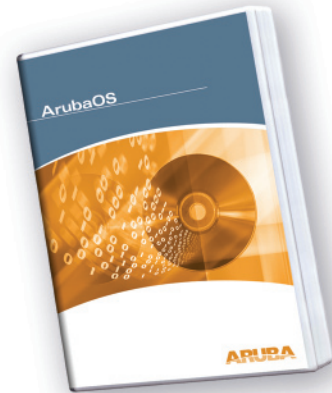


## ArubaOS ESI Module

Aruba Networks External Services Interface (ESI) software module extends multiple network-based services to the mobile edge by enabling any Aruba mobility controller to communicate with external service devices. The ESI selectively redirects interior network traffic, based on policy, to best-of-breed devices providing in-line network services such as virus protection, network intrusion detection, content filtering, content transformation and usage auditing.



### FLEXIBLE DELIVERY OF NETWORK SERVICES

- Expands network-based services from the DMZ to all interior users
- Enables centralized services with no change to wiring closets
- Connects with any network-based service device via open interface
- 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

- Conducts health checking to ensure availability of external devices
- Prevents traffic from being sent to a failed device

### EXTENDING WAN INTERFACE SERVICES TO MOBILE USERS

As networks transform to support an increasingly mobile workforce, services that were once only required at the WAN interface are now critical at all points in the network. The introduction of mobile computing has opened the entire network to external threats.

Client devices such as laptops, PDAs and voice handsets are designed for mobility; they no longer stay in the office, and can no longer be “trusted.” Where in the past, perimeter defenses deployed at the WAN interface would protect against network threats, these mobile devices now connect inside the perimeter. IT managers are struggling to determine how to extend and scale services typically only found at the WAN interface across the entire network.

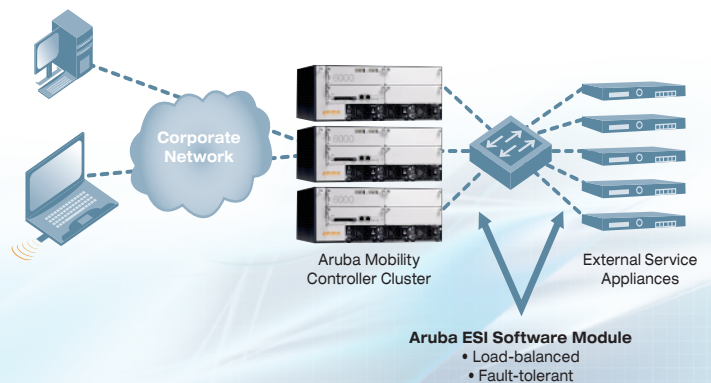
Aruba’s ESI software module for ArubaOS is the industry’s first solution to enable scalable, seamless and intelligent extension of these services from the WAN DMZ to all users throughout the mobile enterprise network.

### 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, 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, 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 require an excessive number of devices to support the traffic load and lead to performance bottlenecks. The Aruba ESI’s policy-based traffic redirection capability enables the network to forward only 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. On the other hand, 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. Alternatively, 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

Aruba Networks' mobility controllers support health checking of external devices in ESI pools. 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 devices in the pool, the system will ensure that traffic is not redirected to a device that is down. Aruba mobility controllers also utilize the Virtual Router Redundancy Protocol (VRRP) to provide resiliency in the event of a mobility controller failure.

### SPECIFICATIONS

#### Topologies Supported

- Transparent (L2)
- Routed (L3)

#### Load Balancing Methods

- Source IP-Destination IP Hash

#### Health Checking

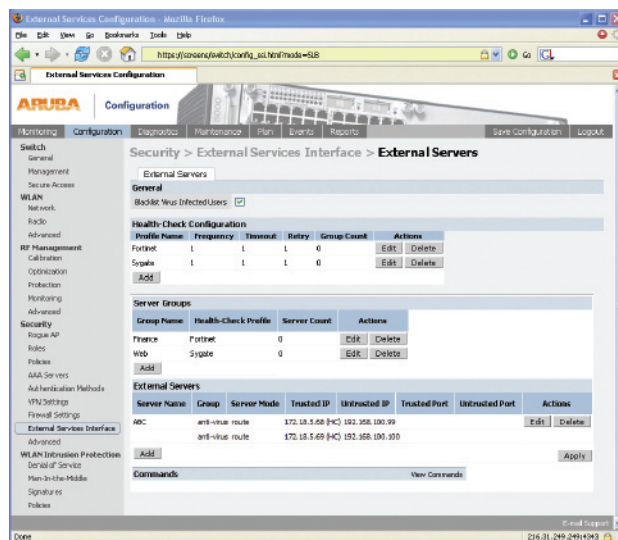
- ICMP Echo
- L2 MAC Frame

#### External Service Pools

16

#### Service Devices Per Pool

16



External Services Interface configuration screen.

#### FEATURE

#### BENEFIT

##### Policy-based access control

- Allows only selected types of traffic to be forwarded to external devices for inspection

##### Open interface

- Allows enterprises to continue using their current devices and vendors of choice
- Allows integration with best-of-breed solutions to avoid vendor lock-in

##### Load-balancing optimization

- Forwards traffic to a pool of service appliances to avoid overloading any one device
- Avoids single points-of-failure while ensuring network responsiveness

##### Fault-tolerant

- Enables health checking of service appliances to determine if the device is operational
- Prevents traffic from being sent to a failed device

##### Unlimited scalability

- Allows additional mobility controllers and service appliances to be added as network traffic grows, supporting virtually unlimited scalability

##### Flexible deployment options

- Permits deployment under varied network topologies; service appliances may be directly attached to mobility controllers or attached to common intermediary devices