Network Admission Control Agentless Host Support

Last Updated: October 24, 2011

The Network Admission Control: Agentless Host Support feature allows for an exhaustive examination of agentless hosts (hosts that are not running the Cisco Trust Agent software). This examination allows customers to build a robust host or examination functionality by integrating any third-party audit mechanisms into the Network Admission Control architecture.

This feature also allows for Extensible Authentication Protocol over UDP (EAPoUDP) bypass, which speeds up the posture validation of hosts that are not using Cisco Trust Agent.

Prerequisites for Network Admission Control Agentless Host Support

- You must be running Cisco IOS Release 12.4(6)T or a later release.
- You must be using a Cisco access control server (ACS) version 4.0 or a later version.
- You must have a Cisco or third-party audit server setup.

Information About Network Admission Control Agentless Host Support

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Network Admission Control

The Cisco Network Admission Control functionality enables the credentials of the endpoint device to be checked for compliance with the security policy before the device is granted access to network resources. This checking requires a security application called Cisco Trust Agent (CTA) to be installed on end devices that gather security state information and communicate it to access servers where policy decisions are made and eventually enforced on Cisco network access devices (such as routers and switches).

Agentless Hosts

End devices that do not run CTA cannot provide credentials when challenged by network access devices (NADs). Such hosts are termed “agentless” or “nonresponsive.” In the Phase l release of Network Admission Control, agentless hosts were supported by either a static configuration using exception lists (an identity profile) or by using “clientless” username and password authentication on an ACS. These methods are restrictive and do not convey any specific information about the host while making policy decisions.

EAPoUDP Bypass

You can use the EAPoUDP Bypass feature to reduce latency of the validation of hosts that are not using CTA. If EAPoUDP bypass is enabled, the NAD does not contact the host to request the antivirus condition (the NAD does not try to establish an EAPoUDP association with the host if the EAPoUDP Bypass option is configured). Instead, the NAD sends a request to the Cisco Secure ACS that includes the IP address, MAC address, service type, and EAPoUDP session ID of the host. The Cisco Secure ACS makes the access control decision and sends the policy to the NAD.

If EAPoUDP bypass is enabled, the NAD sends an agentless host request to the Cisco Secure ACS and applies the access policy from the server to the host.

If EAPoUDP bypass is enabled and the host uses the Cisco Trust Agent, the NAD also sends a nonresponsive-host request to the Cisco Secure ACS and applies the access policy from the server to the host.

Vendor-Specific Attributes for This Feature

The following new attributes are supported for various RADIUS message exchanges:

audit-session-id

The audit-session-id vendor-specific attribute (VSA) is a 32-byte string that uniquely identifies a host session. This identifier is generated by a NAD when the host is detected, and it remains the same until the session is deleted. Session revalidation or reinitialization does not change this identifier. Every time a session is detected, a new identifier is generated. This attribute is included in access requests to the authentication, authorization, and accounting (AAA) server and in web requests to the audit server. The value of this attribute is displayed in **show eou** command output (using the **ip** keyword).

url-redirect-acl

The url-redirect-acl VSA string specifies the name of the access control list (ACL) for URL redirection. Any ingress HTTP from the host that matches the access list that is specified by this attribute is subjected to redirection to the URL address specified by the url-redirect VSA. The access list specified in this attribute has to be locally configured on the NAD as an "ip access-list extended" named ACL. This attribute is specified only in RADIUS access-accept messages. The value of the url-redirect-acl attribute is displayed using the **show eou** command (with the **ip** keyword).

Note Phase 1 of the Network Admission Control feature introduced the url-redirect VSA that allowed the HTTP sessions of users to be redirected to the address specified by the url-redirect VSA. This redirection is useful if you want to remediate hosts that do not comply to network security policy. However, to determine to which users HTTP requests are to be redirected, Phase 1 of Network Admission Control assumed that any HTTP traffic that was intercepted and denied by the host policy ACL (the access control server ACL) was subjected to redirection. The url-redirect-acl VSA provides an option so that users can customize the redirect criteria. The url-redirect-acl VSA supports backward compatibility. If the url-redirect-acl is specified in the access-accept message for the host, any user HTTP sessions that match the ACL are subjected to redirection. However, if the url-redirect-acl attribute is not received, the Phase 1 logic to perform redirection is used. The Phase 1 logic to perform redirection applies only to Cisco IOS routers. The url-redirect-acl attribute is mandatory for Cisco IOS switches.

How to Configure Network Admission Control Agentless Host Support

Configuring a NAD to Bypass EAPoUDP Communication

To configure a NAD to bypass EAPoUDP, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip admission name** *admission-name* **eapoudp bypass**
4. **eou allow clientless**
5. **interface type** *slot* / *port*
6. end

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip admission name** *admission-name* **eapoudp bypass** **Example:** `Router (config)# ip admission name greentree eapoudp bypass`	The IP network admission control rule bypasses EAPoUDP communication.
Step 4	**eou allow clientless** **Example:** `Router (config)# eou allow clientless`	Allows authentication of clientless hosts (systems that do not run Cisco Trust Agent).
Step 5	**interface type** *slot* / *port* **Example:** `Router (config)# interface ethernet 2/4`	Configures an interface type and enters interface configuration mode.
Step 6	end **Example:** `Router (config-if)# end`	Exits configuration modes.

Verifying Agentless Host and EAPoUDP Bypass

To verify your configuration for Agentless Host and EOUoUDP Bypass, perform the following steps. The **debug** and **show**commands can be used independently of each other.

SUMMARY STEPS

1. **enable**
2. **debug eou**
3. **show eou ip** *ip-address*
4. **show ip admission configuration**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug eou** **Example:** `Router# debug eou`	Displays information about EAUoUDP.
Step 3	**show eou ip** *ip-address* **Example:** `Router# show eou ip 10.0.0.0`	Displays information about EAPoUDP global values or EAPoUDP session cache entries.
Step 4	**show ip admission configuration** **Example:** `Router# show ip admission configuration`	Displays information about the agentless and EAPoUDP Bypass configuration.

Configuration Examples for Network Admission Control Agentless Host Support

RADIUS Message Exchange url-redirect-acl VSA Example

ACS Configuration

```
url-redirect=http://audit-server.com/host_session_id=$host_session_id
url-redirect-acl=RedirectACL
```

NAD Configuration

```
Router(config)# ip access-list extended RedirectACL
Router (config-ext-nacl)# permit tcp any 10.0.0.0 0.0.0.255 eq www
Router (config-ext-nacl)# end
```

Show Output Displaying the Value of a Newly Defined VSA

The following **show eou** command output displays EAPoUPD session cache information for a given IP address. The value of the newly defined VSA is also shown.

```
Router# show eou ip 10.0.0.1
Address              : 10.0.0.1
MAC Address          : 0001.027c.f364
Interface            : FastEthernet1/0/3
AuthType             : EAP
Audit Session ID     : 000000001C8A6A330000001812000001
PostureToken         : Infected
Age(min)             : 444
URL Redirect         : http://wwwin.cisco.com
URL Redirect ACL     : RedirectACL
ACL Name             : #ACSACL#-IP-Infected-42835ff7
User Name            : NAC-DEV-PC-3:Administrator
Revalidation Period  : 30000 Seconds
Status Query Period  : 300 Seconds
Current State        : AUTHENTICATED
```

Additional References

Related Documents

Related Topic	Document Title
Configuring AAA and RADIUS for EAPoUDP	Network Admission Control feature module
Network Admission Control	
Security commands	*Cisco IOS Security Command Reference*

MIBs

MIB	MIBs Link
None.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Network Admission Control Agentless Host Support

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1 Feature Information for Network Admission Control: Agentless Host Support

Feature Name	Releases	Feature Information
Network Admission Control: Agentless Host Support	12.4(6)T	The Network Admission Control: Agentless Host Support feature allows for an exhaustive examination of agentless hosts (hosts that are not running the Cisco Trust Agent software). This examination allows customers to build a robust host or examination functionality by integrating any third-party audit mechanisms into the Network Admission Control architecture. This feature also allows for Extensible Authentication Protocol over UDP (EAPoUDP) bypass, which speeds up the posture validation of hosts that are not using Cisco Trust Agent. This feature was introduced in Cisco IOS Release 12.4(6)T. The following commands were introduced or modified: **eou clientless**, **ip admission name**, **show eou**