

BlueCat Networks Authenticated Access Control



Build Scalable, Hygienic Network Infrastructure

Ranked the best by Network Computing Magazine™, the BlueCat Networks Adonis DNS/DHCP Appliance™ and Proteus Enterprise IPAM Appliance™ family is consistently selected to provision scalable and secure IP address infrastructure for government, military and enterprises world-wide.

Protection Against Zero-Day Exploits

Beyond the necessary firewalls for perimeter defense, organizations have deployed anti-virus, anti-spyware and other defense tools within their networks. Despite widespread use, these tools are only as good as the last update and provide little protection against zero-day exploits.

DNS and DHCP are the building blocks of your network and must be protected from exploit.

Beyond the necessary fire-

Policy-Based – Dynamic Threat Mitigation

BlueCat Networks™ and Mirage Networks™ have partnered to build secure, scalable networks that offer advanced “defense-in-depth” protection against zero-day exploits. Together, Mirage and BlueCat provide a solution that goes beyond traditional Network Access Control (NAC) tools to provide security at network entry and post-admission, for both dynamic and static IP environments. The unique architecture of the Mirage NAC™ solution provides policy based post-admission security without introducing software agents or network latency. The BlueCat/Mirage joint solution is effectively invisible to end users and is a logical extension of your existing network infrastructure.



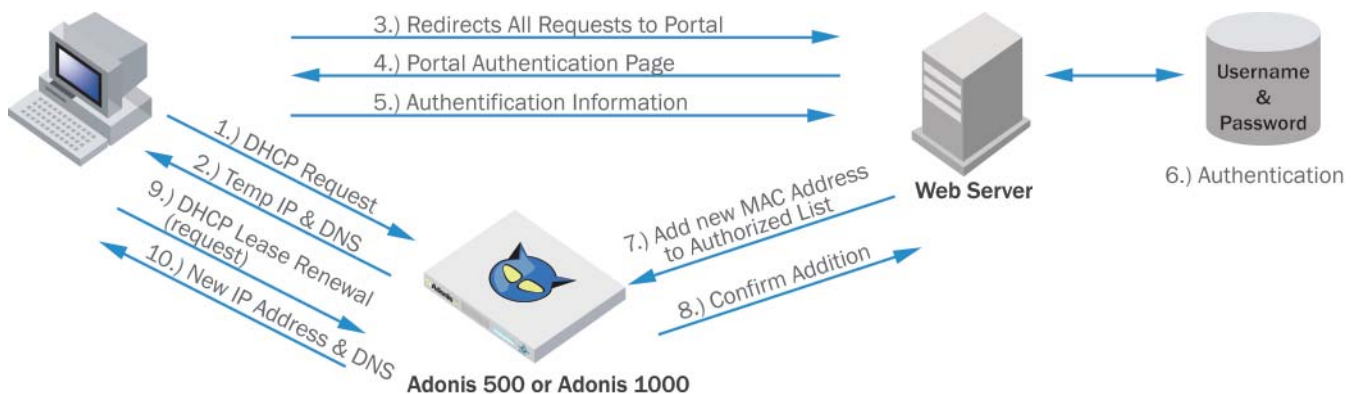
Solution Overview

In a typical deployment, the Adonis DNS/DHCP appliance is used to provide pre-admission NAC screening prior to granting an IP lease to an end user. The Mirage NAC appliance sits out-of-band on the network and provides constant monitoring of IP traffic. Upon detection of a threat or policy violation, the appliance will quarantine the device, optionally interacting with Adonis to revoke the IP address lease and terminate the affected device’s connectivity.

A user connects to the network and requests an IP address lease from the Adonis built-in DHCP server and Pre-Admission NAC Module. The user is authenticated using LDAP, RADIUS, Active Directory

or Kerberos and their MAC address is checked prior to being assigned an IP address. The Adonis appliance maintains a database of all users accessing the network by MAC address and IP address lease; this database is updated whenever new IP leases are granted. Adonis assigns addresses only to those users who have been properly authenticated.

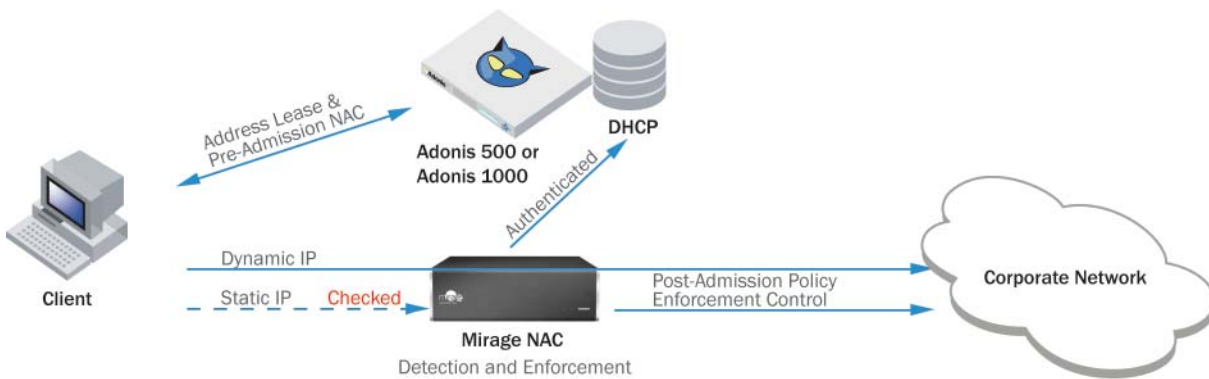
Enterprise Network Hygiene Control



Mirage NAC appliances continuously monitor devices on the network for non-compliant behavior and propagation of malware. A malicious user might try to enter the network and bypass the DHCP authentication check by setting a static IP address. The Mirage NAC appliance detects the static IP address when it enters the network, then quarantines the device and forwards all traffic to the Captive Web Portal Server. The user is authenticated (just as for DHCP address entry). If the user passes authentication, Mirage NAC removes the quarantine and enables full access to the network. If the authentication fails, then the user remains quarantined.

Mirage NAC continuously performs risk assessment of devices on the network to identify behaviors that could indicate policy

violations and threat propagation; to determine whether the device is permitted on the chosen network VLAN; and to determine whether the device is running services that are not permitted (such as IM). Checks include: valid services; device or OS type; wired or wireless access, and managed or unmanaged endpoint status. The Mirage NAC will either quarantine devices that violate these 'checks', or send them to the customer's vulnerability scanner or patch site for deeper checks. When quarantined, the user is directed to a portal for information on the security situation, self-help remediation steps that the user can take, and for information on how to contact IT if required. Once remediation is complete, Mirage NAC™ can automatically readmit the device to the network.



Network Hygiene Solution Benefits

- The combined BlueCat/Mirage solution provides comprehensive Network Access Control for the entire network address space, from the time that devices connect to the time that they disconnect; complete security throughout pre-admission, authentication and post-admission phases.
- Customers achieve comprehensive Identity Management with pre-admission authentication using a combination of MAC filtering and LDAP/ RADIUS/AD/Kerberos services. This solution integrates seamlessly with the Proteus 5000 Enterprise IPAM Appliance™ for enterprise-wide network hygiene.
- IT departments benefit from simplified deployment model: no endpoint agent software and no switch integration required, built-in quarantine capabilities for un-authenticated users.
- The out-of-band solution prevents a single point of failure.

Comprehensive Network Access Control

Additional Integration Possibilities

- Using the IP lease data (IP/MAC/User Name) available to them, corporate help desk staff would proactively know which users were having difficulties, thereby simplifying trouble ticketing in case of quarantine service call.
- The combined solution can be integrated with other network access controls such as CNAC, MSNAP, and TCG NAC, providing a defense-in-depth approach.

Simplified Seamless Integration

Summary

The BlueCat and Mirage Hygiene Solution offers powerful yet flexible, full-cycle Network Access Control. From initial authentication, to pre-admission checks and non-intrusive post-admission checks, the integrated solution safeguards the network against zero-day attacks, policy violations, and unauthorized network access throughout the lifecycle of the network connection.

 **BlueCat Networks, Inc.**
Toll Free: 1.866.895.6931
www.bluecatnetworks.com

