



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring the Extreme Networks Sentriant Security Appliance in an Avaya IP Telephony Infrastructure – Issue 1.1

Abstract

These Application Notes describe a configuration where the Extreme Networks Sentriant network security appliance protects the subnets where an Avaya Media Server and Avaya IP Telephones reside against rapidly propagating threats. During compliance testing, the Sentriant detected basic ping and port scans that often precede threats on the protected subnets, and mitigated basic Denial of Service (DoS) attacks. 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 configuration where the Extreme Networks Senti-ant security appliance is deployed in an Avaya IP telephony infrastructure. Senti-ant is a security appliance that is designed to protect the internal corporate network against rapidly propagating threats and LAN attacks. Senti-ant operates within the network interior, and is complementary to perimeter security solutions.

Senti-ant uses pre-defined and configurable rules in monitoring the network for potential threats. Once a threat is identified, Senti-ant mitigates the threat by “cloaking”, where Senti-ant logically inserts itself in the path between the attacker and the target. Specifically, Senti-ant redirects the attacker communications streams to itself by changing the ARP tables in the attacker and/or target. Senti-ant can then selectively filter out malicious packets and forward the rest to the target. Senti-ant can also be configured to send alerts via e-mail (SMTP), SNMP, and Syslog when threats are identified.

CLEAR-Flow (Continuous Learning, Examination, Action and Reporting of Flows) is a flexible, dynamic and ExtremeWare XOS feature to monitor network traffic in combination with ACL rules to take appropriate action when certain traffic conditions are met. The Extreme Senti-ant can work with integrated CLEAR-Flow rules within the ExtremeWare XOS operating system running on the Extreme Networks switch, such as BlackDiamond 10K. With the application of CLEAR-Flow rules, Senti-ant allows the switch to pre-qualify traffic flows that are considered indicative of operational threat behaviors. If such traffic is detected, that specific traffic flow is selectively mirrored to the Senti-ant device, which performs additional classification and analysis to determine if the specific traffic flow is actually harmful traffic. If the traffic is harmful, the source is determined and mitigated or stopped by the Senti-ant device.

Figure 1 illustrates a sample configuration consisting of an Avaya S8300 Media Server with Avaya G700 Media Gateway, Avaya IP Telephones, an Extreme BlackDiamond 10K switch, an “Attacker” PC, and an Extreme Networks Senti-ant security appliance. Avaya Communication Manager runs on the S8300 Media Server, though the solution described herein is also extensible to other Avaya Media Servers and Media Gateways. The S8300 Media Server resides on VLAN 10 and is connected to the BlackDiamond 10K via an 802.1Q trunk. The IP Telephones reside on VLAN 20 and are connected to the BlackDiamond 10K switch with 802.1Q port. The “Attacker” PC resides on VLAN 30.

The Senti-ant security appliance connects to two ports on the Extreme BlackDiamond 10K switch. The VLANs to be protected (VLANs 10 and 20) are also assigned to the two ports. The protected VLANs are mirrored to one of the two Extreme BlackDiamond 10K ports (the “Reader” port), allowing the Senti-ant to monitor unicast and broadcast traffic on the protected VLANs. The other port (the “Writer” port) allows the Senti-ant to transmit ARP messages onto the protected VLANs and perform cloaking.

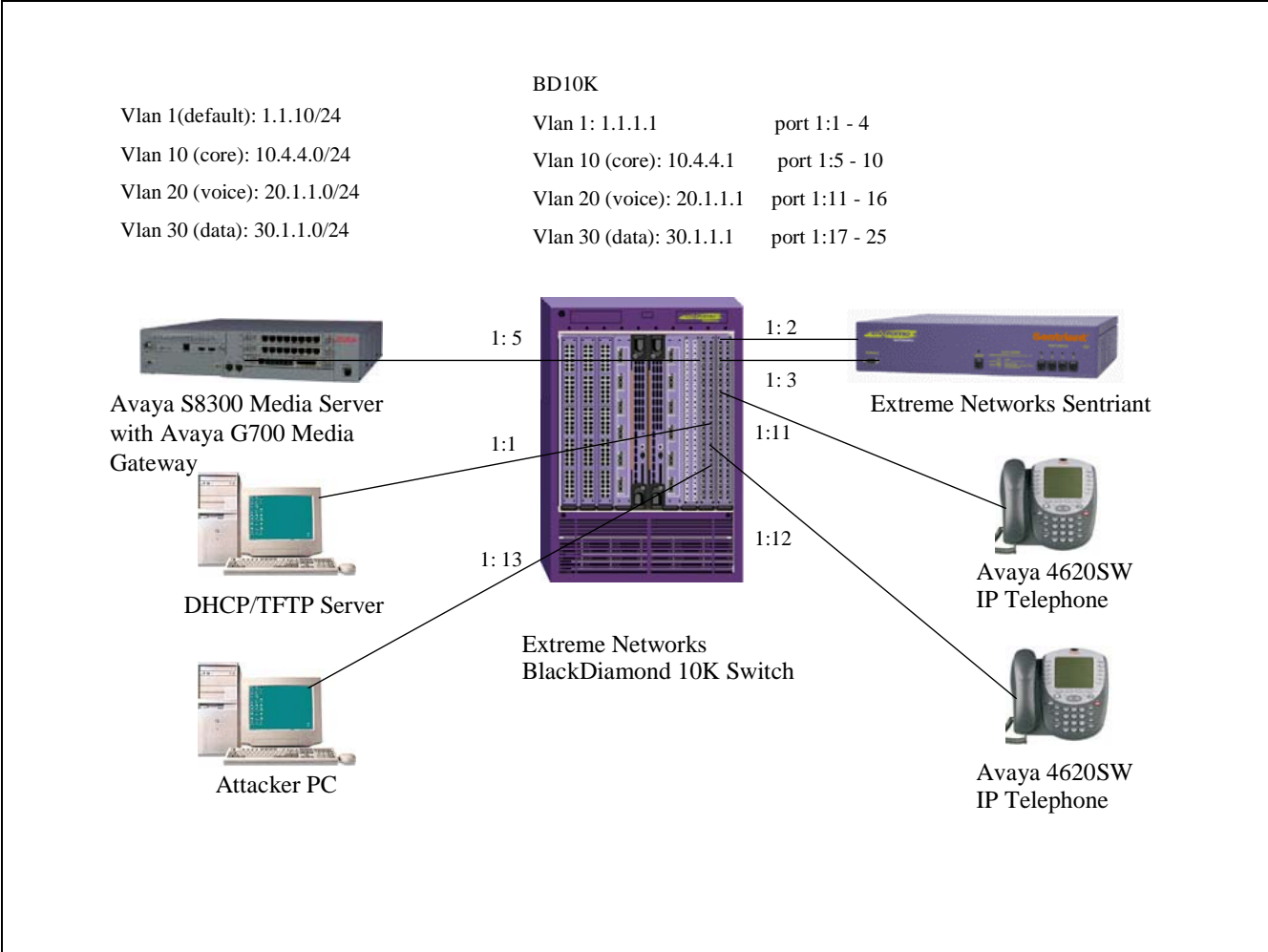


Figure 1: Sample configuration.

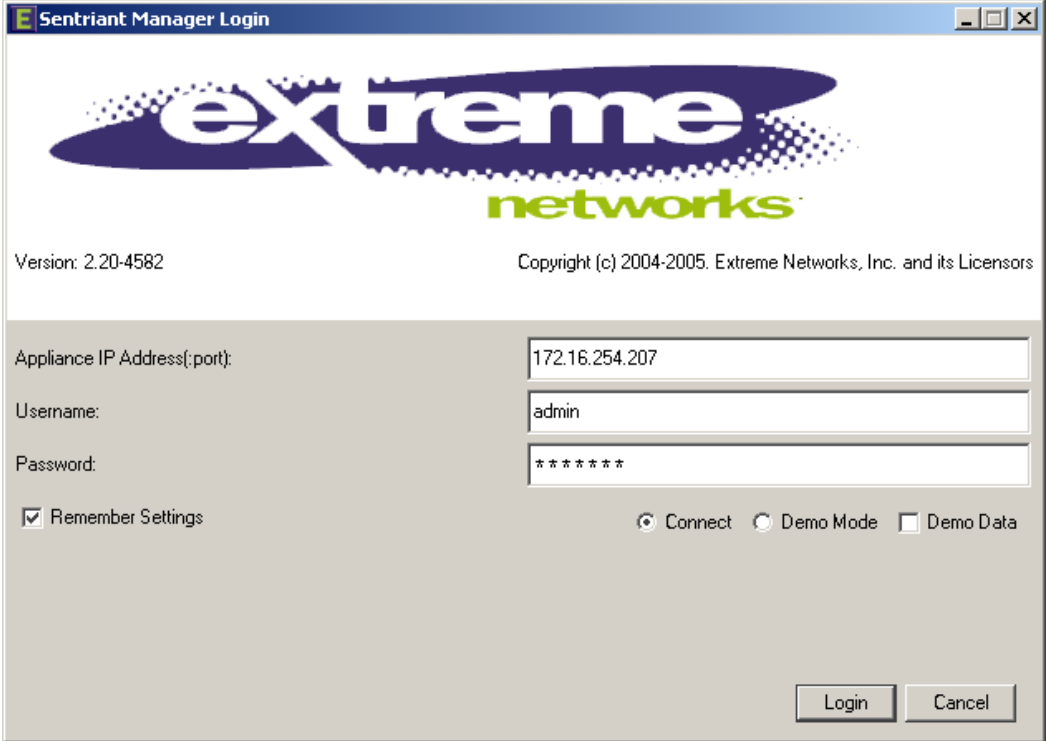
2. Equipment and Software Validated

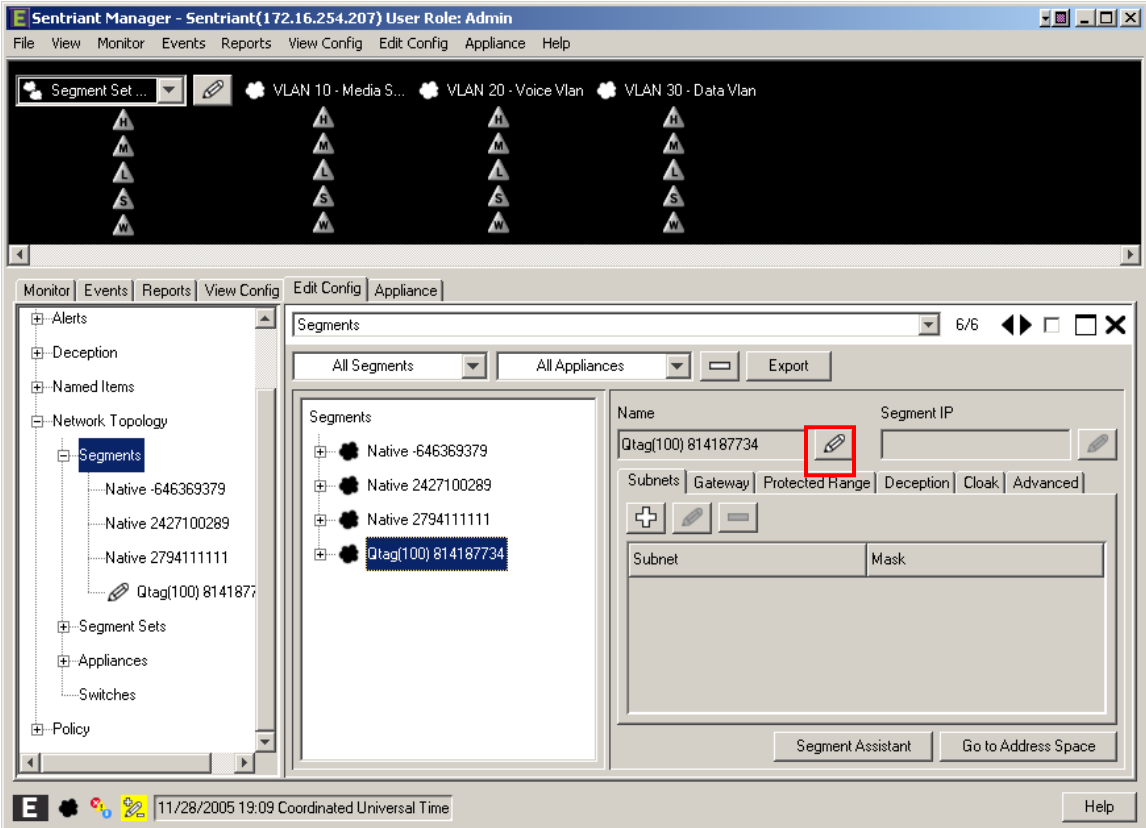
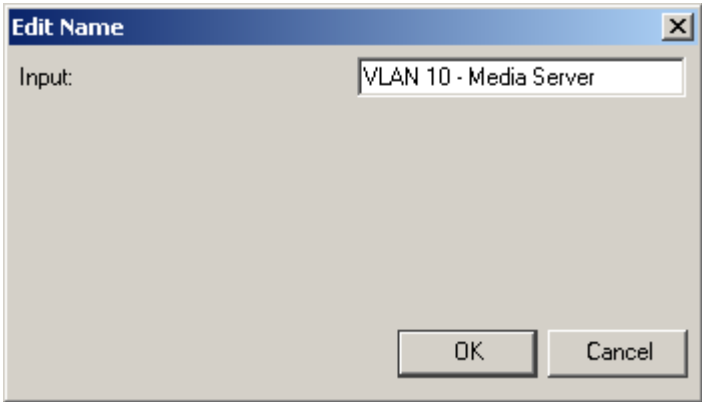
The following equipment and software/firmware were used for the sample configuration provided:

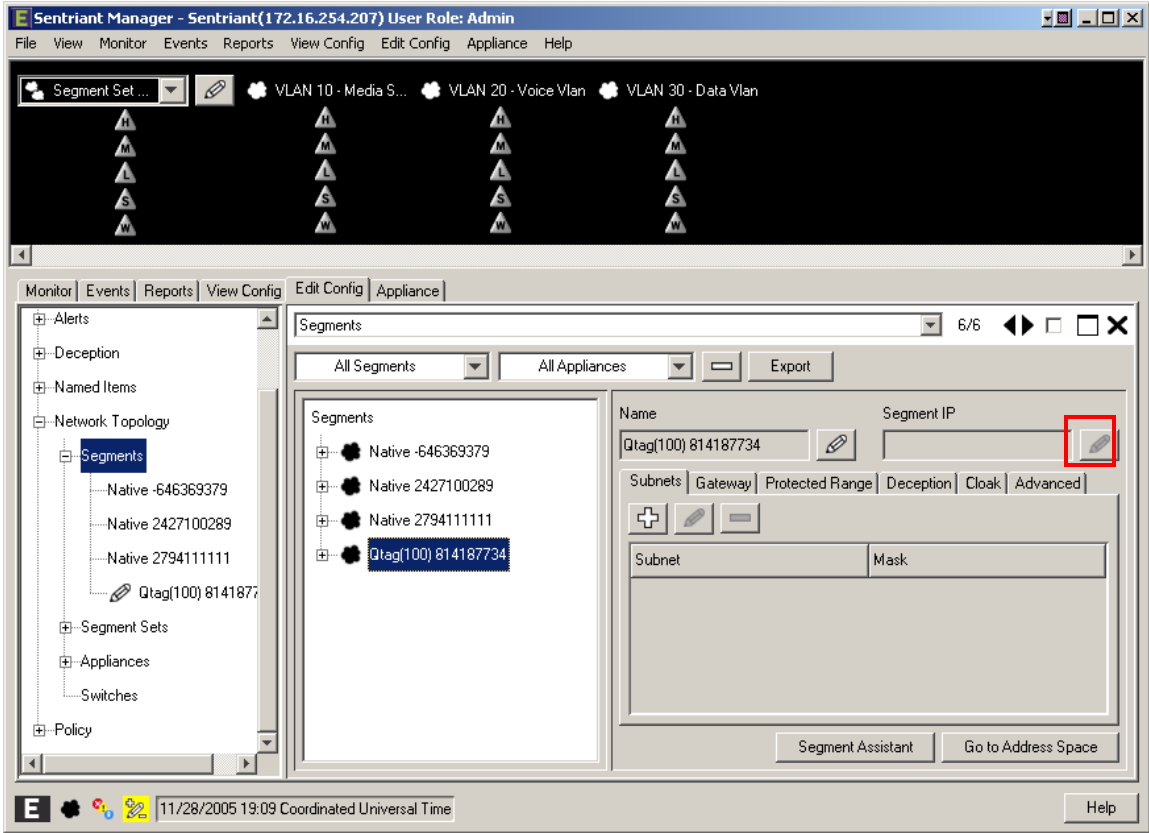
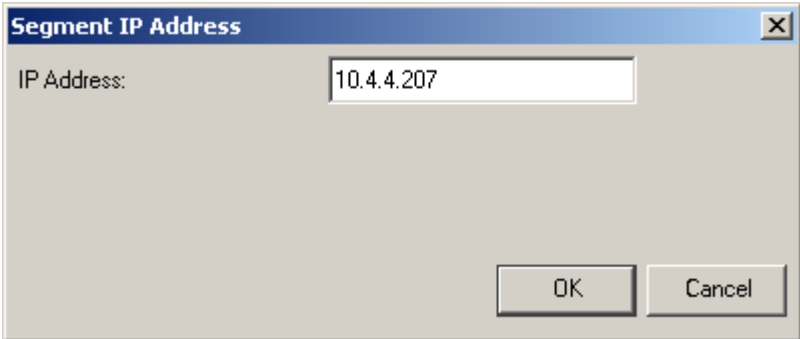
Equipment	Software/Firmware
Avaya S8300 Media Server with G700 Gateway	Avaya Communication Manager 3.0 Load (340.3)
Avaya 4620 Series IP Telephones	2.2.3 (4620SW)
Extreme Networks Sentriant	2.2 Build 4583
Extreme Networks Black Diamond 10K Switch	XOS 11.2.0.5
Attacker PC	Red Hat Linux ES 3

3. Configure Extreme Networks Sentriant

This section describes the steps for configuring the Extreme Networks Sentriant to protect the subnets (VLANs 10 and 20 in the sample configuration) where the Avaya S8300 Media Server and IP Telephones reside. The subnet (VLAN 30) where the attacker PC resides cannot be protected due to the VLAN mirror function of the Extreme BlackDiamond 10K. Specifically, when the Extreme BlackDiamond 10K receives untagged frames from VLAN 30 endpoints, including the attacker PC, the Extreme BlackDiamond 10K copies the untagged frames to the mirror port without applying the VLAN 30 tag. Without the VLAN tag, the Sentriant cannot determine what subnet the frames belong to, and thus has no “visibility” into VLAN 30 and cannot protect the subnet. The Sentriant does have visibility into VLAN 10 and 20 because the Avaya S8300 Media Server and Avaya IP Telephones transmit/receive tagged frames in these two VLANs.

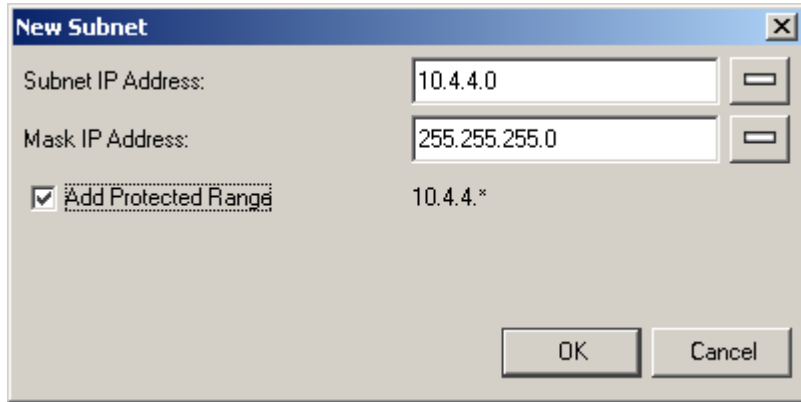
Step	Description
1.	<p>Assume that the Sentiari Manager Application software has been installed on a computer and an IP address 172.16.254.207 has been assigned to Sentiari. Follow the steps below to access Sentiari configuration menu.</p> <ul style="list-style-type: none"> • Launch the Sentiari Manager application. • Enter the IP address in the Appliance IP Address field. • Log in with the appropriate credentials. 

Step	Description
<p>2.</p>	<ul style="list-style-type: none"> • Select the Edit Config tab and expand the Network Topology tree to the Segments level. • Select a QTag (VLAN) and click on the icon next to it. 
<p>3.</p>	<p>Assign a descriptive name and click on “OK”.</p> 

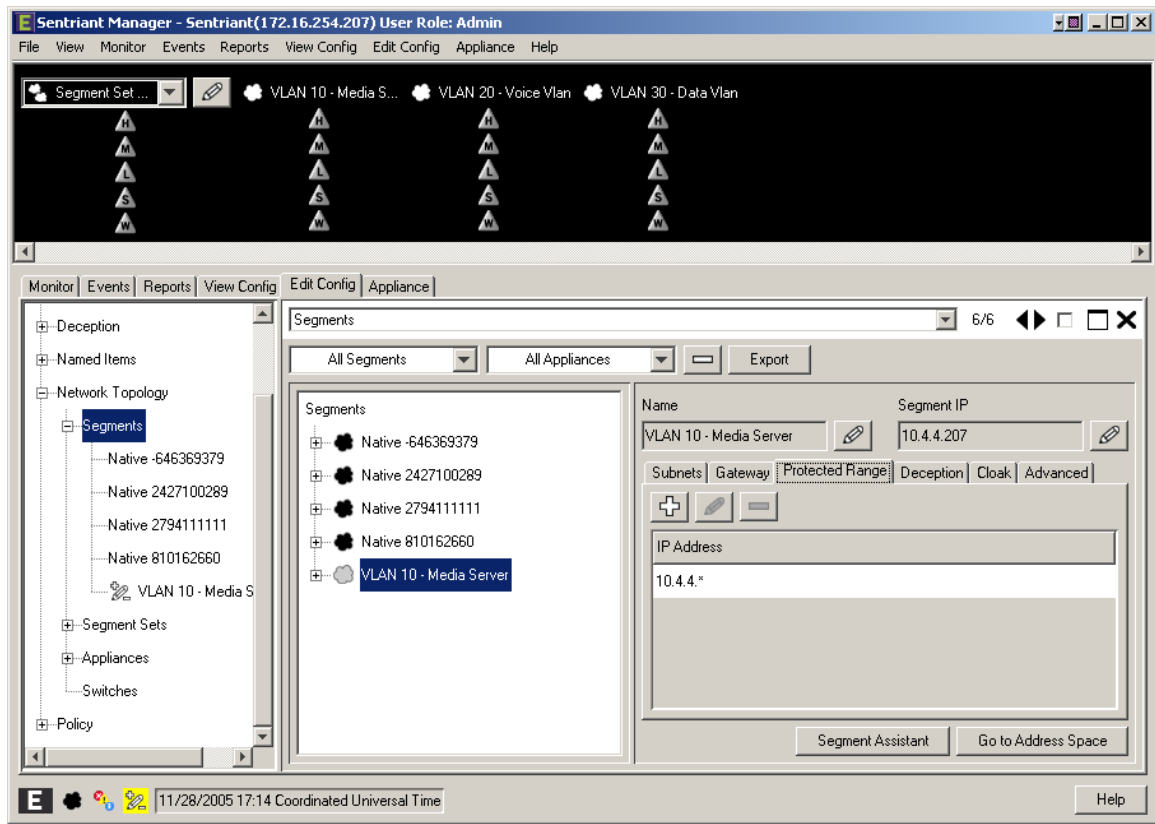
Step	Description
<p>4.</p>	<p>Click on the icon next to Segment IP.</p>  <p>The screenshot shows the 'Sentriant Manager' application window. The main area displays a list of segments under the 'Segments' tab. The segment 'Qtag(100) 814187734' is selected. The configuration details for this segment are shown on the right, including the 'Segment IP' field which is highlighted with a red box. A pencil icon next to the 'Segment IP' field is the target of the instruction.</p>
<p>5.</p>	<p>Assign an available IP Address to the Sentriant on this VLAN and click on “OK”.</p>  <p>The screenshot shows a dialog box titled 'Segment IP Address'. The 'IP Address' field contains the value '10.4.4.207'. There are 'OK' and 'Cancel' buttons at the bottom of the dialog.</p>
<p>6.</p>	<p>Select the Subnets tab and click on the “+” icon.</p>

Step	Description
------	-------------

- | | |
|----|--|
| 7. | <ul style="list-style-type: none"> Enter the subnet information for this VLAN, and check the Add Protected Range checkbox to protect the entire subnet. Click on OK. |
|----|--|



IP subnet 10.4.4.* is included in **Protected Range**.



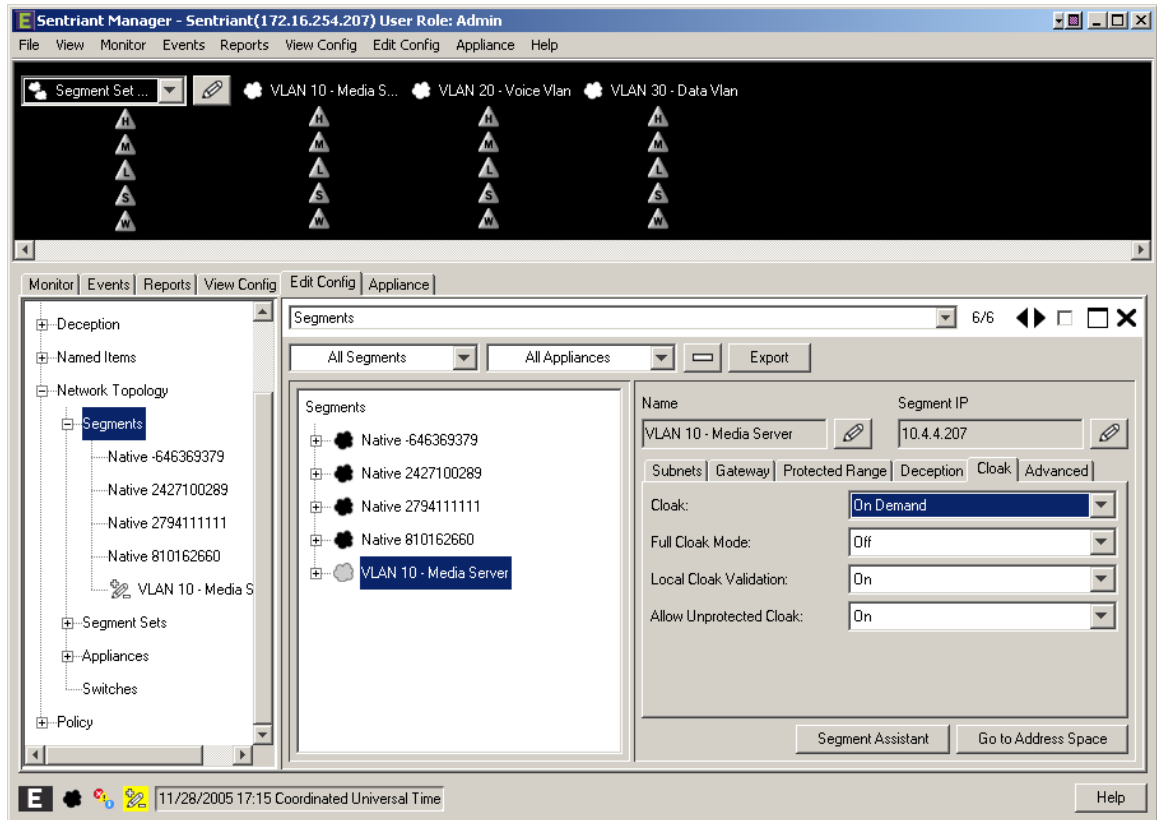
To protect specific ranges within the subnet, uncheck the **Add Protected Rang** checkbox and configure the ranges in the **Protected Range** tab (not described in these Application Notes)

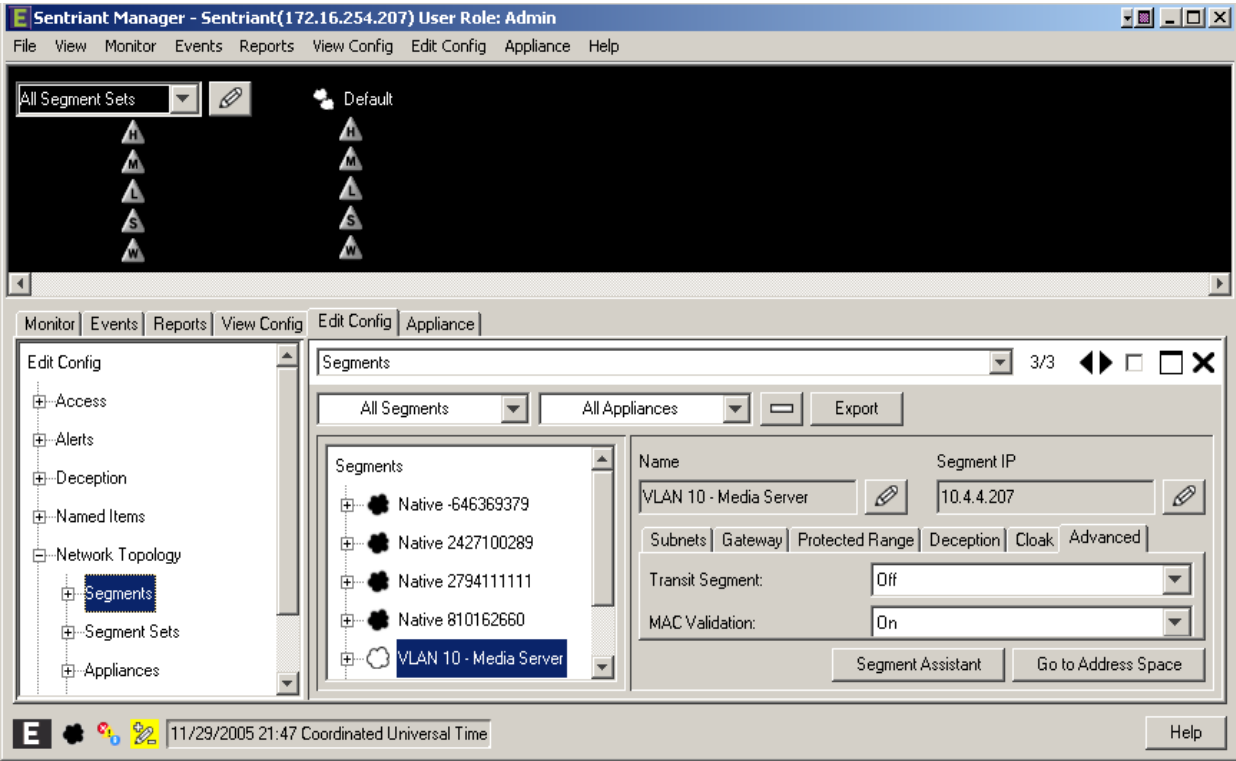
Step	Description
8.	Select the Gateway tab and click on the “+” icon.
9.	Enter the default gateway of the subnet and click on OK . <div data-bbox="500 415 1295 751" style="text-align: center; border: 1px solid gray; padding: 10px; margin: 10px auto; width: fit-content;"> </div>
10.	Select the Deception tab. Set Deception Mode to On . <div data-bbox="326 898 1471 1713" style="text-align: center; border: 1px solid gray; padding: 10px; margin: 10px auto; width: fit-content;"> </div>

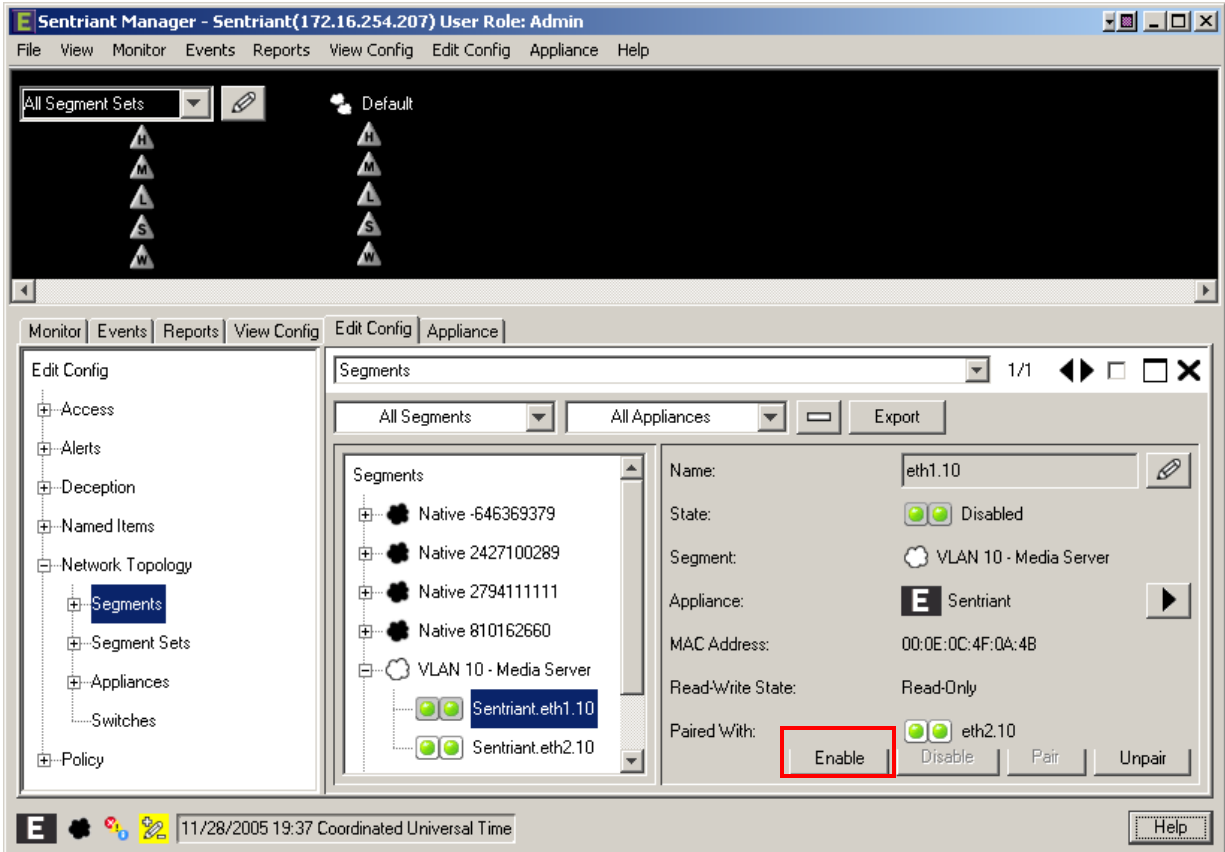
Step

Description

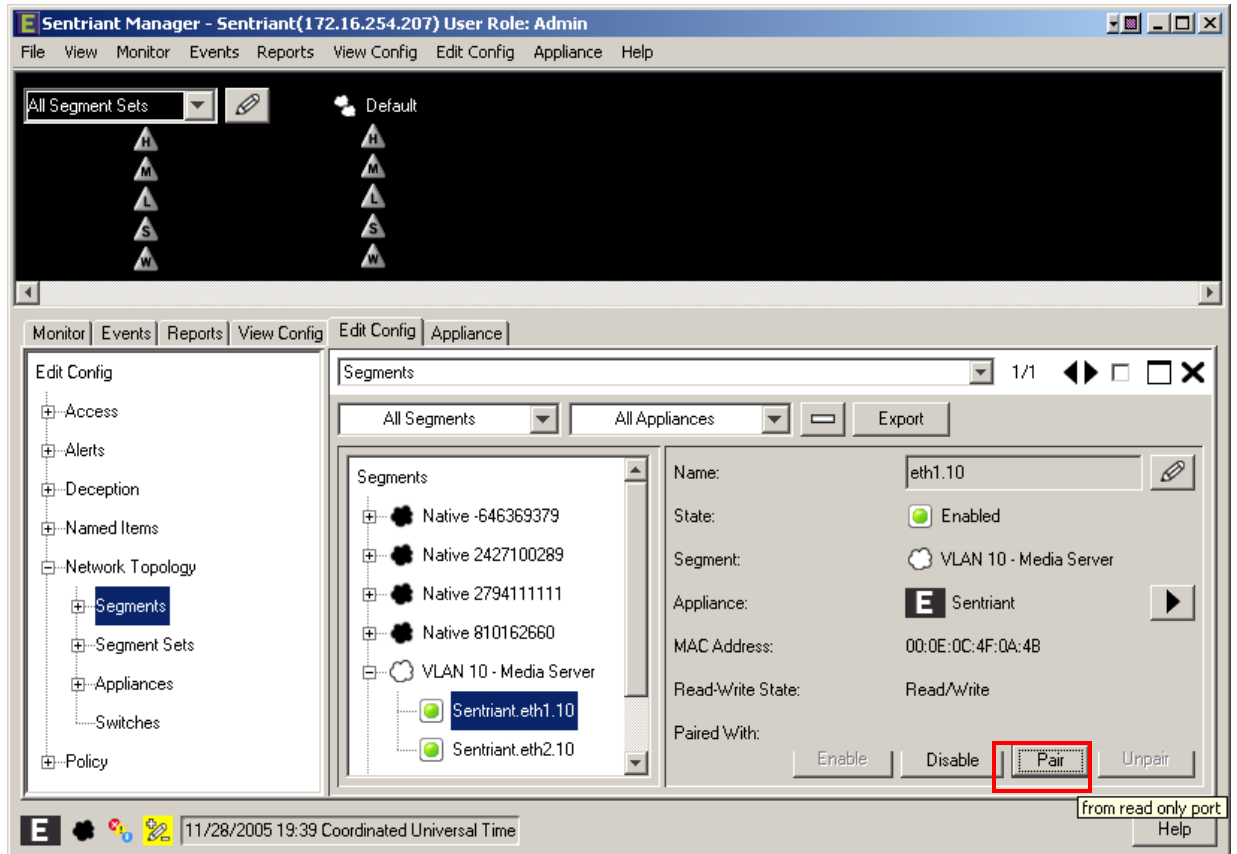
11. Click the **Cloak** tab and retain the default value **On Demand** for the **Cloak** field.



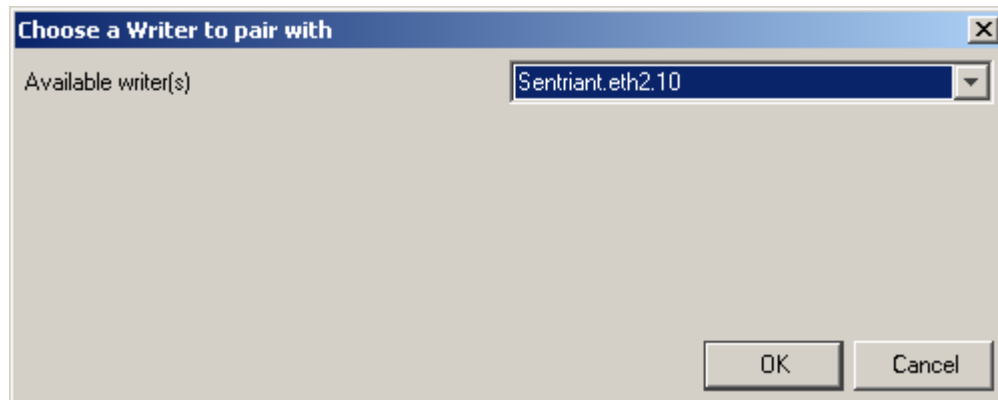
Step	Description
12.	<p>Select the Advanced tab. Set MAC Validation to On.</p> <p>Note: MAC validation is required in order to detect spoofing.</p> 

Step	Description
13.	<p>Expand the VLAN tree and select one of the two interfaces. These two VLAN interfaces reside on the two ports connected to the Extreme BlackDiamond Switch. Click on the Enable tab. Repeat this step for the other interface.</p>  <p>The screenshot shows the Sentriant Manager interface with the following details:</p> <ul style="list-style-type: none"> Browser title: Sentriant Manager - Sentriant(172.16.254.207) User Role: Admin Navigation tabs: Monitor, Events, Reports, View Config, Edit Config, Appliance, Help Left sidebar: Edit Config menu with options like Access, Alerts, Deception, Network Topology, Segments (selected), Segment Sets, Appliances, Switches, and Policy. Main content area: Segments configuration for 'eth1.10'. <ul style="list-style-type: none"> Name: eth1.10 State: Disabled Segment: VLAN 10 - Media Server Appliance: Sentriant MAC Address: 00:0E:0C:4F:0A:4B Read-Write State: Read-Only Paired With: eth2.10 Buttons: Enable (highlighted), Disable, Pair, Unpair Bottom status bar: 11/28/2005 19:37 Coordinated Universal Time

Step	Description
14.	Select one of the interfaces and click on the Pair button. This will make the “Read” port pair to “Write” port.



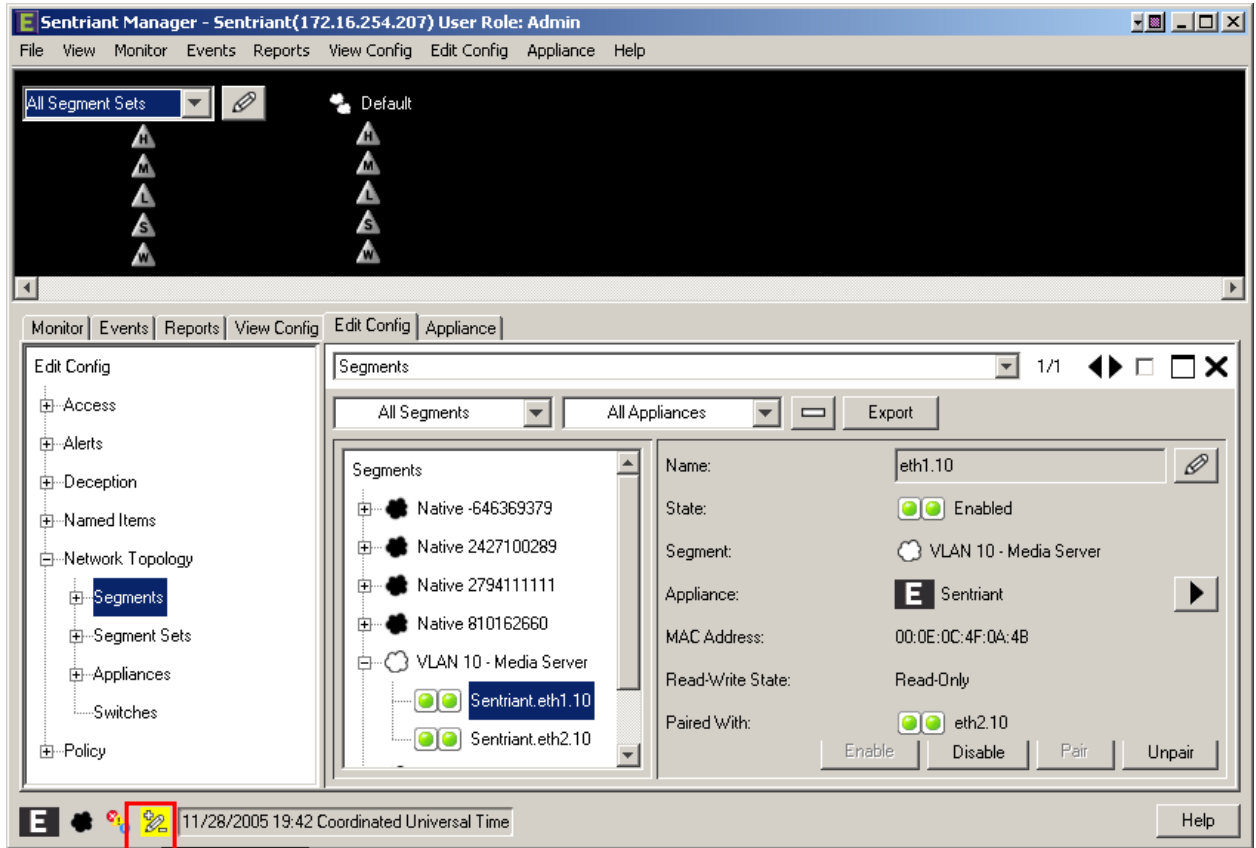
15.	Select the other interface from the pull-down list and click on OK .
-----	---

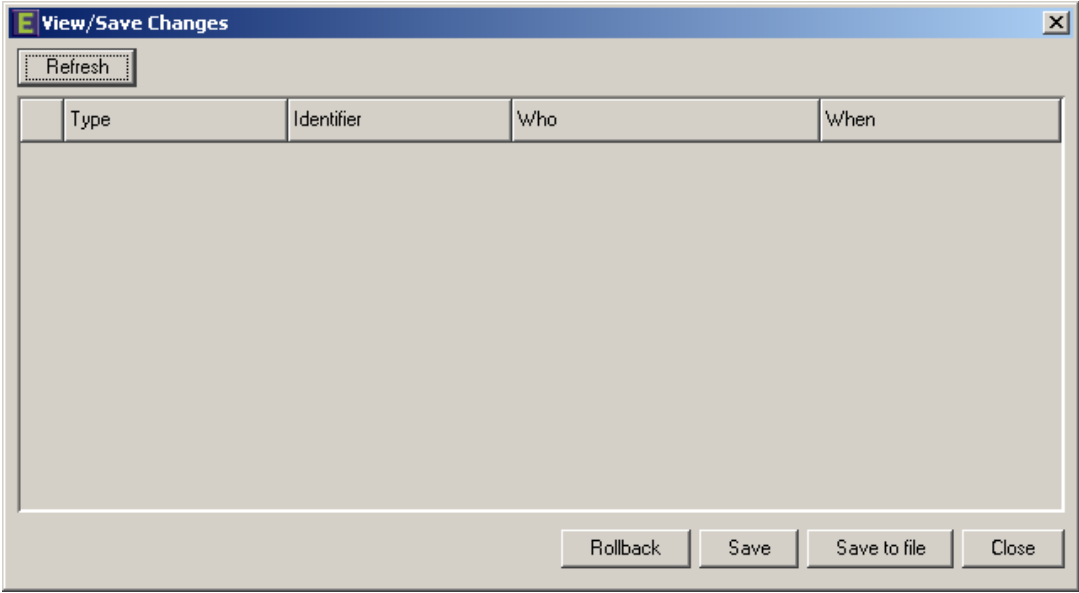


Step

Description

16. Click on the **Configure Changes** icon on the bottom left of the Sentriant Manager main window.



Step	Description
17.	<p>Click on “Save” and then “Close”.</p> 
18.	<p>Repeat Step 2 – 17 as necessary to protect other VLANs. In this configuration, the steps were repeated for VLAN 20 (Voice VLAN).</p>

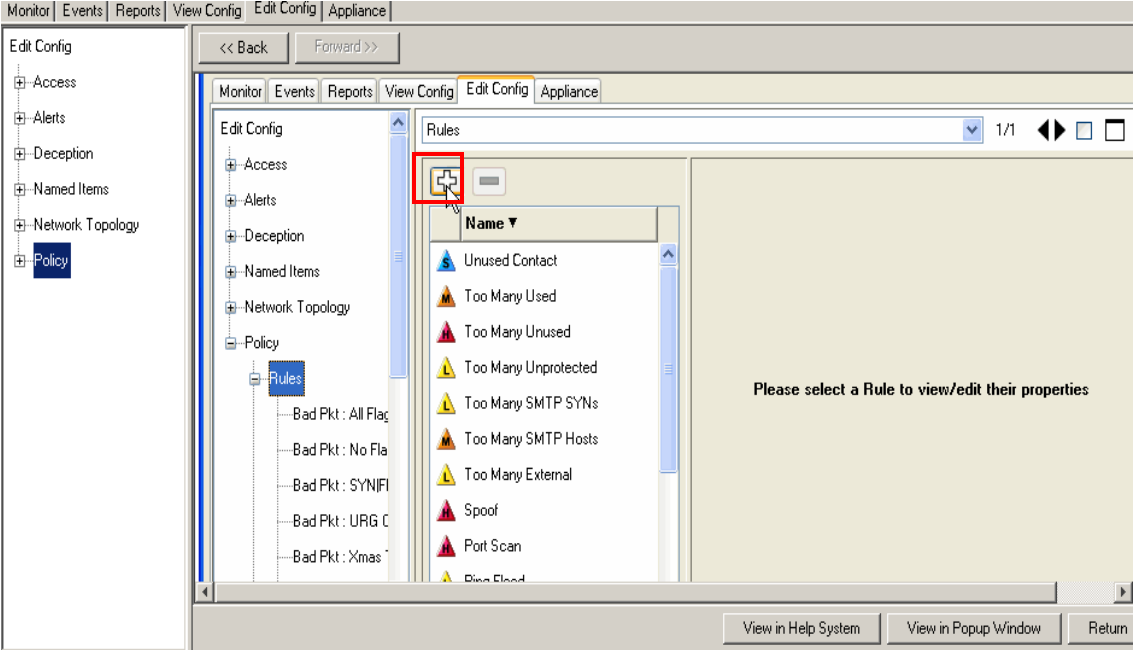
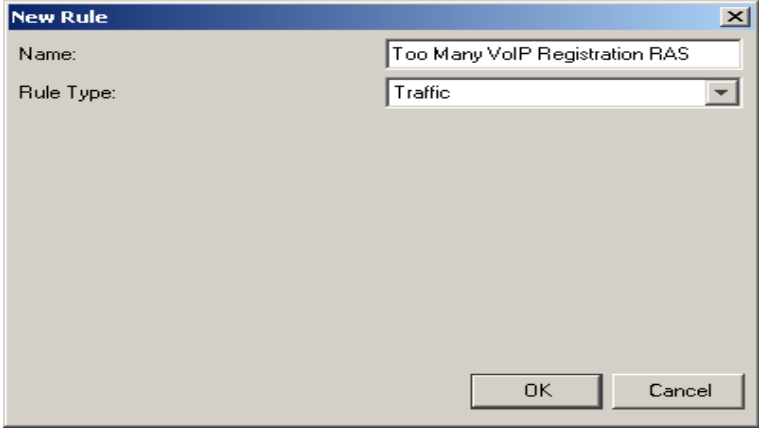
3.1. Configure Rules on Sentriant Security Appliance

Rules are what drive the Detection and Response actions of the Sentriant appliance. Once a segment is configured and is being monitored by the Sentriant appliance, Rules must be assigned before mitigation actions are in effect. There are two components to a rule:

Detection - used to detect malicious network behavior.

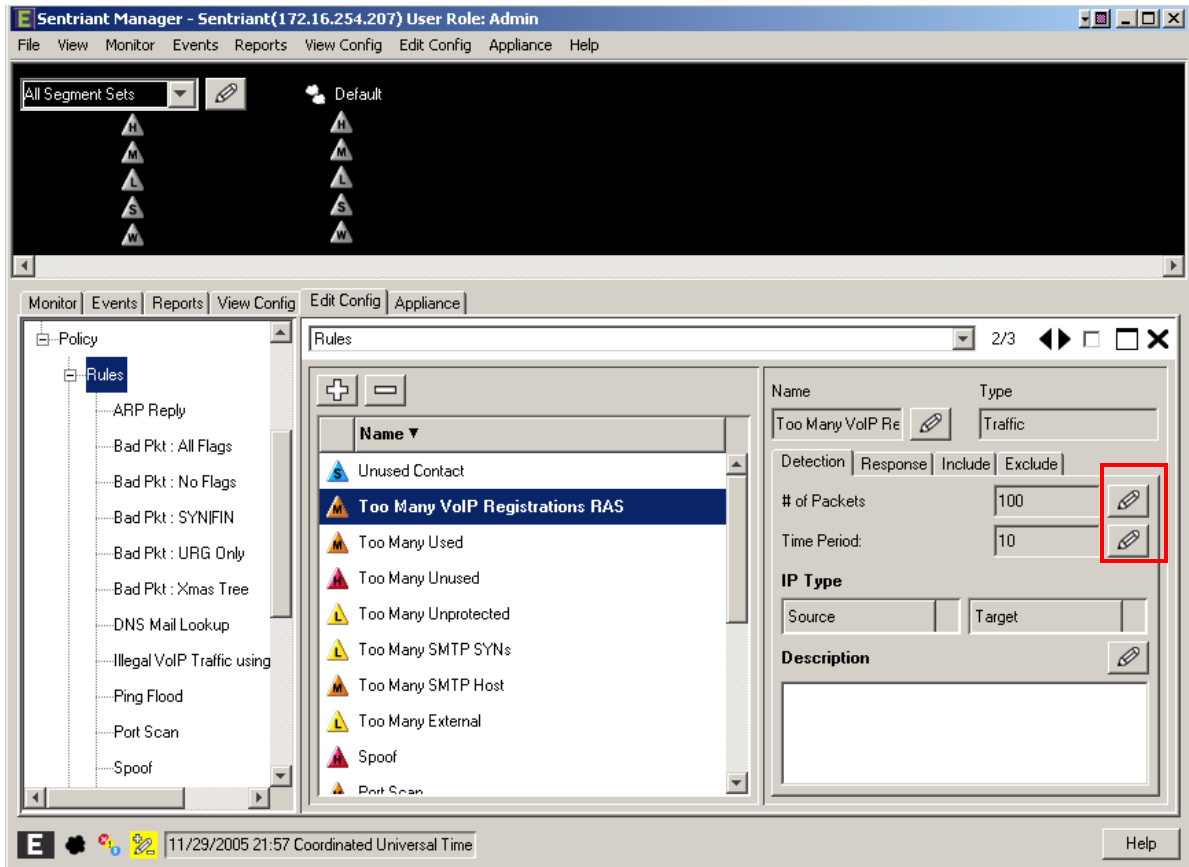
Response - action(s) taken by the Sentriant appliance will take to mitigate malicious network behavior.

A variety of rules can be defined based upon a set of predefined Rule Types. Each rule type represents a different behavioral pattern that can be detected by Sentriant. For detailed rule types, refer to the reference section in this document. In this configuration, a sample rule for H.323 RAS protocol protection is created.

Step	Description
<p>1.</p>	<p>To create a Rule:</p> <ul style="list-style-type: none"> From Edit Config > Network Topology > Policy, click on Rules in the Navigation Panel. Click the “+” icon to add a new rule. 
<p>2.</p>	<ul style="list-style-type: none"> Type the name of the new rule in the Name field. From the Rule Type drop down list, select the rule type. Click OK. 

Step	Description
------	-------------

3.	<p>Click the Detection tab and modify the # of Packets and Time Period. In this configuration, 100 RAS packets in 10 seconds period are selected since there are only two IP telephones in network. These two perimeters must be adjusted according to the number of IP endpoints in the network. The number of RAS packets defined by the rule must be greater than the number of total RAS packets generated by IP endpoints.</p>
----	--

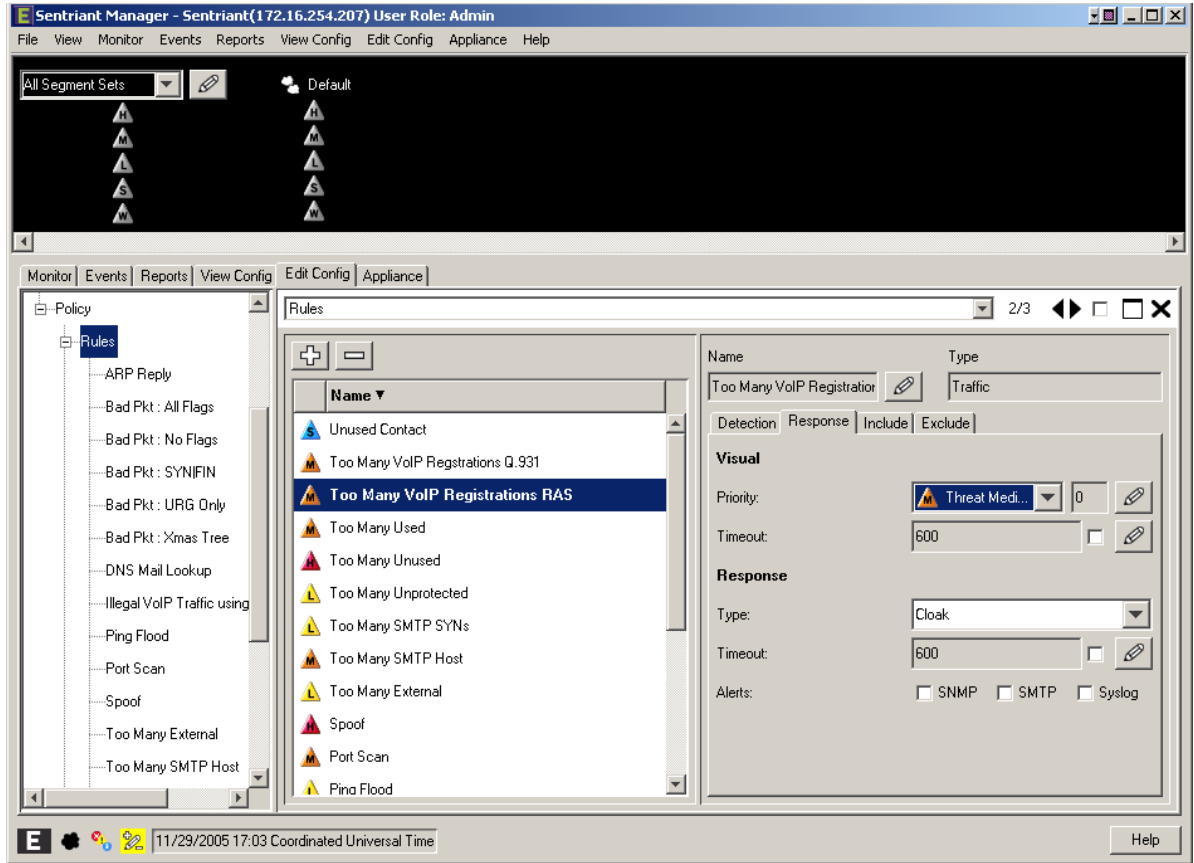


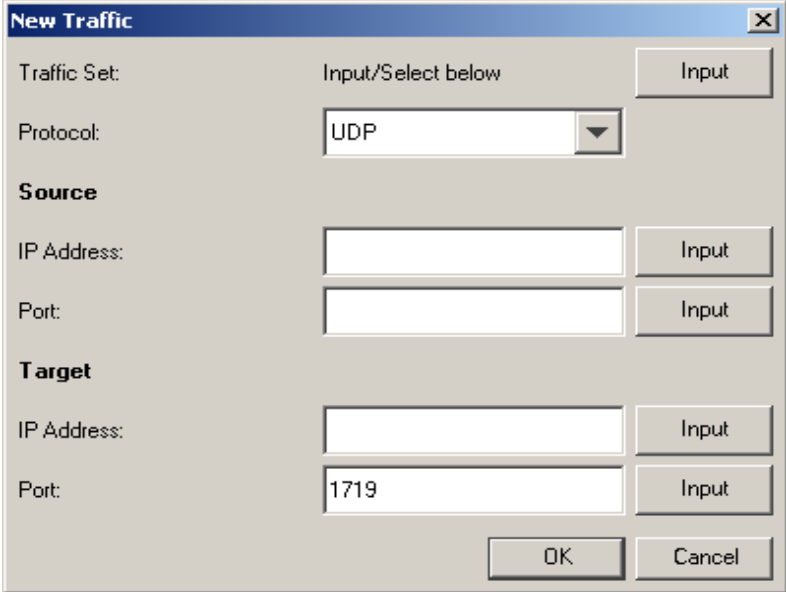
Step

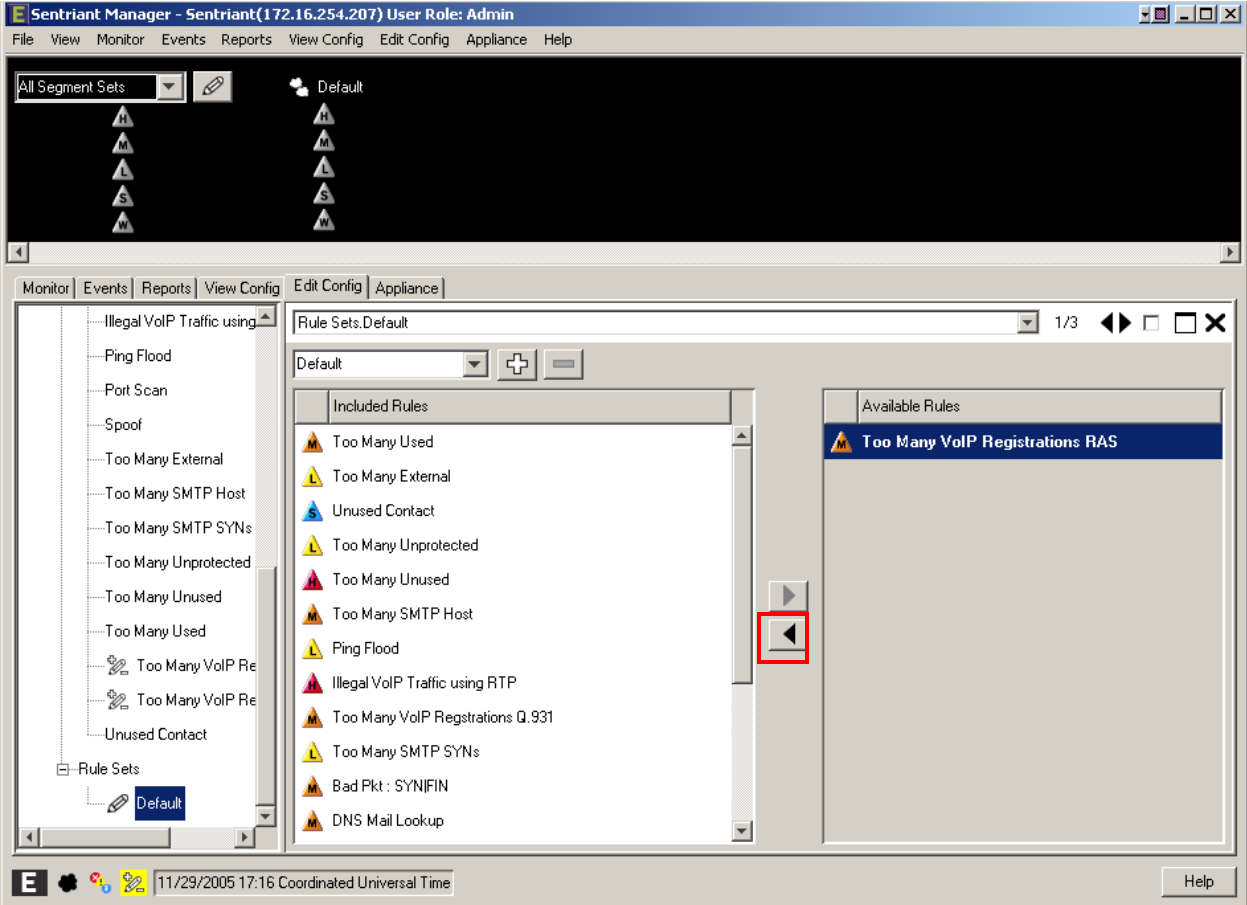
Description

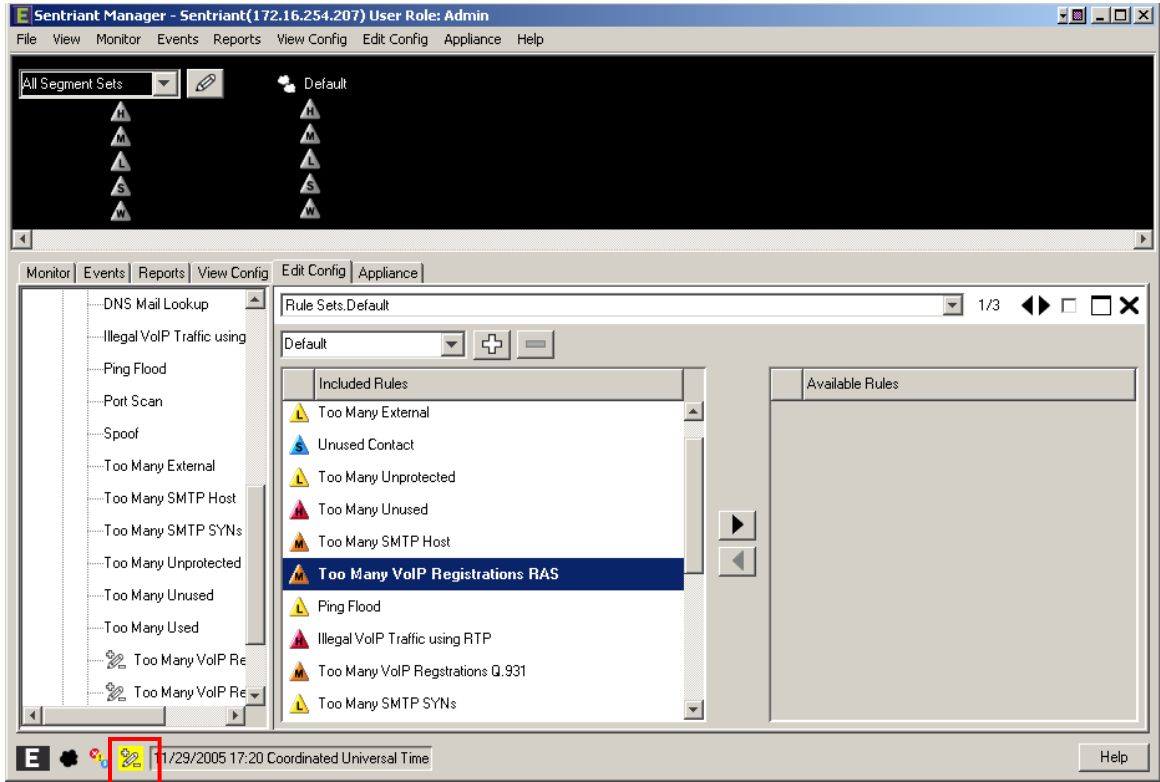
4.

- Click the **Response** tab and select **Threat Medium** from the **Priority** drop down menu.
- Select **Cloak** in the **Type** field.



Step	Description
5.	<ul style="list-style-type: none"> Click the Include tab and select the “+” icon. Select Protocol UDP. Enter 1719 in the Port field under Target. Click OK. 

Step	Description
6.	<p>A Rule Set is added to each Segment Set allowing for the best detection possible based on the type of network segment configuration. When a rule is triggered by a source threat, deception, alerts and cloaking activities are activated.</p> <p>In this configuration, the default rule set is used for protection.</p> <ul style="list-style-type: none"> • From Edit Config > Network Topology > Policy, click on Rule Sets in the Navigation Panel. • Select Rule Set Default. • Select Too Many VoIP Registrations RAS under Available Rules. • Click the right arrow to add this rule into Default rule set. 

Step	Description
7.	<p>Click on the Configure Changes icon on the bottom left of the Sentriant Manager screen.</p> 

Follow steps 1-7 to create other customized rules if needed.

4. Configure Extreme BlackDiamond 10K Switch

This section describes the steps on the Extreme BlackDiamond 10K for configuring the VLAN, port mirroring and Clear-Flow feature for the two ports connected to the Extreme Networks Sentriant.

Step	Description
1.	<p>From the Extreme BlackDiamond 10K Command Line Interface (CLI), assign the protected VLANs (10 and 20 in the sample configuration) to the two ports connected to the Sentriant appliance, and configure the ports as trunk ports with 802.1q encapsulation.</p> <pre>create virtual-router "VR-Default" configure vr VR-Default add ports 1:1-60 # Create VLAN core for S8300 Media Server create VLAN "core" configure VLAN core tag 10 configure VLAN core qosprofile QP7 # Create VLAN voice for Avaya IP Telephones create VLAN "voice" configure VLAN voice tag 20 configure VLAN voice qosprofile QP7 # Create VLAN data (unprotected VLAN) for PCs create VLAN "data" configure VLAN data tag 30 configure VLAN data qosprofile QP1 # Add ports to VLANs configure VLAN core add ports 1:3 tagged configure VLAN core add ports 1:5-10 tagged configure VLAN voice add ports 1:3, 1:11-16 tagged configure VLAN voice add ports 1:17-25 untagged # Assign IP address to VLAN interfaces and enable IP forwarding on these # interfaces. configure VLAN Mgmt ipaddress 172.16.254.58 255.255.255.0 configure VLAN core ipaddress 10.4.4.1 255.255.255.0 enable ipforwarding VLAN core configure VLAN voice ipaddress 20.1.1.1 255.255.255.0 enable ipforwarding VLAN voice configure VLAN data ipaddress 30.1.1.1 255.255.255.0 enable ipforwarding VLAN data</pre>

Step	Description
2.	<p>Configure a monitor session to mirror all VLAN traffic from the protected VLANs to the port in Step 1 connected to the “Reader” port on the Sentiariant.</p> <pre data-bbox="277 338 1523 464"> # Mirroring configuration. Port 1:2 (Read Only), Port 1:3 (Read/Write). enable mirroring to port 1:2 tagged configure mirroring add port 1:3 </pre>
3.	<p>Configure an access list for the protected VLAN and enable CLEAR-Flow on the switch.</p> <pre data-bbox="277 569 1523 823"> # Enable CLEAR-Flow on Extreme Switch and configure Module acl for protected # VLANs. configure access-list universal3 VLAN "core" configure access-list universal3 VLAN "voice" enable clear-flow </pre>

5. Interoperability Compliance Testing

The interoperability compliance testing focused on verifying that the Extreme Networks Sentiariant detected basic ping, port scans and H.323 RAS attack defined by special rule, as well as mitigated basic Denial of Service (DoS) attacks.

5.1. General Test Approach

The general approach was to launch ping scans on the protected VLANs, and port scans, H.323 RAS attacks, and basic DoS attacks on the Avaya S8300 Media Server, as well as the Avaya IP Telephones. The main objectives were to verify that:

- Sentiariant correctly detects basic ping, TCP SYN, and UDP scans on protected subnets.
- Sentiariant correctly detects H.323 RAS attacks against the Avaya S8300 Media Server
- Sentiariant correctly detects basic DoS attacks, such as ping, TCP SYN/FIN, and UDP floods, against the Avaya S8300 Media Server and the Avaya IP Telephones.
- Sentiariant cloaks (mitigates) the basic DoS attacks.
- Avaya IP Telephones on the protected subnets successfully establish and maintain calls during the basic scan and DoS attack activity.
- Avaya IP Telephones on the protected subnets successfully establish and maintain calls when there is no scan or DoS attack activity.

5.2. Test Results

The test objectives of Section 5.1 were verified. The Sentiariant was able to detect the basic ping and port scans as well as H.323 RAS attacks, and mitigate basic non-spoofed DoS attacks generated by the attacker PC.

6. Verification Steps

The following steps may be used to verify the configuration:

- From the attacker PC, run ping scans on the protected subnets and verify that the Sentiariant correctly reports the scans.
- From the attacker PC, run port scans on specific targets in the protected subnets and verify that Sentiariant correctly reports the scans.
- From the attacker PC, run UDP traffic to port 1719 on the Avaya S8300 Media Server and verify that Sentiariant correctly cloaks the traffic with the configured rule.
- From the attacker PC, send basic ping and port floods to specific targets in the protected subnets. Verify that one or more Sentiariant rules are triggered and the Sentiariant correctly reports the attack. If “Cloaked” is reported as the response(s) for the triggered rule(s), verify that the ARP tables of the source, target, and/or Extreme BlackDiamond switch have been changed such that the attack communication streams are redirected to Sentiariant. If “Tracked” is reported as the response(s) for the triggered rule(s), then perform a manual cloak operation and verify the ARP tables as per above.

7. Support

For technical support on the Extreme Networks Sentiariant, consult the support pages at <http://Extremenetworks.com/support.html> or contact Extreme Networks customer support at:

- Phone: 866.869.6767
- E-mail: support@Extremenetworks.com

8. Conclusion

These Application Notes described a configuration where the Extreme Networks Sentiariant security appliance protects the subnets where an Avaya Media Server and Avaya IP Telephones reside against rapidly propagating threats. During compliance testing, the Sentiariant detected basic ping and port scans that often precede threats on the protected subnets, and mitigated basic Denial of Service (DoS) attacks against the aforementioned Avaya IP telephony endpoints.

9. Additional References

[1] Administrator Guide for Avaya Communication Manager - Release 3.0/3.0.1.

<http://support.avaya.com/japple/css/japple?temp.documentID=232034&temp.productID=136527&temp.releaseID=228560&temp.bucketID=159898&PAGE=Document>

[2] Sentriant Manager 2.2 User Guide.

http://www.extremenetworks.com/services/documentation/Sentriant_UG.pdf

©2006 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.