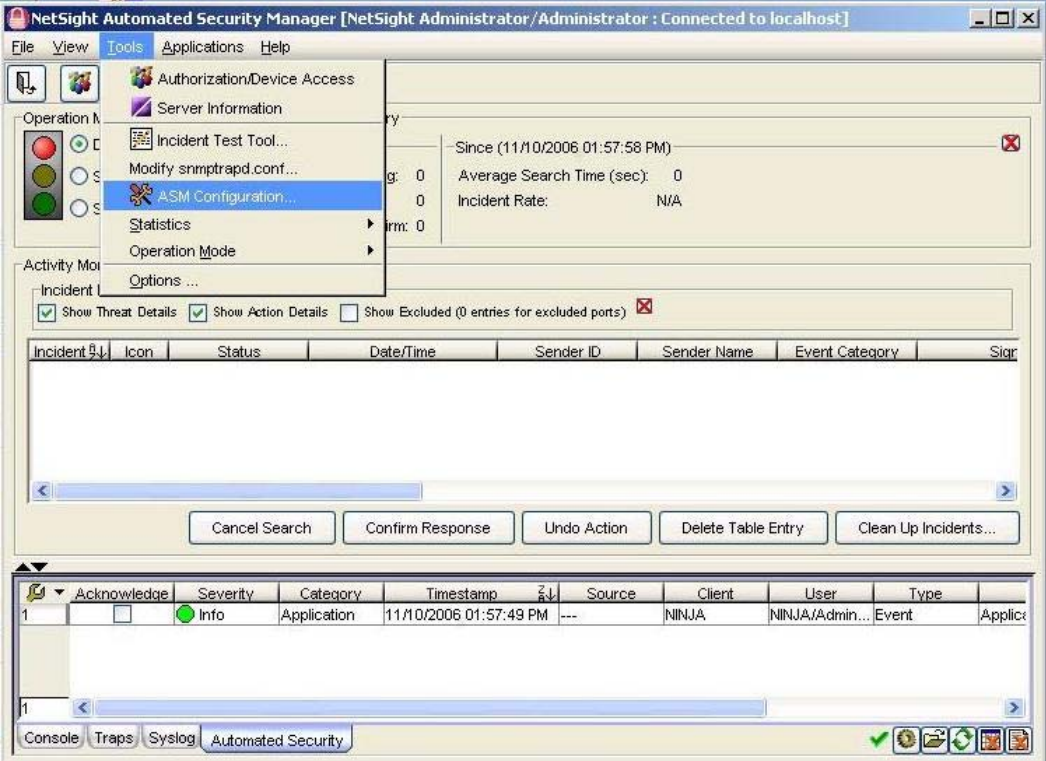
| Step | Description |
|------|--|
| 13. | <p>In the EMS Client window, click the Enterprise View icon () to view all the policies defined.</p>  |

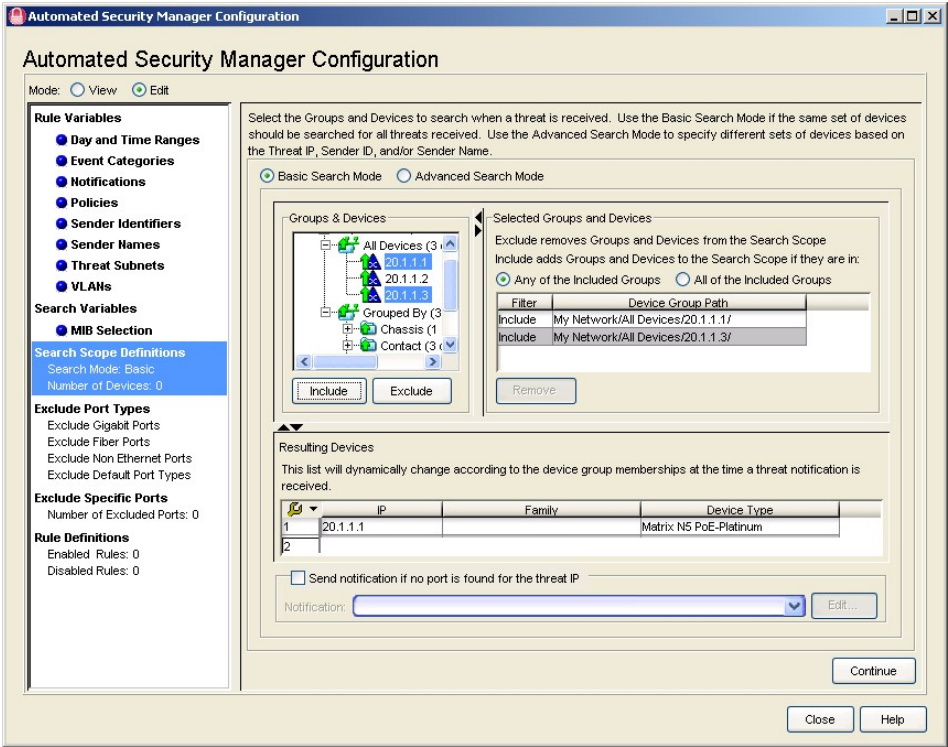
5. Configure Enterasys Networks NetSight Atlas Automated Security Manager

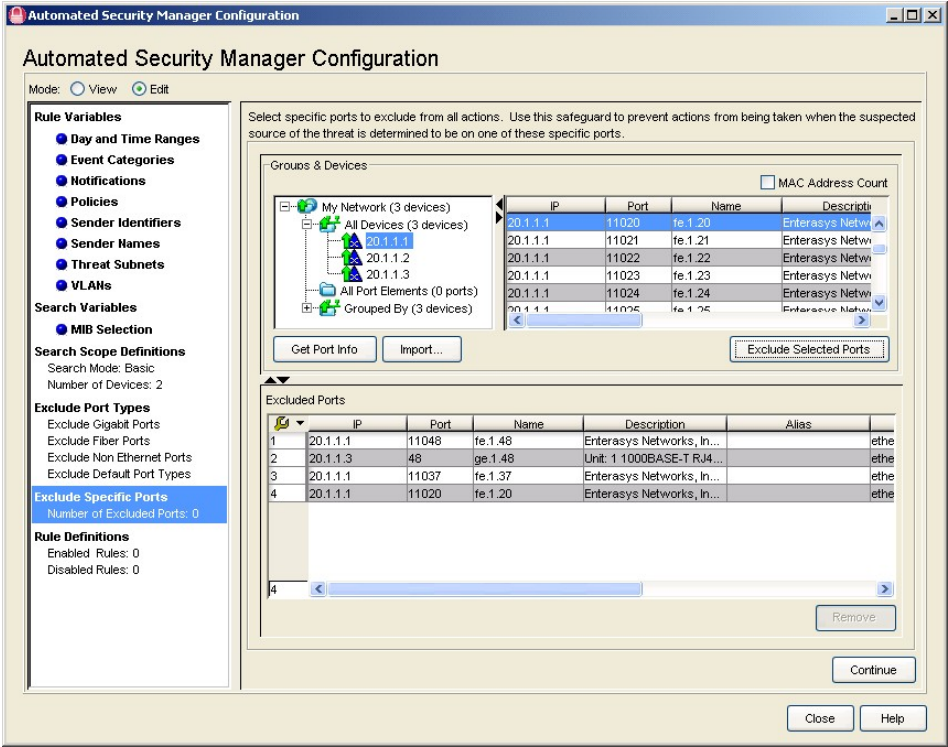
The information provided in this section describes the configuration used to set up Enterasys Networks Dynamic Intrusion Response for this solution using Enterasys NetSight Atlas Automated Security Manager.

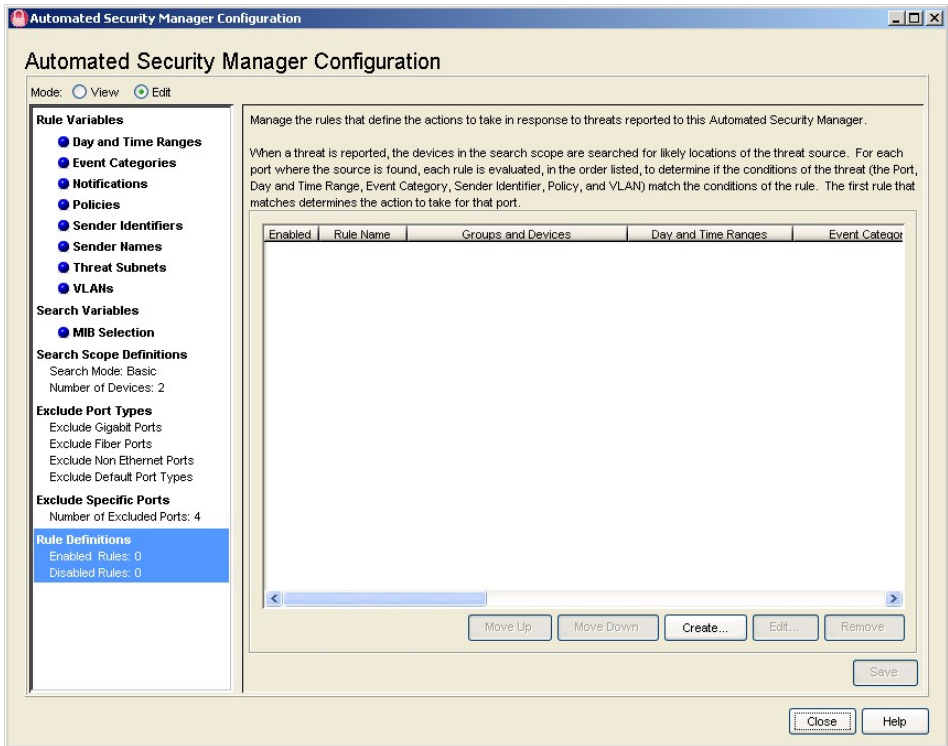
For all other provisioning information such as installation and general configuration, please refer to the product documentation in reference [7].

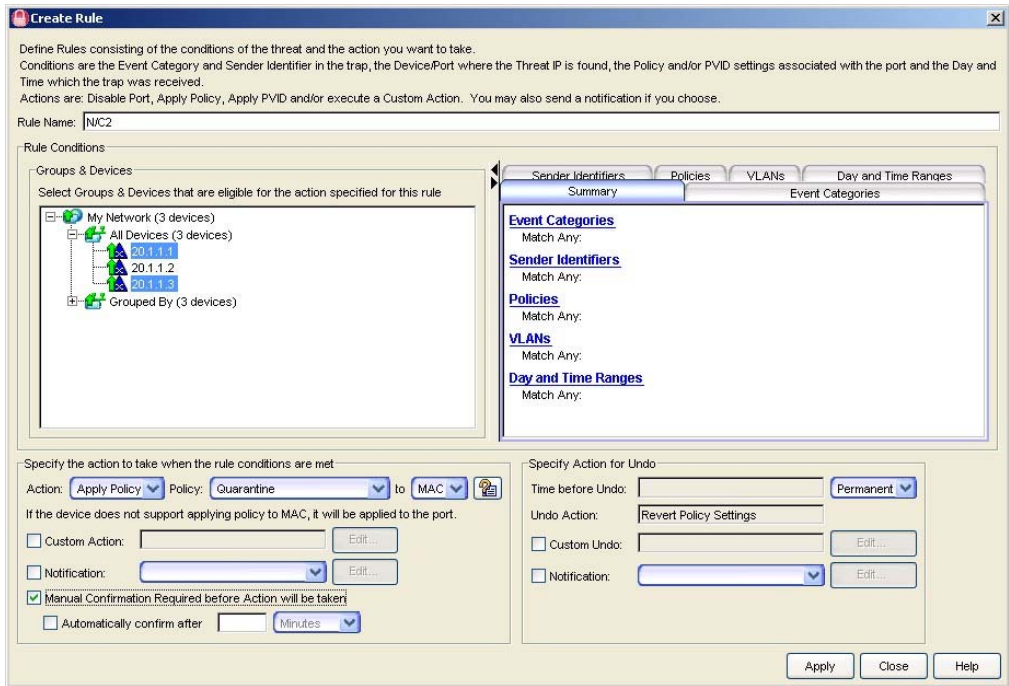
| Step | Description |
|------|--|
| 1. | <p>Log into the Enterasys NetSight Atlas Automated Security Manager PC with administrative privileges. Go to Start → Programs → Enterasys Networks → NetSight Automated Security Manager → Automated Security Manager to launch the Automated Security Manager application.</p> |

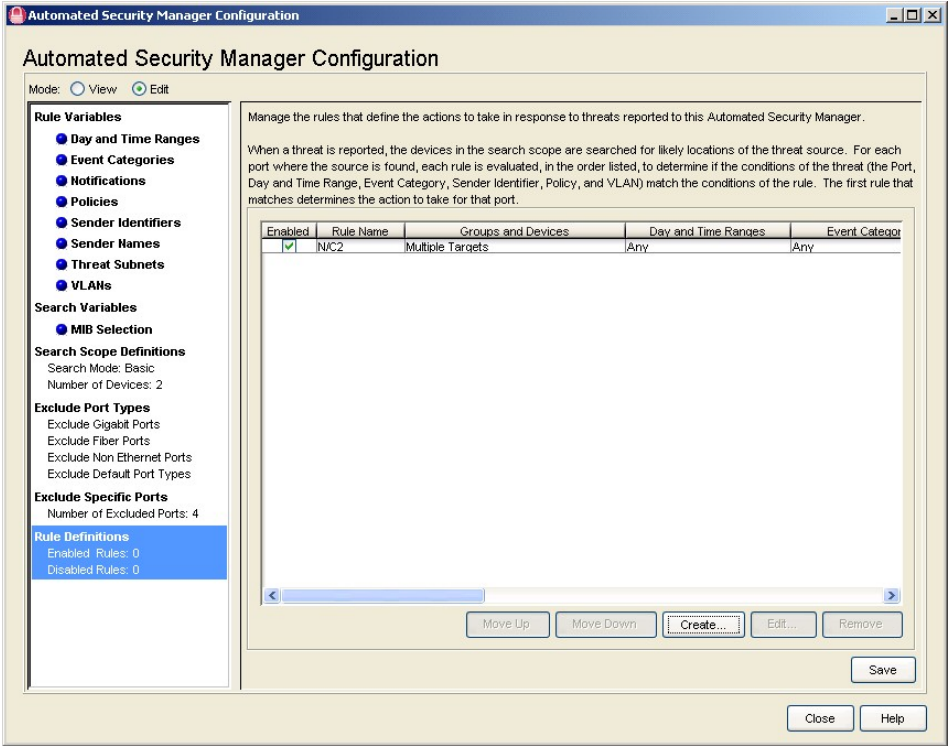

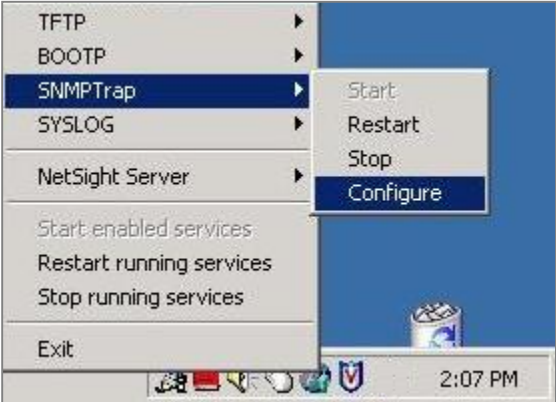
| Step | Description |
|------|--|
| 2. | <p>In the Connect NetSight Automated Security Manager popup that appears, log into the application using the appropriate login credentials.</p>  |
| 3. | <p>In the NetSight Automated Security Manager window that appears, select Tools → ASM Configuration... from the pull-down menu.</p>  |

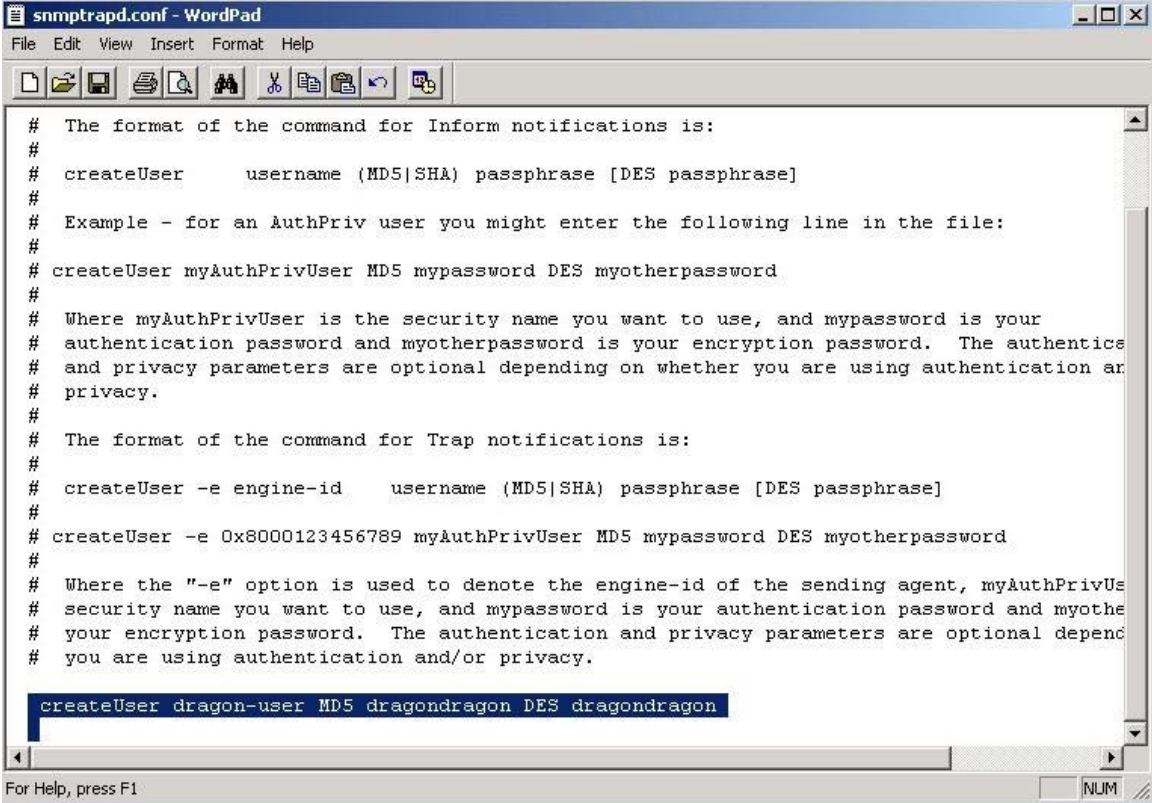

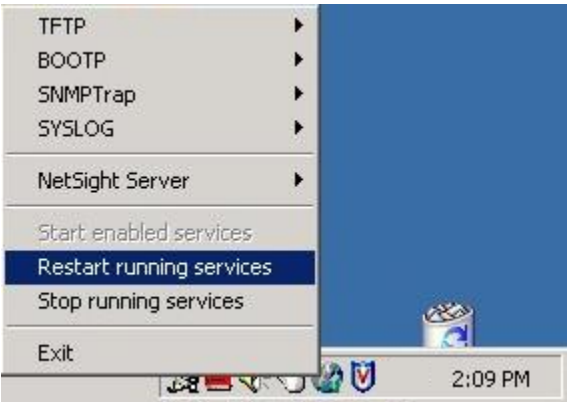
| Step | Description |
|------|---|
| 4. | <p>In the Automated Security Manager Configuration window that appears, select Edit for Mode. Click Search Scope Definitions in the left pane. On the right side of the window, select Basic Search Mode and select (highlight) the Matrix N5 (20.1.1.1) and SecureStack C2 (20.1.1.3) in the Groups & Devices pane. Click Continue.</p>  |

| Step | Description |
|------|--|
| 5. | <p>In the Exclude Specific Ports configuration screen that appears, add the following Matrix N5 ports to the list of Excluded Ports: fe.1.20 (Avaya IP Office port), fe.1.37 (Avaya S8300 with G700 Media Gateway), and fe.1.48 (uplink port connecting to SecureStack C2). Add the following SecureStack C2 port to the list of Excluded Ports: ge.1.48 (uplink port connecting to Matrix N5). Click Continue.</p>  |

| Step | Description |
|------|--|
| 6. | <p>In the Rule Definitions configuration screen that appears, click the Create... button.</p>  <p>The screenshot shows the 'Automated Security Manager Configuration' window. The 'Rule Definitions' tab is selected in the left-hand navigation pane. The main area displays a table with columns: 'Enabled', 'Rule Name', 'Groups and Devices', 'Day and Time Ranges', and 'Event Category'. The table is currently empty. Below the table are buttons for 'Move Up', 'Move Down', 'Create...', 'Edit...', and 'Remove'. At the bottom right are 'Save', 'Close', and 'Help' buttons. The 'Rule Variables' section on the left includes 'Day and Time Ranges', 'Event Categories', 'Notifications', 'Policies', 'Sender Identifiers', 'Sender Names', 'Threat Subnets', and 'VLANs'. The 'Search Variables' section includes 'MIB Selection'. The 'Search Scope Definitions' section shows 'Search Mode: Basic' and 'Number of Devices: 2'. The 'Exclude Port Types' section lists 'Exclude Gigabit Ports', 'Exclude Fiber Ports', 'Exclude Non Ethernet Ports', and 'Exclude Default Port Types'. The 'Exclude Specific Ports' section shows 'Number of Excluded Ports: 4'.</p> |

| Step | Description |
|------|--|
| 7. | <p>In the Create Rule window that appears, set Rule Name to <i>N/C2</i>, select/highlight the Matrix N5 (20.1.1.1) and the SecureStack C2 (20.1.1.3) in the Groups & Devices pane, select Apply Policy for Action, select <i>Quarantine</i> to MAC for Policy, check Manual Confirmation Required before Action will be taken. Click Apply.</p>  |

| Step | Description |
|------|--|
| 8. | <p>In the Automated Security Manager Configuration window, click Save. Click Close.</p>  |
| | <p>Edit snmptrapd.conf file</p> |
| 9. | <p>In the Taskbar Notification Area in the Automated Security Manager PC desktop (on the lower right of the screen), right-click the Enterasys Services Manager icon () and select SNMPTrap → Configure.</p>  |

| Step | Description |
|------|--|
| 10. | <p>In the snmptrapd.conf file that appears in the WordPad editor, define the user for snmp trap notifications to the Automated Security Manager. The username, MD5 passphrase and DES passphrase must match the settings defined in Section 4, Step 12. When finished, save and quit from the WordPad editor.</p>  <pre> # The format of the command for Inform notifications is: # # createUser username (MD5 SHA) passphrase [DES passphrase] # # Example - for an AuthPriv user you might enter the following line in the file: # # createUser myAuthPrivUser MD5 mypassword DES myotherpassword # # Where myAuthPrivUser is the security name you want to use, and mypassword is your # authentication password and myotherpassword is your encryption password. The authentic # and privacy parameters are optional depending on whether you are using authentication and # privacy. # # The format of the command for Trap notifications is: # # createUser -e engine-id username (MD5 SHA) passphrase [DES passphrase] # # createUser -e 0x8000123456789 myAuthPrivUser MD5 mypassword DES myotherpassword # # Where the "-e" option is used to denote the engine-id of the sending agent, myAuthPrivUser # security name you want to use, and mypassword is your authentication password and myothe # your encryption password. The authentication and privacy parameters are optional depend # you are using authentication and/or privacy. createUser dragon-user MD5 dragondragon DES dragondragon </pre> |
| 11. | <p>In the Taskbar Notification Area in the Automated Security Manager PC desktop, right-click the Enterasys Services Manager icon () and select Restart running services.</p>  |

6. Interoperability Compliance Testing

The Interoperability Compliance Test included feature functionality and performance testing. Feature functionality testing examined the ability of devices (Avaya 4600-series IP Telephones, Avaya IP Softphone, and Avaya IP Office Phone Manager Pro) to successfully boot, obtain network configuration from the DHCP Server (Infoblox DNSone), and register to either Avaya Communication Manager or Avaya IP Office as applicable with the Dynamic Intrusion Response policies defined through the Enterasys Networks NetSight Atlas Automated Security Manager. VoIP calls were made to confirm that the defined policies did not impact voice quality. Performance tests verified that the configuration remained stable under load.

6.1. General Test Approach

Feature functionality testing was performed manually. Calls were made between stations that were registered to Avaya Communication Manager for Avaya Communication Manager tests and calls were made between stations that were registered to Avaya IP Office for Avaya IP Office tests. A protocol analyzer was used to monitor call signaling and audio flows to ensure that proper QoS markers at Layer 2 and Layer 3 as defined by the Acceptable Use Policy and were being relayed. Performance testing was done using a data traffic generator to stress the QoS functionality of the devices over a one-hour period.

6.2. Test Results

All feature functionality and performance test cases passed successfully. A one-hour test was conducted with 200 Mbps of traffic saturating the 100 Mbps LAN link between the Matrix N5 switch and the SecureStack C2 and SecureStack B2 respectively³. Various calls were placed between extensions on the Matrix N5 and SecureStack C2 and SecureStack B2 without any call loss or voice quality degradation.

7. Verification Steps

- Verify that the IP Telephones power up, obtain initial DHCP address from the data VLAN, tag on the voice VLAN based on option 176 values and successfully complete the registration process.
- Place IP-to-IP calls and verify audio quality.
- Place IP-to-Digital calls and verify audio quality

³ The policies used in the configuration were rate limiting the traffic entering the Enterasys switches. In order to successfully perform the load test, throughput limits were removed from ports connected to the traffic generator to ensure the network trunk links were properly saturated.

8. Support

For technical support on the Enterasys Secure Networks Solutions, contact the Enterasys Technical Support at 800-872-8440. Technical support email can be sent to support@enterasys.com. Additional information can be found in the Enterasys Support website at <http://www.enterasys.com/services/support>.

9. Conclusion

These Application Notes describe a compliance-tested configuration of Enterasys Secure Networks Dynamic Intrusion Response (DIR) in an Avaya IP Telephony Infrastructure. Features and functionality were successfully validated.

10. Additional References

Available from Avaya (www.avaya.com)

- [1] Application Notes for Enterasys Secure Networks Acceptable Use Policy Solution in an Avaya IP Telephony Infrastructure – Issue 1.0, January 2007
- [2] Application Notes for Enterasys Networks Matrix N5, Enterasys Networks SecureStack C2 and Enterasys Networks SecureStack B2 with Avaya Communication Manager – Issue 1.0, December 2006
- [3] Application Notes for Enterasys Networks Matrix N5, Enterasys Networks SecureStack C2, and Enterasys Networks SecureStack B2 with Avaya IP Office – Issue 1.0, December 2006
- [4] Application Notes for Infoblox DNSone in an Avaya Communication Manager IP Telephony Infrastructure – Issue 1.0, March 2006
- [5] Avaya IP Office Monitor (SysMon), Issue 1e, 13th October 2005
- [6] Avaya Application Solutions: IP Telephony Deployment Guide, 555-245-600, Issue 3.4.1, June 2005

Available from Enterasys (www.enterasys.com)

- [7] Enterasys Networks Automated Security Manager Help
- [8] Enterasys NetSight Policy Manager, Version 1.8.2
- [9] Enterasys Networks Matrix N Standalone (NSA) Platinum Series Configuration Guide, Firmware Version 5.14.xx

©2007 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya Developer*Connection* Program at devconnect@avaya.com.