CHAPTER 8

Configuring NAC

This chapter describes how to configure Network Admission Control (NAC) on NX-OS devices.

This chapter includes the following sections:

Information About NAC

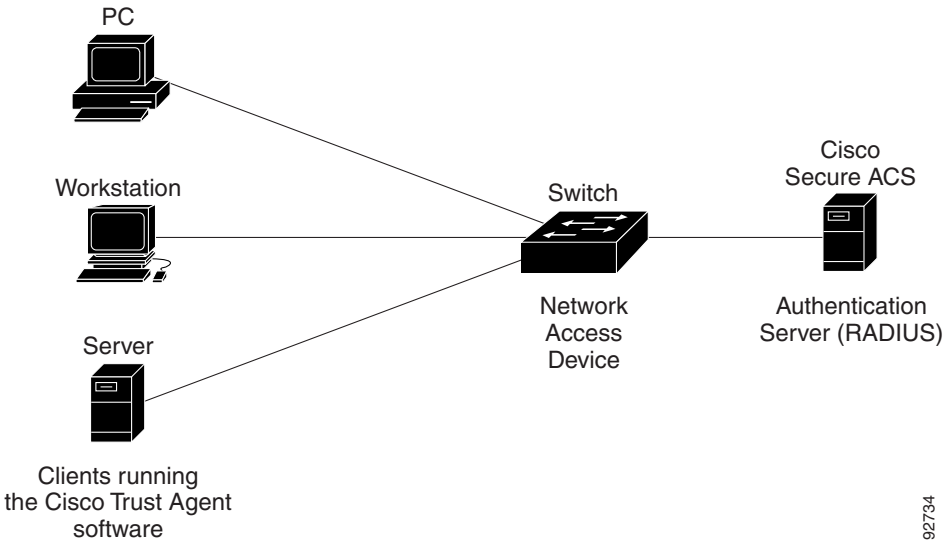
posture validation

devices can access protected areas of the network. For devices that comply with the security policies, NAC allows access to protected services in the network. For devices that do not comply with security policies, NAC allows access to the network only for remediation, when the posture of the device is checked again.

This section includes the following topics:

NAC Device Roles

Figure 8-1 Posture Validation Devices



NAC supports the following roles for network devices:

Endpoint device—Systems or clients on the network such as a PC, workstation, or server that is connected to an NX-OS device access port through a direct connection. The endpoint device, which is running the Cisco Trust Agent software, requests access to the LAN and switch services and responds to requests from the switch. Endpoint devices are potential sources of virus infections, and NAC must validate their antivirus statuses before granting network access.

Note *posture agent* *antivirus client*
For more information on Cisco Trust Agent software, go to the following URL:
http://www.cisco.com/en/US/products/sw/secursw/ps5057/index.html

Network access device (NAD)— Cisco NX-OS device that provides validation services and policy enforcement at the network edge and controls the physical access to the network based on the access policy of the client. The NAD relays Extensible Authentication Protocol (EAP) messages between the endpoints and the authentication server.

The NAD queries for posture credentials whenever it detects a new connection to the network. When the endpoint device has a posture agent (PA) installed, the NAD performs an in-band posture validation. The NAD acts as a relay agent between the endpoint device and AAA server for all messages in the posture validation exchange. If the NAD does not find a PA, the NAD performs an out-of-band posture validation through an audit server.

The NAD controls which hosts have access to network destinations through that device based on a network access profile received from the AAA server once the posture validation exchange completes (whether in-band or out-of-band). The access profile can be one of the following forms:

–

–

NAC process (for example, access to the Dynamic Host Configuration Protocol (DHCP) server, remediation server, audit server).

The NAD triggers the posture validation process at the following times:

When a new session starts.

When the revalidation timer expires.

When you enter a system administrator command.

When the posture agent indicates that the posture has changed (only for an endpoint device with a posture agent).

For Cisco NX-OS devices, the encapsulation information in the Extensible Authentication Protocol (EAP) messages is based on the User Datagram Protocol (UDP). When using UDP, the NX-OS device uses EAP over UDP (EAPoUDP or EoU) frames.

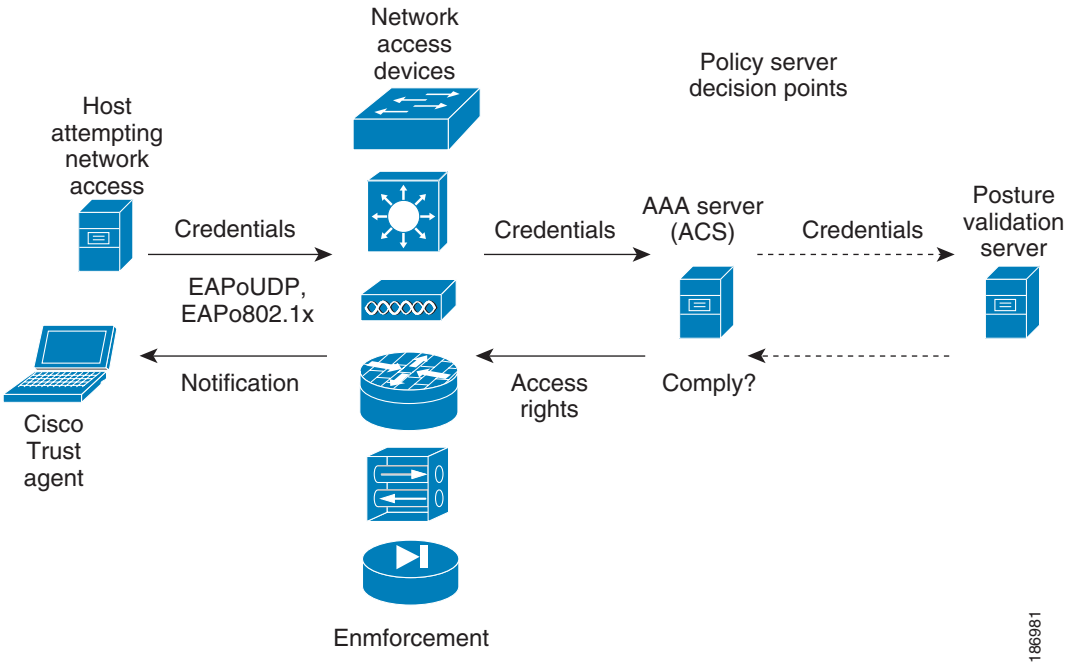
Authentication server— Server that performs the actual validation of the client. The authentication server validates the antivirus status of the client, determines the access policy, and notifies the NAD if the client is authorized to access the LAN and NAD services. Because the NAD acts as the proxy, the EAP message exchange between the NAD and authentication server is transparent to the NAD.

The Cisco NX-OS device supports the Cisco Secure Access Control Server (ACS) Version 4.0 or later with RADIUS, authentication, authorization, and accounting (AAA), and EAP extensions.

Posture validation server—Third-party server that acts as an application-specific policy decision point in NAC for authorizing a set of posture credentials against a set of policy rules. The posture validation server receives requests from an authentication server.

NAC Posture Validation

Figure 8-2 NAC Endpoint Device Posture Validation



posture tokens (APTs). An APT represents a compliance check for a given vendor's application. The AAA server aggregates all APTs from the posture validation servers into a single system posture token (SPT) that represents the overall compliance of the endpoint device. The value SPT is based on the worst APT from the set of APTs. Both APTs and SPTs are represented using the following predefined tokens:

Healthy—The endpoint device complies with the posture policy so no restrictions are placed on this device.

Checkup—The endpoint device is within policy but does not have the latest software; an update is recommended.

Transition—The endpoint device is in the process of having its posture checked and is given interim access pending a result from a complete posture validation. A transition result may occur when a host is booting and complete posture information is not available, or when complete audit results are not available.

Quarantine—The endpoint device is out of compliance and must be restricted to a quarantine network for remediation. This device is not actively placing a threat on other endpoint devices but is vulnerable to attack or infection and must be updated as soon as possible.

Infected—The endpoint device is an active threat to other endpoint devices; network access must be severely restricted and the endpoint device must be placed into remediation or denied all network access to the endpoint device.

Unknown—The AAA server cannot determine the posture credentials of the endpoint device. You need to determine the integrity of the endpoint device so that proper posture credentials can be attained and assessed for network access authorization.

IP Device Tracking

-

-

Note

NAC LAN Port IP Validation

-

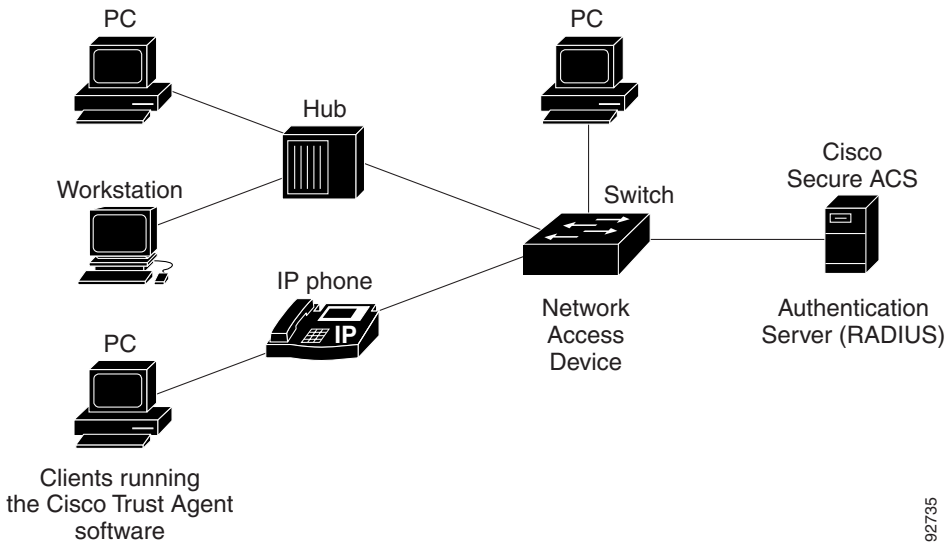
- Subjects all hosts sending IP traffic on the port to posture validation.

LPIP validation triggers admission control by snooping on DHCP messages or Address Resolution Protocol (ARP) messages rather than intercepting IP packets on the data path. LPIP validation performs policy enforcement using access control lists (ACLs).

LPIP validation can process a single host connected to a NAD port or multiple hosts on the same NAD port as shown in Figure 8-3.

When you enable LPIP validation, EAPoUDP only supports IPv4 traffic. The NAD checks the antivirus status of the endpoint devices or clients and enforces access control policies.

Figure 8-3 Network Using LPIP Validation



, page 8-6
Admission Triggers, page 8-6
Posture Validation Methods, page 8-7
Policy Enforcement Using ACLs, page 8-8
Audit Servers and Nonresponsive Hosts, page 8-8
NAC Timers, page 8-9
NAC Posture Validation and Redundant Supervisor Modules, page 8-11

Posture Validation

"Configuring DHCP Snooping").

Admission Triggers

Note

Posture Validation Methods

-
-

Exception Lists

EAPoUDP

Note

Note

Policy Enforcement Using ACLs

[PACL]). The active MAC ACL could either be a statically configured PACL or an AAA server-specified PACL based on 802.1X authentication.

The PACL defines a group that expands to a list of endpoint device IP addresses. The PACLs usually contain the endpoint device IP addresses. Once the NAD classifies an endpoint device using a particular group, the NAD adds the IP address that corresponds to the endpoint device to the appropriate group. The result is that the policy is applied to the endpoint device.

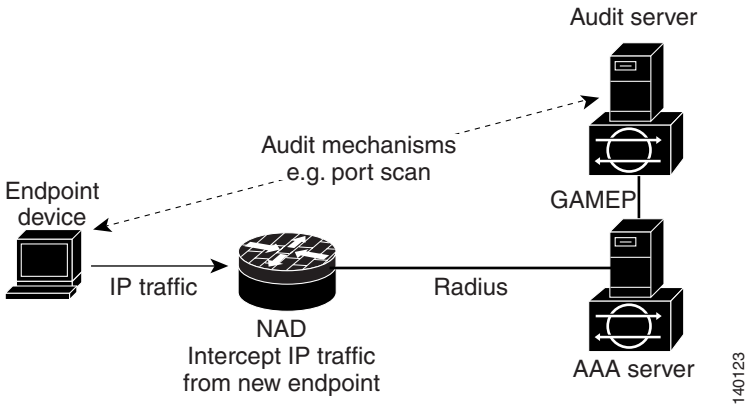
When you configure LPIP validation for an NAD port, you must also configure a default PACL on that NAD port. In addition, you should apply the default ACL to the IP traffic for hosts that have not completed posture validation.

If you configure the default ACL on the NAD and the Cisco Secure ACS sends a host access policy to the NAD, the NAD applies the policy to that traffic from the host that is connected to a NAD port. If the policy applies to the traffic, the NAD forwards the traffic. If the policy does not apply, the NAD applies the default ACL. However, if the NAD gets an endpoint device access policy from the Cisco Secure ACS but the default ACL is not configured, the LPIP validation configuration does not take effect.

Both DHCP snooping and ARP snooping are enabled per VLAN. However, security ACLs downloaded as a result of NAC Layer 2 posture validation are applied per port. As a result, all DHCP and ARP packets are intercepted when these features are enabled on any VLAN.

Audit Servers and Nonresponsive Hosts

Figure 8-4 NAC Device Roles



Hold Timer

AAA Timer

Note

Retransmit Timer

Note

Revalidation Timer

-
-
-
-

Status-Query Timer

NAC Posture Validation and Redundant Supervisor Modules

LPIP Validation and Other Security Features

-
-
-
-
-
-
-
-

802.1X

Port Security

DHCP Snooping

Dynamic ARP Inspection


Note


Note

IP Source Guard


Note

Posture Host-Specific ACEs


Note

Active PACL


Note

VACLs


Note

Virtualization Support

Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.0

Licensing Requirements for NAC

Product	License Requirement
	Cisco Nexus 7000 Series NX-OS Licensing Guide, Release 4.0

Prerequisites for NAC

-

NAC Guidelines and Limitations

-
-

LPIP Limitations

-
-
-
-
-
-
-

Configuring NAC

-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-

Note

Process for Configuring NAC

Step 1

Step 2

Step 3

Step 4

Enabling EAPoUDP

BEFORE YOU BEGIN

switchto vdc

SUMMARY STEPS

1. **config t**
   feature eou
   exit
   copy running-config startup-config

	Command	Purpose
Step 1	**config t** **Example:** switch# config t switch(config)#	
	feature eou **Example:** switch(config)# feature eou	
	switch(config)# exit switch#	
	copy running-config startup-config **Example:** switch# copy running-config startup-config	

Enabling the Default AAA Authenication Method for EAPoUDP

Note

BEFORE YOU BEGIN

switchto vdc

Configure RADIUS or TACACS+ server groups, as needed.

aaa authentication eou default group

exit

show aaa authentication

5.

DETAILED STEPS

	Command	Purpose
Step 1		
Step 2	**aaa authentication eou default group** *group-list* default group RadServer	*named-group*
	switch(config)# exit switch#	
	show aaa authentication **Example:**	
	copy running-config startup-config **Example:**	

Applying PACLs to Interfaces

/

mac access-group

exit

show running-config interface

6.

DETAILED STEPS

	Command	Purpose
Step 1		

Step 2	/
	
	Example:
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`	

	access-list `switch(config-if)# mac access-group acl-01`	
	`switch(config-if)# exit` `switch(config)#`	
	`switch(config)# show running-config interface`	
	`switch(config)# copy running-config startup-config`	

nac enable

exit

7.

8.

DETAILED STEPS

	Command	Purpose
Step 1		
Step 2		
Step 3		
Step 4		
Step 5	**nac enable** **Example:** switch(config-if)# nac enable	
	switch(config-if)# exit switch(config)#	

	Command	Purpose
Step 7		
Step 8		

policy-name

object-group

description " "

exit

show identity policy

identity profile eapoudp

device {**authenticate** | } { [*ipv4-subnet-mask*
mac-address *mac-subnet-mask* *name*

9.

10.

11.

DETAILED STEPS

	Command	Purpose
Step 1		
Step 2	*policy-name* switch(config)# identity policy AccType1 switch(config-id-policy)#	
	object-group **Example:** switch(config-id-policy)# object-group maxaclx	
	description "*text* "This policy prevents endpoint device without a PA"	
	switch(config-id-policy)# exit switch(config)#	
	switch(config)# show identity policy	
	switch(config)# identity profile eapoudp switch(config-id-prof)#	
	device { | } { *ipv4-address* [*ipv4-subnet-mask*]| *mac-address* [*mac-subnet-mask*]} *name* switch(config-id-prof)# device authenticate ip-address 10.10.2.2 policy AccType1	
	switch(config-id-prof)# exit switch(config)#	

	Command	Purpose
Step 10		
Step 11		

Allowing Clientless Endpoint Devices

BEFORE YOU BEGIN

SUMMARY STEPS

1.
2.
3.
4.
5.

DETAILED STEPS

	Command	Purpose
Step 1		
Step 2		
Step 3		

	Command	Purpose
Step 4		
Step 5		

Enabling Logging for EAPoUDP

BEFORE YOU BEGIN

SUMMARY STEPS

1.
2.
3.
4.
5.

DETAILED STEPS

	Command	Purpose
Step 1		
Step 2		
Step 3		

	Command	Purpose
Step 4		
Step 5		

Changing the Global EAPoUDP Maximum Retry Value

BEFORE YOU BEGIN

SUMMARY STEPS

1.
2.
3.
4.
5.

DETAILED STEPS

	Command	Purpose
Step 1		
Step 2		
Step 3		

	Command	Purpose
Step 4		
Step 5		

Changing the EAPoUDP Maximum Retry Value for an Interface

BEFORE YOU BEGIN

SUMMARY STEPS

1.
2.
3.
4.
5.
6.

DETAILED STEPS

	Command	Purpose
Step 1		
Step 2		
Step 3		

	Command	Purpose
Step 4		
Step 5		
Step 6		

Changing the UDP Port for EAPoUDP

BEFORE YOU BEGIN

SUMMARY STEPS

1.
2.
3.
4.
5.

DETAILED STEPS

	Command	Purpose
Step 1		
Step 2	`switch(config)# eou port 27180`	
	`switch(config)# exit` `switch#`	

switch# show eou	
switch# copy running-config startup-config	

switch# config t switch(config)#	
number-of-sessions switch(config)# eou ratelimit 15	
switch(config)# exit switch#	

`switch# show eou`	
`switch# copy running-config startup-config`	

`switch# config t` `switch(config)#`	
`switch(config)# eou revalidate`	
`switch(config)# eou timeout revalidation 30000`	

switch(config)# exit switch#	
switch# show eou	
switch# copy running-config startup-config	

switch# config t switch(config)#	
switch(config)# interface ethernet 2/1 switch(config-if)#	
switch(config-if)# eou revalidate	
switch(config-if)# eou timeout revalidation 30000	
switch(config-if)# exit switch(config)#	
switch(config)# show eou	
switch(config)# copy running-config startup-config	

eou timeout status-query

exit

show eou

copy running-config startup-config

`switch# config t` `switch(config)#`	
`switch(config)# eou timeout aaa 30`	
`switch(config)# eou timeout hold-period 300`	
`switch(config)# eou timeout retransmit 10`	

switch(config)# eou timeout revalidation 30000	
eou timeout status-query **Example:** switch(config)# eou timeout status-query 360	
switch(config)# exit switch#	
switch# show eou	
switch# copy running-config startup-config	

switchto vdc

`switch# config t` `switch(config)#`	
`switch(config)# interface ethernet 2/1` `switch(config-if)#`	
`switch(config-if)# eou timeout aaa 50`	
`switch(config-if)# eou timeout hold-period 300`	
`switch(config-if)# eou timeout retransmit 10`	
`switch(config-if)# eou timeout revalidation 30000`	
`switch(config-if)# eou timeout status-query 360`	

switch(config-if)# exit switch(config)#	
switch(config)# show eou	
switch(config)# copy running-config startup-config	

switch# config t switch(config)#	
switch(config)# eou default	
switch(config)# exit switch#	

`switch# show eou`	
`switch# copy running-config startup-config`	

`switch# config t` `switch(config)#`	
`switch(config)# interface ethernet 2/1` `switch(config-if)#`	
`switch(config-if)# eou default`	

ip device tracking enable

ip device tracking probe count interval

radius server host *hostname ip-address username password minutes*

hostname ip-address

ip device tracking enable **Example:** switch(config)# ip device tracking enable	
{ | } switch(config)# ip device tracking probe count 4	
{*hostname ip-address*} [*username* [*password* *minutes* 10.10.1.1 test username User2 password G1r2D37&k idle-time 5	
switch(config)# exit switch#	
switch# show ip device tracking all	
{ } switch# show radius-server 10.10.1.1	
switch# copy running-config startup-config	

`switch# clear ip device tracking all`	
`switch# clear ip device tracking interface ethernet 2/1`	
`switch# clear ip device tracking ip-address 10.10.1.1`	
`switch# clear ip device tracking mac-address 000c.30da.86f4`	
`switch# show ip device tracking all`	

eou initialize all

eou initialize authentication clientless eap static

eou initialize interface ethernet /

eou initialize ip-address

eou initialize mac-address

eou initialize posturetoken

show eou all

eou initialize all **Example:** switch# eou initialize all	
{ | | }	
switch# eou initialize authentication static	
switch# eou initialize interface ethernet 2/1	
switch# eou initialize ip-address 10.10.1.1	
switch# eou initialize mac-address 000c.30da.86f4	

`switch# eou initialize posturetoken Healthy`	
`switch# show eou all`	

`switch# eou revalidate all`	
`{ | | }` `switch# eou revalidate authentication static`	
`switch# eou revalidate interface ethernet 2/1`	

switch# eou revalidate ip-address 10.10.1.1	
switch# eou revalidate mac-address 000c.30da.86f4	
switch# eou revalidate posturetoken Healthy	
switch# show eou all	

	Command	Purpose
Step 1		
Step 2		
Step 3		
Step 4		
Step 5		
Step 6		Note
Step 7		

Caution

BEFORE YOU BEGIN

SUMMARY STEPS

1.
2.

3.

4.

DETAILED STEPS

	Command	Purpose
Step 1		
Step 2		 **Caution**
Step 3		
Step 4		

Verifying the NAC Configuration

Command	Purpose

Example NAC Configuration

```
interface Ethernet8/1
  mac access-group macacl-01
```

Default Settings

Table 8-1 Default NAC Parameters

	Default

Additional References

-

Related Documents

Related Topic	Document Title