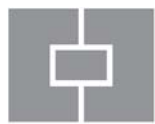


SOPHOS



sophos **nac**

ADVANCED

Integration with IP Phones



Copyright © 2010 Sophos Limited. All rights reserved. No part of this publication may be reproduced, stored in retrieval system, or transmitted, in any form or by any means electronic, mechanical, photocopying, recording or otherwise unless you are either a valid licensee where the documentation can be reproduced in accordance with the licence terms or you otherwise have the prior permission in writing of the copyright owner.

Sophos and Sophos Anti-Virus are registered trademarks of Sophos Limited. All other product and company names are trademarks or registered trademarks of their respective owners.

Document version 3.2
Published December 2010

Table of Contents

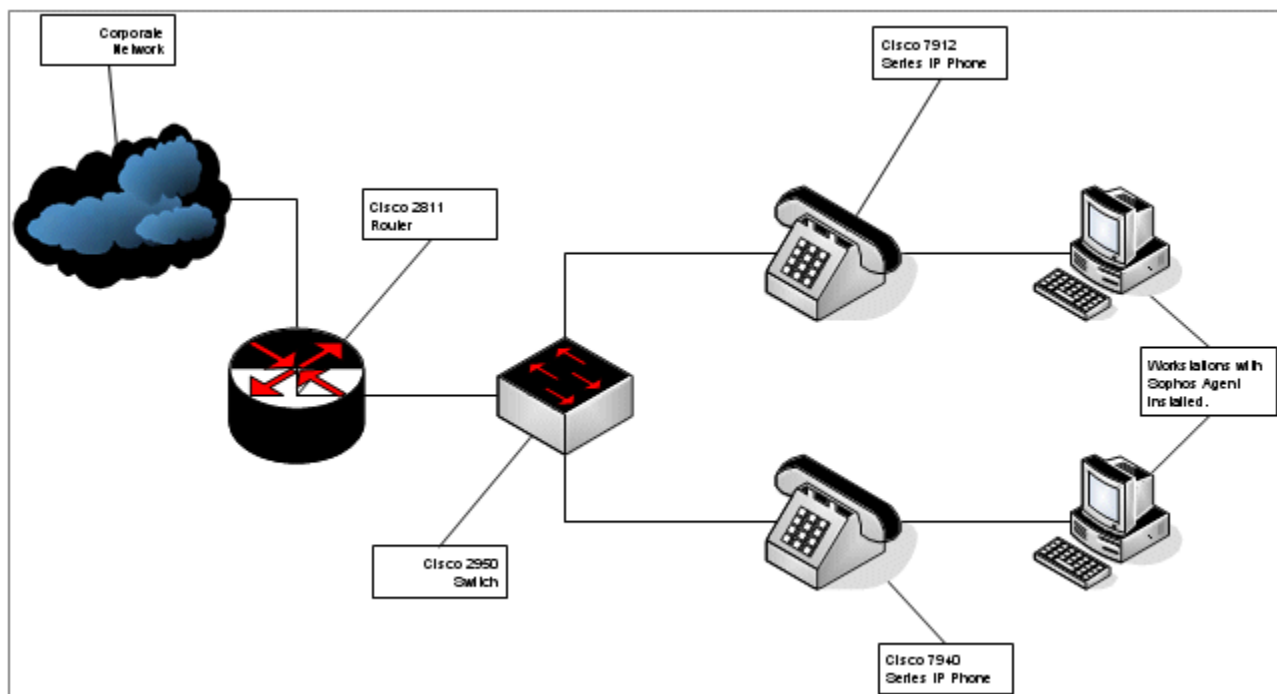
Sophos NAC Advanced Integration with IP Phones.....	4
Configuring the Network to Support IP Phones and Sophos NAC Advanced	4
Configuring Sophos NAC Advanced to Support IP Phones.....	5
Operating the Endpoints and IP Phones	6

Sophos NAC Advanced Integration with IP Phones

This document provides information on integrating Sophos NAC Advanced with a network where endpoints are connected through switches imbedded in IP phones. The IP phone models for this test are the Cisco® 7912 and 7940.

The key to the integration is to set up separate VLANs and use 802.1x authentication with RADIUS to access the separate VLANs based on compliance. While Cisco equipment was used for the purposes of this testing, other equipment that support 802.1x and RADIUS authentication are also supported with Sophos NAC Advanced.

The following diagram displays a simplified view of the configuration that is used:



Important: This configuration ensures that the IP phones will work regardless of which VLAN the endpoint has access to or whether the endpoint is turned off. More importantly, all voice traffic is shuttled to VLAN 100, which is not used by Sophos NAC Advanced.

Configuring the Network to Support IP Phones and Sophos NAC Advanced

This configuration requires running Cisco Call Manager (v3.0 or above) on the 2811 router. Call Manager supports configuration and administration of the IP phones that are connected to the network.

Three VLANs must be created: one dedicated to voice, one for Sophos permitted access, and one for Sophos denied access. This test uses the following VLANs:

VLAN	Purpose
VLAN 100	Voice
VLAN 102	Permit access
VLAN 103	Deny access

The ports on the switch must be configured to carry traffic from a voice VLAN. To do this, type the following command for each port while in privileged EXEC mode:

```
switchport voice vlan <vlan-id>
```

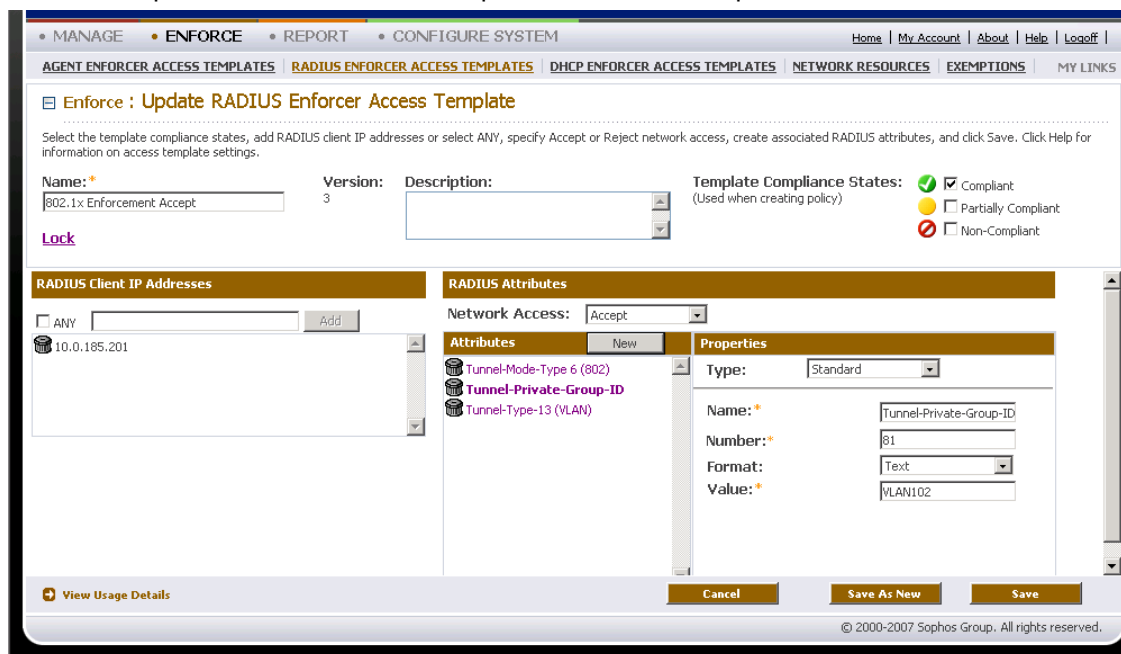
The specified VLAN then supports **all** voice traffic from the IP phone, while data traffic is carried on one of the other two VLANs. This configuration ensures that voice traffic on the IP phone is always available, even if Sophos NAC Advanced determines that the endpoint is not compliant with the defined security policy.

Configuring Sophos NAC Advanced to Support IP Phones

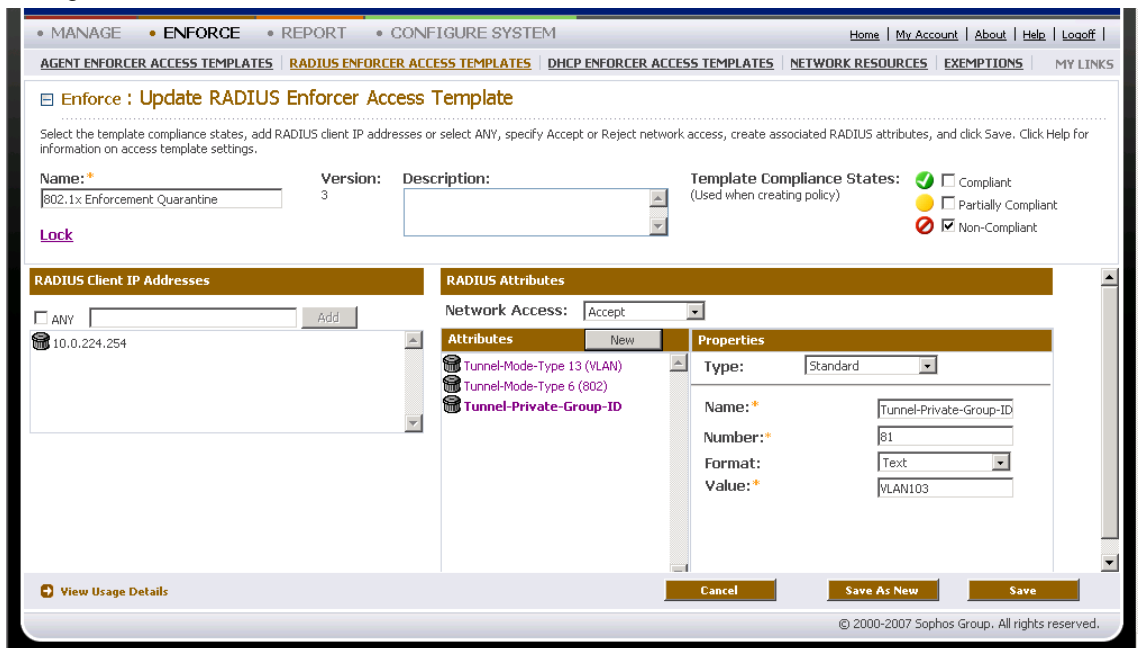
The Sophos Compliance Application Server must have a RADIUS compliance setting to support the other two VLANs (102 and 103 in this case). For more information on configuring dynamic VLANs for 802.1x authentication, see the *802.1x Dynamic VLAN Assignment* document located on the Sophos web site:

http://www.sophos.com/sophos/docs/eng/manuals/nacadv8021x_32_tgeng.pdf

Using the Sophos Compliance Manager, create a new RADIUS setting with the **IP address** pointing to the switch. For this test, the Cisco 2950 switch is used. The following Tunnel-Private-Group-ID attribute will send data traffic from the endpoint to VLAN 102 when Sophos NAC Advanced permits access.



Setting up the Deny Attribute involves specifying the **deny VLAN** in the Tunnel-Private-Group-ID deny attribute, as follows. Once the permit and deny attributes are specified, click the **Save** button to create and save these RADIUS settings.



Operating the Endpoints and IP Phones

If you experience problems getting the Compliance Agent to work behind the phone using 802.1x, do the following:

1. Plug the computer directly into the 802.1x-enabled port and confirm that it authenticates without the phone.
2. Set up the phone on the switch (make sure you have added that port to the voice VLAN) and confirm that it connects without issue.
3. Plug the computer into the switch port on the phone and try to get connected using the desired supplicant.
4. If you still aren't being authenticated, packet sniff the subnet to confirm that RADIUS protocol packets are being sent.
5. Open up the Event Viewer on the Compliance Application Server and go to the system logs. If you see Internet Authentication Service (IAS) or Network Policy Server errors (depending on operating system), then you know that the request is passing all the way to the server, at which point the server will issue a permit or deny entry in the logs.
6. If you are being granted access with RADIUS but still aren't able to log in with the Compliance Agent, go into the switch and see what error messages are generated during the authentication. If there is a problem with the RADIUS attributes or with your VLAN naming convention, you will see these errors on the switch.
7. If you still are unable to register or retrieve your policy, enable client logging (right-click the Agent system tray icon, select About Sophos Network Access Control, and then select the Enable Logging check box to enable client logging.) Once enabled, check for endpoint compliance (right-click the Agent system tray icon, and select Check Compliance). Then, open c:\program files\endforce\log\ and locate the trace log for your session to view errors. Any errors that are occurring will be listed there for further troubleshooting.

The endpoints must access the appropriate VLAN, VLAN 102, or VLAN 103, depending on compliance, by initiating the Sophos Agent and an 802.1x supplicant on the endpoint. For more information on this process, see the *802.1x Dynamic VLAN Assignment* document located on the Sophos web site:

http://www.sophos.com/sophos/docs/eng/manuals/nacadv8021x_32_tqeng.pdf