

ArubaOS

External Service Interface Module

ArubaOS

The External Services Interface (ESI) software module extends the capabilities of Aruba's user-centric networks to outside control points, allowing an Aruba Mobility Controller to communicate with external service devices and support advanced interaction with AAA infrastructure.

Control-plane integration with external systems is enabled through Application Programming Interfaces (APIs) provided with ESI that link ArubaOS with advanced authentication servers, dynamic authorization control points, and location tracking servers. To integrate the data plane with external systems, ESI can redirect selected network traffic to devices that provide in-line network services such as virus protection, network intrusion detection, billing and accounting, content filtering, content transformation and usage auditing. Traffic redirection is done based on policy, and external devices are both load balanced and health checked to prevent bottlenecks or single points of failure.

Extended Authorization Control API

Extended authorization control allows fine-grained control of users from the authentication server. Controls such as automatic disconnection from the network, role re-assignment, and dynamic updates of policies can be enabled. This functionality is enabled by two Application Programming Interfaces (APIs): IETF standard RFC 3576, and a simple, yet flexible, XML-based API. These APIs both allow external systems to exert user and policy control over an Aruba mobility controller. A third integration interface is available in the form of the Syslog Processor. This interface accepts syslog messages from outside systems, processes them according to a regular-expression rule language, and then provides configurable actions such as changing the role of a user or placing a user on a blacklist. Extended authorization control is especially useful in providing guest access, where access can be customized for each visitor, allowing access only to required services and for the exact period of time necessary.

Specifications:

AAA Interfaces

- XML API, RFC 3576, Syslog Processor

Traffic Redirection Topologies Supported

- Transparent (L2), Routed (L3)

Load Balancing Methods

- Source IP-Destination IP Hash

External Service Health Checking

- ICMP Echo, L2 MAC Frame

External Service Pools

- 16

Service Devices Per Pool

- 16

Product Overview



Benefits:

Extended Authorization Control Using API

- Dynamic modification of user privileges based on metrics such as client behavior
- Automatically disconnects users when pre-defined conditions are matched
- Interfaces to external systems through RFC 3576, a flexible XMLAPI, and the Syslog Processor

External Captive Portal

- Links Aruba's identity-based security with external web-based captive portal authentication systems
- Allows unlimited customization of user experience
- Per-SSID customization of portals optimized for service providers and hospitality establishments

Product Overview

More Benefits:

Flexible Delivery of Network Services

- Centralizes network-based services by bringing traffic from the users to a central location, requiring no change to wiring closets or underlying infrastructure
- Preserves investment with existing security and service vendors

Policy-Based Network Traffic Inspection

- Directs traffic to external appliances based on user identity or trust state
- Redirects traffic selectively, based on policy, to avoid service device overload

Fault Tolerance For Mission-Critical Networks

- Continuous health checking to ensure availability of external devices
- Load balancing to prevent traffic from being sent to a failed device

LTI DataComm
23020 Eaglewood Ct. #100
Sterling, VA 20166
www.ltidata.com
800-677-5050

External Captive Portal

ArubaOS provides integrated captive portal authentication in the base system, with the ability to customize the captive portal look and feel on a per-SSID basis. Organizations wishing to develop more extensive captive portal systems, with custom scripting, database operations, or other advanced behavior may do so using the ESI's authentication API. This simple XML-based API allows an external captive portal server to learn information about users connected to the Aruba Mobility Controller and to signal authentication state, including user role information, to the Mobility Controller. With ESI, there is no limit to the amount of captive portal customization that may be provided.

Flexible Delivery of Network Services

A vast array of network service devices exists in the marketplace today. Typically deployed in a DMZ or at an organization's Internet gateway, these devices provide services such as virus protection, content inspection and filtering, intrusion detection and prevention, content transformation, protocol-based bandwidth shaping and more.

Until now, deploying such services in the interior of the corporate network required placement of network service devices in every wiring closet, where they were placed in-line with all network traffic. Aruba's ESI takes a centralized approach, enabling scalable and manageable deployments that minimize both capital and operational costs.

The ESI module features an open interface, permitting the redirection of traffic to any standard in-line device that supports transparent L2 or routed L3 mode. This allows network managers to use equipment they already own and know, protecting and leveraging their existing investments. Aruba's External Services Interface (ESI) software module for ArubaOS enables the scalable and seamless extension of WAN DMZ services throughout the network.

Policy-Based Network Traffic Inspection

Although all "at risk" traffic should be screened, passing all network traffic through network service devices could lead to performance bottlenecks. Aruba's ESI makes this process more efficient by only forwarding traffic that meets established criteria to service appliances.

For example, some traffic types, such as Enterprise Resource Planning (ERP) traffic or SQL database transactions, do not carry viruses and do not need to be filtered for virus protection. Alternatively, Web, email and file-transfer traffic does require virus filtering. By using the ESI to specify which traffic types are redirected to a network service device, network managers need deploy only enough service capacity for that specified subset of network traffic and will not need to deploy as many, if any, additional appliances.

Similarly, Aruba's ESI can selectively redirect traffic for only certain users or types of users based on authentication or trust state. As an example, enterprises can use endpoint integrity software on employee computers to enforce updates and patches for anti-virus software, personal firewall software and operating systems. If host-based software is up to date on these devices, the network can decide not to perform network-based virus filtering for traffic going to these clients. Contrarily, employees and visitors using their own equipment can be assigned a lower trust level and subjected to strict filtering of all network traffic.

Fault Tolerance For Mission-Critical Networks

The ESI module allows Aruba Networks' mobility controllers to support health checking and load-balancing of traffic to external devices. Flexible health checking techniques permit Aruba Mobility Controllers to determine the operational state of external devices without custom software development or vendor lock-in. By health checking a pool of devices, the system can ensure that traffic is not redirected to a device that is down.