GLOSSARY

A

ACL Access control list. This is a list of access permissions attached to an object that specify which users or processes are granted access to this or other objects, including what operations can be allowed on a given object. Entries in an ACL can specify permission for a user, an operation, a port, or a hostname.

ACS Access Control System. This is a policy-based security server that provides standards-compliant Authentication, Authorization, and Accounting (AAA) services to your network. ACS facilitates the administrative management of Cisco and non-Cisco devices and applications.

AD Active Directory. This is a directory service created by Microsoft that stores all information and settings for a deployment in a central database. AD allows administrators to assign policies, and deploy and update software from small network installations with a small number of computers, users, and printers to much larger network environments with multiple domains and different locations.

D

DACL Downloadable access control list. Cisco ISE supports a downloadable list of access permissions attached to an object that specify which users or processes are granted access to this or other objects, including what operations can be allowed on a given object. Entries in an DACL can specify permission for a user, an operation, a port, or a hostname.

H

HTTPS Hypertext Transfer Protocol Secure. This combination of the Hypertext Transfer Protocol (HTTP) with the SSL/TLS protocol provides secure, encrypted communication and secure identification for network and Internet traffic. HTTPS connections are often used for sensitive transactions within corporate, financial, or commercial systems. HTTPS uses a different port that provides an additional layer of encryption and authentication between HTTP and TCP.

L

LDAP Lightweight Directory Access Protocol. It is an application protocol for querying and modifying data in directories using directory services running over TCP/IP. An LDAP directory in this sense is an organized set of records, such as a telephone directory is an alphabetical list of persons and organizations, each with an address and phone number that comprises a "record". A common method of securing LDAP communication is using an SSL tunnel.

M

MAC address Media access control address. A quasi-unique identifier assigned by the manufacturer to most network adapters or network interface cards for identification.

N

NDG Network device group. In Cisco ISE, a device group is a hierarchical structure that contains network device groups (NDGs) that are a logical grouping of similar devices based on criteria such as location or device type. For example, you can group devices by continent, region, or country location, or you can group devices like firewalls, routers, or switches by types. In Cisco ISE, you can also use NDGs in policy conditions.

P

PI Programmatic Interface. A mechanism for external applications to interact with Cisco Secure ACS.

R

RADIUS Remote Authentication Dial In User Service. This is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for computers to connect and use a network service.

T

TACACS Terminal Access Controller Access-Control System. It is a remote authentication protocol that is used to communicate with an authentication server commonly used in UNIX networks. TACACS allows a remote access server to communicate with an authentication server in order to determine if the user has access to the network.

V

VSA Vendor specific attribute. A proprietary property or characteristic not provided by the standard RADIUS attribute set. VSAs are defined by vendors of remote access servers to customize RADIUS for their servers.