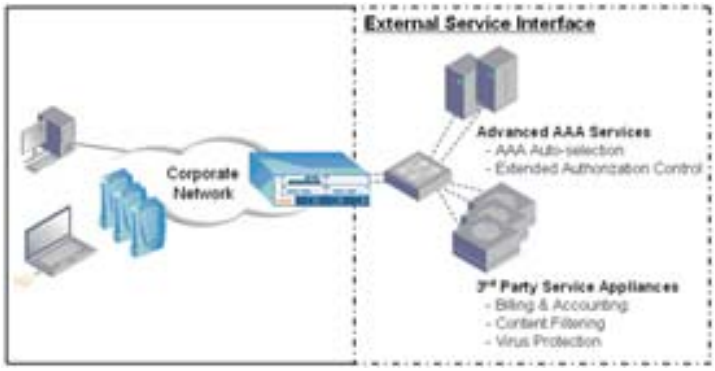
ArubaOS ESI Module

The External Services Interface (ESI) software module provides standards-based extensibility, allowing an Aruba mobility controller to communicate with external service devices and support advanced interaction with AAA infrastructure.

The ESI selectively redirects interior network traffic, based on policy, 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. Advanced Application Programming Interfaces (APIs) provide integration with these external systems as well as with AAA servers. These systems are most effective when they can directly control the authentication and authorization state of wireless clients.



Aruba's External Services Interface (ESI) software module for ArubaOS enables the scalable, seamless extension of WAN services throughout the network and supports advanced interaction with AAA infrastructure

FLEXIBLE DELIVERY OF NETWORK SERVICES

- Expands network-based services from the DMZ to all interior users, 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

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 or a flexible XML API

AAA AUTO-SELECTION

- Redirects users to different authentication servers based on a fully-qualified domain name or realm
- Simplifies corporate mergers and consolidations where multiple authentication servers must be integrated

FLEXIBLE DELIVERY OF NETWORK SERVICES

As networks transform to support an increasingly mobile workforce, services that were built for fixed networks must be extended to accommodate mobility.

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. Aurba'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. Thus, they 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.

EXTENDED AUTHORIZATION CONTROL USING 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.

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.

AAA AUTO-SELECTION

Aruba's ESI module now lets enterprises and service providers to provision AAA auto-selection, which redirects users to different authentication servers based on fully qualified domain name (FQDN) or realm. Realms and domains are commonly used in authentication systems. A realm is normally the first part of a username, separated from the actual username by a leading slash. In a Windows Active Directory network, the Active Directory domain is used as the realm. Usernames also often appear in the FQDN format. These addresses appear similar to an email address (eg. "bob@acme.com").

Enterprises can now use this capability to authenticate users from different organizational units. Especially in the case of corporate mergers, it may take months or years to merge the IT infrastructure. Aruba's ESI module makes this integration easy. Realm-based selection of authentication servers allows the users of both companies to use the same network infrastructure while identity information continues to be managed by two different directory services.

SPECIFICATIONS

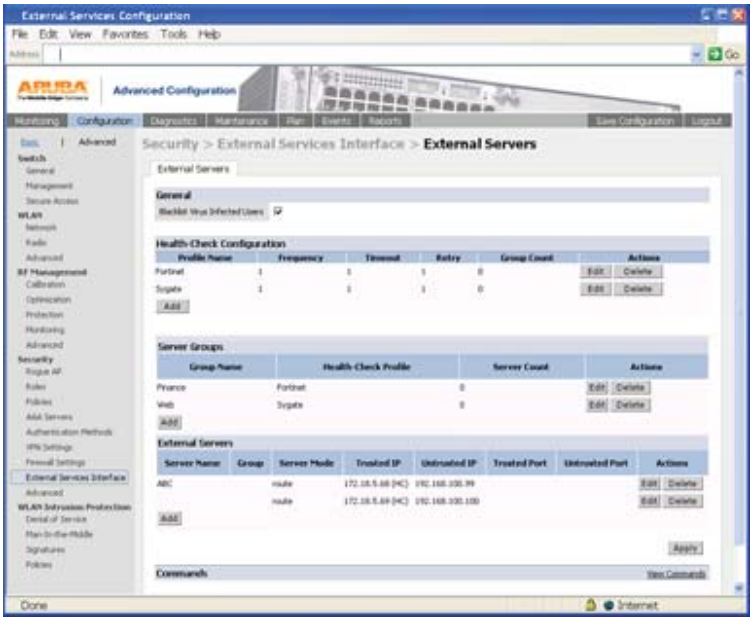
Topologies Supported
Transparent (L2)
Routed (L3)

Load Balancing Methods
Source IP-Destination IP Hash

Health Checking
ICMP Echo
L2 MAC Frame

External Service Pools
16

Service Devices Per Pool
16



External Services Interface configuration screen

FEATURE	BENEFIT
Policy-based access control	• Forward specific traffic from select users to external devices for inspection
Open interface	• Provides an open, yet secure interface for integration with best of breed 3rd party devices
Load-balancing optimization	• Forwards traffic to a pool of service devices to avoid overloading any one device • Avoids single points-of-failure while ensuring network responsiveness
Fault-tolerant	• Enables health checking of service appliancesl • Prevents traffic from being sent to a failed device
Flexible deployment options	• Permits deployment under varied network topologies; service appliances may be directly attached to mobility controllers or attached to common intermediary devices
Extended Authorization Control	• Dynamically change user's access rights, which can be used to adjust a user's bandwidth, disconnect a user from a network or open and close 'walled gardens' on the fly
AAA Auto-Selection	• Merge departments and organizations easily by mapping authentication requests to different authentication servers based on realm or domain

ARUBA™
The Mobile Edge Company
www.arubanetworks.com

1322 Crossman Avenue
Sunnyvale, California 94089
Tel: 408.227.4500 • Fax: 408.227.4550

7.06.SSESI.mp.10.1