



Mirage NAC™ Full-Cycle Module: Advanced Threat Protection

According to leading analyst firm Gartner, a complete Network Access Control (NAC) solution plays a critical role in a robust network security strategy designed to protect an organization from data theft and network compromise. Complete NAC offers both pre- and post-admission checks, as well as quarantine and remediation of offending endpoints.

Full-cycle, self-contained NAC from Mirage Networks® delivers complete network protection within a flexible, scalable, and easy-to-implement approach. The product family includes the Mirage NAC core software, which offers best-of-breed threat mitigation based on patent-pending behavioral rules, and the Full-Cycle Module™ (FCM), which complements the Mirage threat-termination functionality with policy enforcement and advanced threat mitigation. The FCM delivers:

- » Enforcement of policy on entry and on the network
- » User-appropriate quarantine options
- » Policy-driven remediation of endpoints

POLICY ENFORCEMENT

The FCM comes with built-in policy checks that determine the following characteristics about any device entering or on the network:

- registered or unregistered device status
- operating system
- services running
- threat and policy compliance history
- VLAN entered

This enables IT to easily triage at-risk devices by defining critical risk characteristics according to security policy and user type, and to take user-appropriate action including: sending the device to specific quarantine areas for deeper checks and remediation; limiting the device's network access to certain traffic types, speeds, or network areas; or revoking the device's network access altogether.

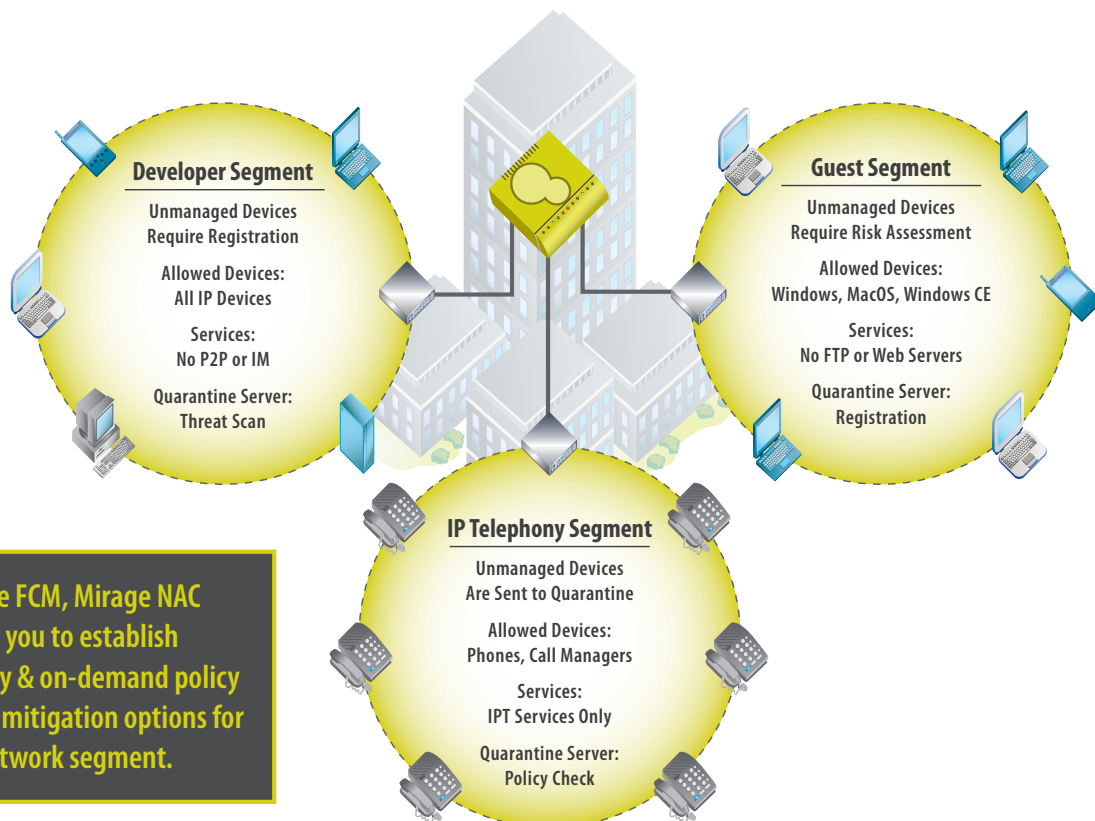
For deeper endpoint checks, Mirage offers integrations with the technology of leading security vendors, including authentication, vulnerability scanning, antivirus management, policy management and enforcement, patch management and security information management. By way of the Mirage API, Mirage NAC can either trigger a third-party security action, or

take direction from the third-party solution to serve as the point of policy enforcement.

With the FCM, Mirage NAC checks endpoints for policy violations and threats both on entry to the network and continually while on the network. At any time, should a risk be discovered on a device, Mirage NAC can, through integration enabled by the Mirage API, trigger third-party solutions to take action, from deep policy vulnerability scans to patching operating systems to authentication and more. These, in turn, can deliver results of the scans, checks, and remediation actions to the Mirage NAC appliance, resulting in policy-driven action, such as network readmission, continued quarantining for further remediation, or lockout from the network entirely.

PRE-ADMISSION NAC

At network entry, the FCM enables scanning of all devices entering sensitive, customer-defined areas of the network, such as guest subnets reserved for use by contractors. The FCM can also be configured to trigger third-party endpoint scanning and remediation only for a specific range of IP addresses. IT can choose to quarantine the device and scan it before allowing access to the network, or to have the scans run in the background, enabling users to continue using the network while the risk is still being assessed, in the knowledge that Mirage NAC's behavioral rules are in force at all times to prevent any threat propagation.



With the FCM, Mirage NAC enables you to establish on-entry & on-demand policy scans & mitigation options for each network segment.

POST-ADMISSION NAC

To ensure post-admission security, the FCM scans all network traffic for indications of policy violations, both continually and on-demand. Additionally, the FCM can be configured so that a device is either tracked or automatically quarantined when a Mirage NAC rule is broken, indicating a potential policy violation. An example might be when a user attempts to access a server that he should not, or when a non-IP telephony device attempts to get on an IP telephony LAN.

QUARANTINE AND REMEDIATION

Mirage NAC delivers first-level quarantine and remediation options by surgically removing an offending device from the network and informing the user of this status through a browser window. While in quarantine, the offending devices are isolated to prevent cross-infection with other at-risk devices. The FCM expands on these capabilities, redirecting quarantined endpoints to user-appropriate Web remediation servers, which can be customized with remediation options, such as:

- No network access until remediation is complete
- Limited network access, such as Internet access only, until remediation is complete
- Redirection of the device for user-appropriate remediation

This functionality and flexibility enable organizations to leverage existing security technology, to increase user productivity by decreasing remediation time, and to reduce support costs.

DEPLOYMENT

Like the entire Mirage NAC family, the Full-Cycle Module is OS- and device-agnostic, and does not require network rearchitecture.

Each network segment or segment set with a Mirage NAC appliance can use its own Web remediation server, to ensure user-appropriate mitigation. In the event that the Web remediation server is hosted behind a proxy server, this network traffic requires a non-standard Web port.

The Mirage API enables additional security activity, providing integration points with many leading security technology vendors. These solutions may require deployment on a separate server.

» features

- » Provide comprehensive NAC coverage
- » Enable users to self-remediate
- » Automate policy enforcement
- » Track devices and their security history
- » Ensure policy enforcement on entry and on network

» benefits

- » Achieve more control over the devices accessing the network
- » Ensures that devices on the network adhere to corporate policy
- » Address at-risk devices to prevent rapidly propagating infections
- » Increase productivity by reducing remediation time
- » Decrease IT help desk burden and support costs

SYSTEM REQUIREMENTS

Web Browser Support

- Microsoft® Internet Explorer® version 6
- Mozilla® Firefox® version 1.0.7
- Apple® Safari® version 1.3.1

The Mirage NAC Full-Cycle Module works with the following components:

- Mirage NAC Appliances: N-125, N-145, N-245, N-245HA
- Mirage Management Servers: M-SW, M-2050, M-2060

Note: if integrating Mirage NAC with a third-party security solution, this may require additional system resources; requirements will vary by vendor.

You Can't Control People. Control What's On Your Network.™

IMPLEMENTATION

The FCM may be installed on a new appliance or added to an existing appliance. The FCM integrates with the Mirage NAC management options, which provides centralized monitoring and management of all Mirage NAC appliances in your environment.

About Mirage Networks

Mirage Networks is an Austin, Texas-based network security company dedicated to delivering real world, complete network access control solutions, serving the enterprise through a strong channel of resellers, original equipment manufacturers and managed security service providers. Mirage solutions ensure a user-friendly and IT-friendly experience that never forces a compromise between business objectives, effectiveness and usability. The company's passion for innovation has paved the way for the development of patent-pending behavioral technology that consistently wins industry awards. Contact us today to learn more about the industry's only self-contained network access control solution.

Contact Us Today:

Mirage Networks
6801 North Capital of Texas Highway
Building 2, Suite 200
Austin TX 78731

phone: 866.869.6767

fax: 512.874.7806

email: info@miragenetworks.com

web: <http://www.miragenetworks.com>