CCNP Security - SISAS

AAA Concepts

What is AAA ?

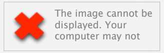
- AAA stands for
  - Authentication
  - Authorization
  - Accounting
- AAA can be used for multiple purposes
  - Network Device administration
  - Network Access (wired, wireless, VPN)
- Authentication
  - Provide identification of who you are
  - Various options: username and password , certificates

The image cannot be displayed. Your computer may not

What is AAA ?

» Authorization

- Defines what you are allowed to do
- For network administration:
  - privilege-level
  - Allowed commands
- For network access:
  - VLAN
  - Access-list
  - Security Group Tag
  - Encryption



What is AAA ?

» Accounting

- Provides evidence of what you have done, like auditing
- For network administration:
  - Typed commands for forensics analysis
- For network access:
  - Session statistics for billing
  - Session identification (MAC address, IP address, username)
  - Session state (connected or disconnected)

AAA Model

» Three-party authentication model

- Supplicant / end-client
  - Device requesting access
  - Speaks with the authenticator
- Authenticator
  - Device enforcing the authentication , known as NAD
  - Bridges information between supplicant and authentication server
- Authentication Server
  - Device performing the authentication
  - Connected to identity sources: username/password, PKI
  - Can behave like a proxy towards another authentication server

AAA Protocols

- Between supplicant and authenticator
  - For device administration
    - console
    - Telnet / SSH
    - HTTP / HTTPS
  - For network access
    - EAPOL
    - HTTP / HTTPS
- Between authenticator and authentication server
  - RADIUS
  - TACACS+

RADIUS

- IETF standard (RFC2865)
    - Has additional RFC’s for specific features
    - Combines authentication and authorization in one process
    - Uses UDP port 1645/1812 for authentication
    - Uses UDP port 1646/1813 for accounting
    - Initial ports of 1645/1646 were also used by **datametrics** service
    - RADIUS key with MD5 used to hide the user’s password
- Performs its scope via RADIUS attributes
    - IETF standard defined
    - Vendor Specific Attributes (VSA’s)

The image cannot be displayed. Your computer may not

RADIUS

- IETF standard (RFC2865)
  - Mainly used for network access
  - Has additional RFC’s for specific features
  - Combines authentication and authorization in one process
  - Uses UDP port 1645/1812 for authentication
  - Uses UDP port 1646/1813 for accounting
  - Initial ports of 1656/1646 were also used by **datametrics** service
  - RADIUS key with MD5 used to hide/protect the user’s password
- Performs its scope via RADIUS attributes
  - IETF standard defined
  - Vendor Specific Attributes (VSA’s)

The image cannot be displayed. Your computer may not

TACACS+

» Developed by Cisco

- Mainly used for device administration
- Developed by Cisco from original TACACS protocol (RFC1492)
- Uses separate processes for authentication, authorization and accounting
- Uses TCP port 49
- Encrypts entire body of TACACS packet, leaves clear-text header

» RADIUS vs. TACACS

- http://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/13838-10.html

The image cannot be displayed. Your computer may not

Cisco's Authentication Servers

- Access Control System (ACS)
  - Supports both TACACS+ and RADIUS
  - Mainly used for TACACS+
- Identity Services Engine (ISE – NGN RADIUS)
  - Supports RADIUS with Change of Authorization (CoA)
  - TACACS+ supported in ISE 2.0
  - Mainly used for RADIUS
  - Additional features not supported by ACS
    - Profiling , posture assessment
    - Web portal services

The image cannot be displayed. Your computer may not

Q&A