

SOPHOS



sophos **nac**

ADVANCED

Configuring Cisco ASA to integrate with
Sophos NAC Advanced



Copyright 2009 Sophos Group. 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 license terms or you otherwise have the prior permission in writing of the copyright owner.

All other product and company names are trademarks or registered trademarks of their respective owners.

Document version 3.2
Published May 2009

Table of Contents

Configuring Cisco ASA to integrate with Sophos NAC Advanced	4
Integration Overview.....	4
Step One: Configure the ASA to use the Compliance Application Server (RADIUS).....	5
Step Two: Define a Tunnel Group and its Authentication Type	5
Step Three: Create your Access Lists.....	6
Step Four: Configure VPN Restrictions.....	6
Step Five: Configure IAS to accept the ASA connections.....	7
Step Six: Test/Troubleshooting	8
Appendix A: Sample Configuration.....	10

Configuring Cisco ASA to integrate with Sophos NAC Advanced

This document outlines the steps necessary to implement VPN/RADIUS integration using the Cisco Adaptive Security Appliance (ASA) and Sophos NAC Advanced. The steps outlined for this integration utilize the ASA command line, which can be accessed using HyperTerminal with a console cable. This document was created with Cisco ASA 5505 running version 7.2 (4), Device Manager version 5.2(4).

The steps in this document show you how to configure the ASA for integration with NAC Advanced. The following is assumed about the existing VPN environment:

- You are running Cisco Adaptive Security Appliance Software version 7.x. If you are running an older version, it is possible that it will not support the features defined in this document or may implement them differently.
- You have existing knowledge of the ASA command line interface and access lists.
- Your ASA is already set up and working with a regular VPN configuration.
- You have an installed/working configuration of the NAC Advanced software.
- You have a working Active Directory/LDAP Store that is also working with NAC Advanced.

Integration Overview

NAC uses the username for compliance lookups to determine what response to send back to the ASA/VPN server. This username is entered when the Compliance Agent is registered, and every time the Agent performs an assessment on the user's machine, the compliance state is reported up to the Compliance Application Server. It is this compliance state that determines what attributes a user will receive during the VPN login process. Since the compliance state is determined during the VPN login, it is necessary for users to log off and then log on to the VPN again if they were first considered to be "non-compliant" with policy at the time of login and have become "compliant" with policy after login.

Note: Since the username is the criteria used for compliance state lookups, the username that is entered into the Compliance Agent must be the same username (identical format) that is used for the VPN login. If the two do not match, then NAC will apply the same enforcement options as for a non-compliant user.

ASA with NAC Advanced integration has four different options for controlling access using VPN enforcement. You can determine your preferred method of enforcement based on the following options:

1. **Basic Authentication:** This method is used when the administrator does not want to limit a non-compliant user's access to the network, and simply wants to block access to all non-compliant users and allow full access to compliant users. This method is the simplest to set up, as it only requires that the ASA forward the authentication traffic to the Compliance Application Server.
Note: This method should also work with any other VPN solutions that allow RADIUS authentication.
2. **Filter-ID:** These are access lists that are already defined on the ASA. By using this method, NAC would define which access lists to apply to a user when they are compliant, partially compliant, or not compliant with NAC policy. This method provides a very basic way to control a user's access with ACLs.
3. **Group Policy:** Group Policies are a collection of user-oriented attribute/value pairs that can be applied to a Tunnel-Group. NAC utilizes Internal Group Policies, which can define such things as tunneling protocols, access lists, access hours, idle timeout, DNS, WINS and DHCP scopes, banners, default domain, and much more. This option is recommended for administrators who want the ability to control a wide range of options when quarantining users.
4. **Downloadable Access Lists:** Downloadable ACLs allow you to create custom access lists through the Compliance Manager to be applied to users in their various compliance states. By using this feature, you can periodically update ACLs for different compliance states without modifying the configuration on the Cisco ASA. Note that if you incorrectly type an ACL statement (such as *permit ip any any any*), then the user will not be

allowed to log on since the ASA will not know how to interpret the ACL and the default will be set to Deny All traffic. For this reason, it is important to test that the new or updated ACL is working as expected prior to putting it into a production NAC policy. This method provides a way to quickly update ACLs without having to log on to the ASA.

Note: These enforcement methods are definable for each NAC policy and each compliance state in NAC, and through Tunnel-Groups on the ASA. For example, if you had the CEO assigned to the Executives group within NAC that had a corresponding policy, then you could set up the policy to never assign any of the above enforcement methods, or you could simply have all of the executives' VPN configurations set to use a different Tunnel-Group that does not have enforcement options applied to it.

Step One: Configure the ASA to use the Compliance Application Server (RADIUS)

The ASA must be configured to point to the Compliance Application Server for Authentication, Authorization, and Accounting (AAA – RADIUS) so that users can be authenticated and their policy compliance state can be confirmed. At this stage, NAC will send back a response based upon the compliance state associated with the username.

Note: The commands used in this document are based on a sample configuration. For more information, see **Appendix A: Sample Configuration on page 10**. You must test your solution before deploying it in a production environment. The commands are in **RED** and the comments for the commands are in **GREEN**. Some of the commands are displayed on a second line because of space constraints.

1. Log on to the ASA, create a AAA Server group called "RADIUS".
2. Specify the protocol as RADIUS.
3. Specify the IAS/RADIUS Server with the interface it is located on (inside or outside) as a member of the "RADIUS" group, and provide the location and shared secret. The interface is the IP address of the Sophos Compliance Application Server.

```
aaa-server RADIUS protocol radius  
aaa-server RADIUS host 10.0.224.150 (IP address of the Compliance Application Server)  
key cisco123 (shared secret that will be used for the transaction)
```

Step Two: Define a Tunnel Group and its Authentication Type

The default Tunnel Group of DefaultRAGroup is used in this example. The Tunnel Group is the group that the user will be using in the VPN client to log on to the ASA. If there are other groups that have been created, such as Sales, Marketing, etc., configure these groups in the same manner:

1. Since you are using the DefaultRAGroup as the VPN Group that you want to enforce, configure that group to use the RADIUS pool that you created in **Step One**:

```
tunnel-group DefaultRAGroup general-attributes (modify the DefaultRAGroup Tunnel Group)  
authentication-server-group RADIUS (enable Authentication using RADIUS)  
authorization-server-group RADIUS (enable Authorization)  
accounting-server-group RADIUS (enable Accounting)
```

The Basic Authentication enforcement method is fully configured now that the RADIUS Server/Tunnel Groups have been created in **Step One** and **Step Two**. If you planned on using this enforcement method, your setup for the ASA is complete, and you can continue with **Step Five: Configure IAS to accept the ASA connections on page 7**.

Note: If you want to allow non-compliant users to log on to the VPN and then restrict their access to network resources, continue with **Step Three: Create your Access Lists on page 6**. The Basic Authentication enforcement method will only allow or deny a user's access based on whether they are compliant or non-compliant with the associated policy.

Step Three: Create your Access Lists

If you plan on using any enforcement method other than Basic Authentication (option 1), you must create access lists to define the network locations your users can access when they are in a compliant or non-compliant state.

1. If you plan to use enforcement methods 2 or 3 (Filter ID, Group Policy), then you must define the access lists (ACLs) on the ASA. You do not need to define ACLs here with enforcement method 4 (Downloadable Access Lists). This example creates an ACL for port 80 (Internet) traffic only:

access-list acl_http_only permit tcp any any eq www (create the ACL)

Step Four: Configure VPN Restrictions

You must decide which of the four enforcement methods you wish to use with NAC: Basic Authentication, Filter-ID, Group Policy, and Downloadable Access Lists. The option you plan to use corresponds with and determines which of the following procedures you should follow:

Basic Authentication Enforcement

1. Go to **Step Five: Configure IAS to accept the ASA connections on page 7** since the default RADIUS Enforcer access templates within the Compliance Manager are already configured for this method.

Filter-ID Enforcement

1. Log on to the Compliance Manager and click **Enforce > RADIUS Enforcer Access Templates**.
2. Click the **Default – RADIUS Reject All** template.
3. Click the **Network Access** list box, and change its value from “Reject” to “Accept”.
4. Click **New** to create a new attribute, and specify the following properties:
 - **Type:** Standard
 - **Name:** Filter-ID
 - **Number:** 11
 - **Format:** Text
 - **Value:** acl_http_only

Note: This value is the name of the ACL that you created in **Step Three**.

Group Policy Enforcement

1. Configure the ASA with the following:
 - ip local pool quarantine 192.168.1.201-192.168.1.253 (address pool for quarantine users)*
 - group-policy QuarantineGroupPolicy internal (create an internal Quarantine Group Policy)*
 - group-policy QuarantineGroupPolicy attributes (define the Group Policy attributes)*
 - vpn-filter value acl_http_only (define the Group Policy's ACL)*
 - default-domain value quarantine.com (define the default domain)*
 - address-pools value quarantine (use the quarantine pool created above)*
2. Log on to the Compliance Manager and click **Enforce > RADIUS Enforcer Access Templates**.
3. Click the **Default – RADIUS Reject All** template.
4. Click the **Network Access** list box, and change its value from “Reject” to “Accept”.
5. Click **New** to create a new attribute, and specify the following properties:
 - **Type:** Standard

- **Name:** Filter-ID
- **Number:** 25
- **Format:** Text
- **Value:** QuarantineGroupPolicy

Note: This value is the name of the ACL that you created in **Step Three**.

Downloadable ACL Enforcement

You must define the ACLs in the Compliance Manager in order to apply them to the user when they are non-compliant with NAC policy:

1. Log on to the Compliance Manager and click **Enforce > RADIUS Enforcer Access Templates**.
2. Click the **Default – RADIUS Reject All** template.
3. Click the **Network Access** list box, and change its value from “Reject” to “Accept”.
4. Click **New** to create a new attribute, and specify the following properties:
 - **Type:** Vendor-Specific
 - **Name:** Cisco-AV-Pair
 - **Number:** 26
 - **Vendor Code:** 9
 - **Vendor Subattribute:** 1
 - **Format:** Text
 - **Value:** ip:inacl#18=permit tcp any any eq www

Note: This value is the actual ACL. In this case, we are creating an ACL that only allows port 80 traffic. The Number (18 in this example) should be the number of an ACL that doesn’t already exist. The default final line of a downloadable ACL is “deny any any”; so, you do not have to enter this line.

You will also need to enable downloadable ACLs on the ASA:

access-group outside_access_in in interface outside per-user-override (in this example, the ACL of outside_access_in on the outside interface is applied on a per user basis)

Usage: access-group access-list {in | out} interface if_name per-user-override

Explanation:

After downloadable ACLs are accepted from a AAA server, they must be treated like any other access list and be applied to an interface. Therefore, you can use the per-user-override keyword when you apply an access list to an interface with the access-group command. Any downloadable ACLs override the contents of the existing access list for a given user. The access list statements are not replaced; however, the per-user ACL is evaluated first, ahead of the regular access list.

Note: Downloadable ACLs are active as long as the user is authenticated on the firewall. As soon as the uauth timer expires for a user, the corresponding downloadable ACL is removed. When the user initiates a new connection and authenticates again, the downloadable ACL is retrieved and put into service once more.

Step Five: Configure IAS to accept the ASA connections

For users to be authenticated through NAC, you must configure Internet Authentication Service (RADIUS) to allow the remote VPN authentications:

1. Log on to the Compliance Application Server, and select **Start > Administrative Tools > Internet Authentication Service** to open IAS.
2. Right-click the RADIUS Clients folder, and select **New RADIUS Client**.
3. Type **VPN** in the **Friendly name** field.

4. Type the corresponding IP address or DNS name of the Cisco ASA in the **Client Address (IP or DNS)** field, and click **Next**.
5. In the **Client-Vendor** list box, keep the default **RADIUS Standard** option. Then, type and confirm the shared secret that you entered in **Step One** (the example used "Cisco123"), and click **Finish**.
6. In the left navigation area, select **Remote Access Policies**. Then, right-click the corresponding policy name that will be used by the ASA (default is "Connections to other access servers"), and select **Properties**.
7. In the **Properties** window, click **Edit Profile**.
8. In the **Edit Dial-in Profile** window, click the **Authentication** tab, and select the **Microsoft Encryption Authentication version 2 (MS-CHAPv2)**, **Microsoft Encryption Authentication (MS-CHAP)**, and **Unencrypted authentication (PAP, SPAP)** check boxes if they are not already selected, and click **OK**. The ASA can use any of these methods for authentication.
9. Click **OK** to close the **Properties** window.
10. In the left navigation area, expand the **Connection Request Processing** folder, and select **Connection Request Policies**. Then, right-click the "Use Windows Authentication for all users" option, and select **Properties**.
11. In the **Properties** window, click **Edit Profile**.
12. Ensure that the **Authenticate requests on this server** option button is selected, and click **OK**.
13. Click **OK** to close the **Properties** window.
14. Exit IAS.

Step Six: Test/Troubleshooting

To confirm if your enforcement method has worked or to troubleshoot a non-working configuration, you can log on to the ASA and type the following:

show uauth username (where username is the user you are logging into the VPN with)

One of the following should display, depending on the enforcement method you are using:

Filter-ID

Using the Filter-ID enforcement method, you should see the ACL that was applied by NAC:

```

Current      Most Seen
Authenticated Users      1          1
Authen In Progress      0          0
ipsec user 'jamesbond' at 10.0.224.252, authenticated
access-list acl_http_only (*)
    
```

Group Policy

Using the Group Policy enforcement method, you should see the ACLs that were applied to your Group-Policy:

```

Current      Most Seen
Authenticated Users      1          1
Authen In Progress      0          0
ipsec user 'jamesbond' at 10.0.224.252, authenticated
access-list acl_http_only (*)
    
```

Downloadable ACL

Using the Downloadable ACL enforcement method, you should see the customized dynamically created ACL that the ASA automatically created when it received the ACL from NAC:

```

Current      Most Seen
Authenticated Users      1          1
Authen In Progress      0          0
ipsec user 'jamesbond' at 10.0.224.252, authenticated
access-list AAA-user-jamesbond-99DF0707 (*)
    
```

If you do not see the corresponding entry after configuring the desired method, then check the ASA's log using the following commands to display the Cisco Adaptive Security Device Manager's (ASDM) log of activity:

show log asdm | grep username (where username is the user you are logging into the VPN with – this will show the authentication attempts for this user)

show log asdm | grep aaa (this should show all RADIUS attempts)

show log asdm | grep aaa Marking (this should show RADIUS attempts that failed)

show log asdm | grep aaa transaction (this should show RADIUS attempts that succeeded)

show log asdm | grep aaa retrieved (this should show what RADIUS attributes were returned)

Alternatively, you can open the ASDM and view the log at the bottom of the home page, or you can click **Monitoring** (at the top), click **Logging** (bottom left), and then click **View** to view the real-time log. This method shows a much friendlier log listing; however, the ASDM can be difficult to get working properly due to Java issues.

View the Compliance Manager Troubleshooting Report

Check that the user was authenticated to Compliance Application Server:

1. Log on to the Compliance Manager.
2. Click **Report > Troubleshooting**, select **RADIUS Enforcer** from the list box, and click **Run** to display the report.
3. A list of usernames should display who has authenticated with NAC and the access template that was applied. If the "Default – RADIUS Reject All" access template was applied, then the settings you have configured should have been applied to the machine.

View the System Event Logs

You should see entries in the System Event Log showing the authentication attempts from VPN users. If you do not see these entries, then it is possible that the RADIUS Group was not configured correctly or was not applied to the Tunnel Group correctly. If you see that users are being denied access due to Connection Request Policy problems, then it is likely that PAP did not get set up as one of the allowed authentication protocols, or that the VPN users are accessing the wrong Connection Request Policy.

Appendix A: Sample Configuration

The following is the sample configuration used in the creation of this document:

```
ASA Version 7.2(4)
!
hostname ciscoasa
domain-name default.domain.invalid
enable password 8Ry2Yjlyt7RRXU24 encrypted
passwd 2KFQnbNIdl.2KYOU encrypted
names
!
interface Vlan1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
!
interface Vlan2
 nameif outside
 security-level 0
 ip address dhcp setroute
!
interface Ethernet0/0
 switchport access vlan 2
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Ethernet0/4
!
interface Ethernet0/5
!
interface Ethernet0/6
!
interface Ethernet0/7
!
ftp mode passive
dns server-group DefaultDNS
 domain-name default.domain.invalid
access-list outside_access_in extended permit ip 10.0.192.0 255.255.255.0 any
access-list 10 remark Permit All Traffic
access-list 10 extended permit ip any any
```

```
access-list ProductionNetwork_splitTunnelAcl standard permit any
access-list inside_nat0_outbound extended permit ip any 10.0.224.250 255.255.255.254
access-list inside_nat0_outbound extended permit ip any 10.0.224.252 255.255.255.254
access-list acl_http_only extended permit tcp any any eq www
access-list acl_http_only extended deny ip any any
pager lines 24
logging enable
logging asdm informational
mtu inside 1500
mtu outside 1500
ip local pool pool1 192.168.1.50-192.168.1.100
ip local pool pool2 192.168.1.101-192.168.1.200
ip local pool quarantine 192.168.1.201-192.168.1.253
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-524.bin
no asdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 0 access-list inside_nat0_outbound
nat (inside) 1 0.0.0.0 0.0.0.0
access-group outside_access_in in interface outside per-user-override
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
aaa-server RADIUS protocol radius
aaa-server RADIUS (outside) host 10.0.224.150
key password
radius-common-pw password
acl-netmask-convert auto-detect
http server enable
http 10.0.224.0 255.255.255.0 outside
http 10.0.192.0 255.255.255.0 outside
http 192.168.1.0 255.255.255.0 inside
http authentication-certificate outside
http redirect outside 80
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
crypto ipsec transform-set my-set esp-des esp-md5-hmac
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto dynamic-map dynmap 10 set transform-set my-set
crypto dynamic-map dynmap 10 set reverse-route
crypto dynamic-map dynmap 30 set pfs group1
```

```
crypto dynamic-map dynmap 30 set transform-set ESP-3DES-SHA
crypto dynamic-map dynmap 50 set pfs group1
crypto dynamic-map dynmap 50 set transform-set ESP-3DES-SHA
crypto map mymap 10 ipsec-isakmp dynamic dynmap
crypto map mymap interface outside
crypto ca trustpoint local
  enrollment self
  subject-name CN=Default Certificate
crl configure
crypto isakmp enable outside
crypto isakmp policy 10
  authentication pre-share
  encryption des
  hash md5
  group 2
  lifetime 1000
crypto isakmp policy 65535
  authentication pre-share
  encryption 3des
  hash sha
  group 2
  lifetime 86400
telnet timeout 5
ssh timeout 5
console timeout 0
management-access outside
dhcpd auto_config outside
!
dhcpd address 192.168.1.2-192.168.1.33 inside
dhcpd enable inside
!

webvpn
  svc enable
group-policy DfltGrpPolicy attributes
  banner none
  wins-server none
  dns-server none
  dhcp-network-scope none
  vpn-access-hours none
  vpn-simultaneous-logins 3
  vpn-idle-timeout 30
  vpn-session-timeout none
  vpn-filter none
  vpn-tunnel-protocol IPSec l2tp-ipsec webvpn
```

```
password-storage disable
ip-comp disable
re-xauth disable
group-lock none
pfs disable
ipsec-udp disable
ipsec-udp-port 10000
split-tunnel-policy tunnelall
split-tunnel-network-list none
default-domain none
split-dns none
intercept-dhcp 255.255.255.255 disable
secure-unit-authentication disable
user-authentication disable
user-authentication-idle-timeout 30
ip-phone-bypass disable
leap-bypass disable
nem disable
backup-servers keep-client-config
msie-proxy server none
msie-proxy method no-modify
msie-proxy except-list none
msie-proxy local-bypass disable
nac disable
nac-sq-period 300
nac-reval-period 36000
nac-default-acl none
address-pools value pool1
smartcard-removal-disconnect enable
client-firewall none
client-access-rule none
webvpn
functions url-entry
html-content-filter none
homepage none
keep-alive-ignore 4
http-comp gzip
filter none
url-list none
customization value DfltCustomization
port-forward none
port-forward-name value Application Access
sso-server none
```

deny-message value Login was successful, but because certain criteria have not been met or due to some specific group policy, you do not have permission to use any of the VPN features. Contact your IT administrator for

```
more information
  svc none
  svc keep-installer installed
  svc keepalive none
  svc rekey time none
  svc rekey method none
  svc dpd-interval client none
  svc dpd-interval gateway none
  svc compression deflate
group-policy QuarantineGroupPolicy internal
group-policy QuarantineGroupPolicy attributes
vpn-filter value acl_http_only
vpn-tunnel-protocol IPSec l2tp-ipsec webvpn
default-domain value quarantine.com
address-pools value quarantine
tunnel-group DefaultRAGroup general-attributes
authentication-server-group RADIUS
authentication-server-group (outside) RADIUS
authorization-server-group RADIUS
authorization-server-group (outside) RADIUS
accounting-server-group RADIUS
tunnel-group DefaultRAGroup ipsec-attributes
pre-shared-key *
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
parameters
  message-length maximum 512
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect h323 h225
inspect h323 ras
inspect rsh
inspect rtsp
inspect esmtp
inspect sqlnet
inspect skinny
inspect sunrpc
inspect xdmcp
inspect sip
```

```
inspect netbios
inspect tftp
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:12a58b266fb1fde81618590c838b0cd0
: end
asdm image disk0:/asdm-524.bin
asdm location 10.0.192.0 255.255.255.0 outside
asdm location 10.0.192.55 255.255.255.255 outside
asdm location 10.0.224.0 255.255.255.0 outside
no asdm history enable
```