Reference Information

This appendix provides a list of acronyms and definitions of terms used in Network Admission Control (NAC). It provides sources of further information about NAC and includes the following sections:

Acronyms

Table B-1 Acronyms

Acronyms	Definition
AAA	Authentication, Authorization, and Accounting
ACE	Access Control Element
ACL	Access Control List
Cisco Secure ACS	Access Control Server
APT	Application Posture Token
AV	Anti Virus
AVP	Attribute Value Pair
CA	Certificate Authority
CTA	Cisco Trust Agent
EAP	Extensible Authentication Protocol
FW	Firewall
HCAP	Host Credential Authorization Protocol
HTTPS	Secure Hyper Text Transfer Protocol
IDS	Intrusion Detection Systems
NAC	Network Admission Control
NAD	Network Access Device
PA	Posture Agent
PB	Posture Broker

Table B-1 Acronyms (continued)

Acronyms	Definition
PEAP	Protected Extensible Authentication Protocol
RADIUS	Remote Access Dial In User Service
SPT	System Posture Token
TACS+	Terminal Access Controller Access Control System Plus
TLS	Transport Layer Security
TLV	Type Length Value
UDP	User Datagram Protocol
VPN	Virtual Private Network

Definitions

Table B-2 Definitions

Term	Definition
AAA Server	Evaluates credentials from peer and determines network access policy for enforcement by Authenticator. May use back-end servers for credential evaluation, such as vendor-specific posture servers such as the NAI AV Server. Also supports access policies for “clientless hosts”.
Access Accept	AAA Server returns Access Accept to Authenticator to indicate that the peer has had its credentials evaluated successfully and (optionally) that a new access policy is to be enforced as a result. Successful evaluation means that the Authenticator must keep state that the Peer has had its credentials checked so that the Peer is not checked again until it is time to re-validate the Peer.
Access Reject	AAA Server returns Access Reject to indicate that the credentials have not been evaluated successfully, and no (new) access is to be provided to the peer. Unsuccessful evaluation means that the Authenticator does not maintain state about the peer; that is, the peer credentials need to be checked again after some configurable hold period. The default access policy continues to apply to rejected peers.
Accounting	The process of collecting quantitative data about sessions for the purposes of troubleshooting, capacity planning, or auditing.
Association	A single instance of the L3 access control protocol (Apocope) between peer and authenticator. Represented by state of conversation, IP address of other party, active timers, keys used in status query.

Table B-2 Definitions (continued)

Term	Definition
Authentication	In the case of identity, the use of credentials to establish that a principal is who he or she claims to be. In the case of posture, the use of credentials to establish that the posture of the end-system is what the principal says it is.
Authenticator	Logical entity in the gateway that initiates the exchange of EAP credentials, relays EAP credential requests and responses between peer and AAA server, and enforces network access policy on a particular port or interface based on the results from the AAA server. Same functionality as authenticator in EAP or 802.1X, but does not include any AAA server functionality. In addition to acting as an EAP "pass-through" for EAP methods that require a AAA server, the authenticator implements EAP methods that do not require AAA server functionality, in particular, the EAP status query method.
Authorization	The act of determining what part of the network a principal is permitted to access based on identity or posture or both.
Cisco Trust Agent	Cisco software that implements peer functionality
Clientless host	A TCP/IP host that does not have the posture agent installed
Credential	A piece of information presented by a principal in support of a claim of identity or posture. Includes identity and posture information itself. Examples include username, password, and AV signature file version.
Default Access Policy	Access policy applied to a peer when the policy has not been updated as a result of an Access Accept
End-system	A TCP/IP host; for example, desktop, server, IP phone, printer
Gateway	L3 network device that has authenticator functionality. May be one or more hops from peer
Identity	A unique name associated with a principal.
IP Intercept ACL	A special type of access control list (ACL) that indicates which packets on an interface trigger validation of the peer (source IP address of the packet)
Network Access Device	First hop network device (as measured from peer) that has authenticator functionality
Network Access Filtering	A method of changing the downloadable access list depending on which network access device is receiving the download.
Network Device	L2 or L3 networking equipment such as switches, routers, wireless access points, and VPN concentrators
Peer	Logical entity in end-system that responds to requests for credentials from authenticator for the purposes of gaining access to restricted network. Referred to as supplicant in 802.1x. Same as peer in EAP.
Posture	The state of a device; for example, set of applications loaded on desktop; AV scan engine version and signature file version; FW version and rules file

Table B-2 Definitions (continued)

Term	Definition
Posture Agent	The software implementing the posturing process on a client machine. This includes, but is not limited to, the Cisco Trust Agent.
Posture Client	Cisco or third-party software that resides on the peer and responds to requests from posture agent for posture credentials.
Posture Server	Cisco or third-party back-end server that responds to requests from AAA server to validate vendor-specific posture credentials from posture client.
Principal	Something with an identity; for example, a user or a device.
Provisioning	Configuration of network devices and servers needed to deliver services for a principal.
User	A human being using a device.

Related Documentation

This section provides URLs to websites where you can obtain additional information about NAC. It includes the following topics:

- Configuring Network Admission Control
- CTA Documentation

Configuring Network Admission Control

- Implementing Authentication Proxy—
http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_tech_note09186a0080094eb0.shtml
- Configuring Authentication Proxy—
http://www.cisco.com/en/US/docs/ios/12_1/security/configuration/guide/scdauthp.html
- Cisco Secure ACS 3.3—
http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/

CTA Documentation

- CiscoWorks SIMS—
http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000_b/sims/3_1_1/
- Cisco Security Agent—
http://www.cisco.com/univercd/cc/td/doc/product/vpn/ciscosec/csa/40/index.htm