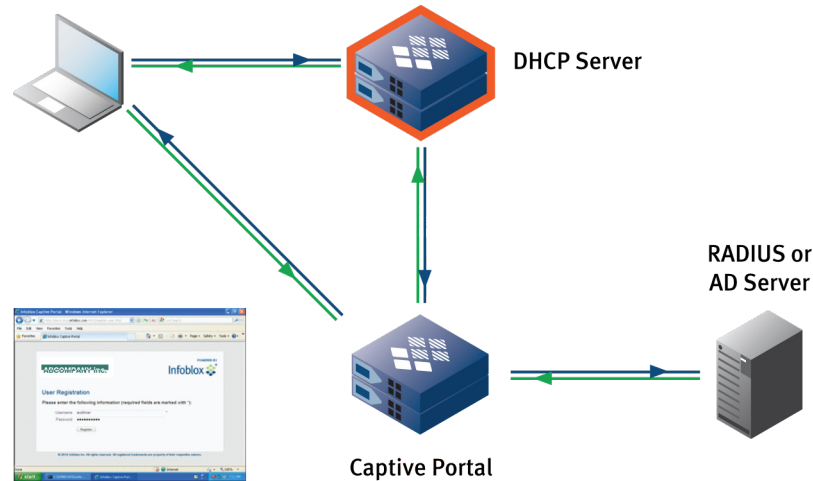


SOLUTION NOTE

Introduction

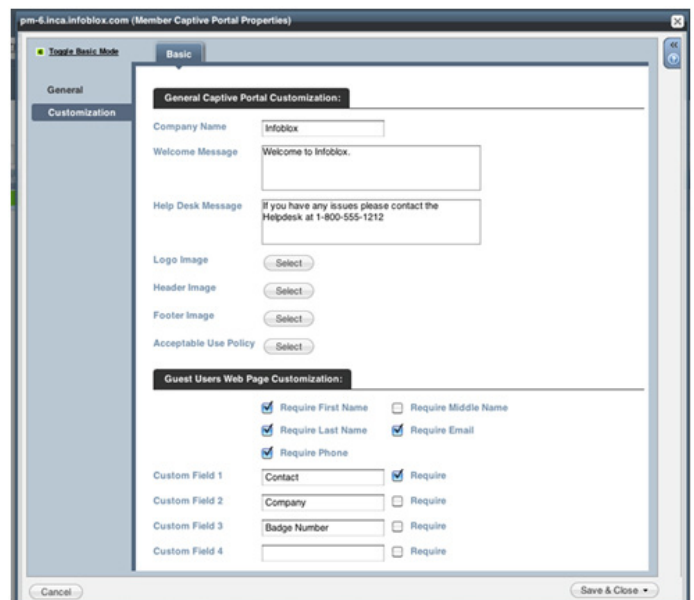
One of the ways to force user authentication before accessing network resources is through the use of a Captive Portal (which uses Authenticated DHCP). A captive portal is a web page that can provide an option to register as an authenticated user or as a guest. A network can be segmented for unauthenticated, authenticated and guest users, and the DHCP server assigns clients to the appropriate segment based on their MAC addresses and authentication credentials. For example, a network can be divided into one or more production segments for valid employees, a guest segment with access only to the Internet, and a quarantine segment with access to a captive portal only.

How does it work?



A typical case scenario would be the deployment of a captive portal on a college campus as explained below:

- A student with a wireless laptop tries to login to a web site from a college campus. A DHCP client on the student's laptop sends a DHCP request to a member DHCP server. Since this will be the first time the DHCP server sees such a request and doesn't have the MAC address of the DHCP client, the DHCP server issues the student's laptop a Quarantined IP address
- The Quarantined DHCP client is then directed to a captive portal where the student enters his/her user name and password which is then authenticated by an authentication server such as RADIUS or Active Directory
- Assuming the authentication was successful, the DHCP server adds the MAC address to the list of authenticated students and assigns the student's laptop an authenticated IP through which it can then connect to the Internet



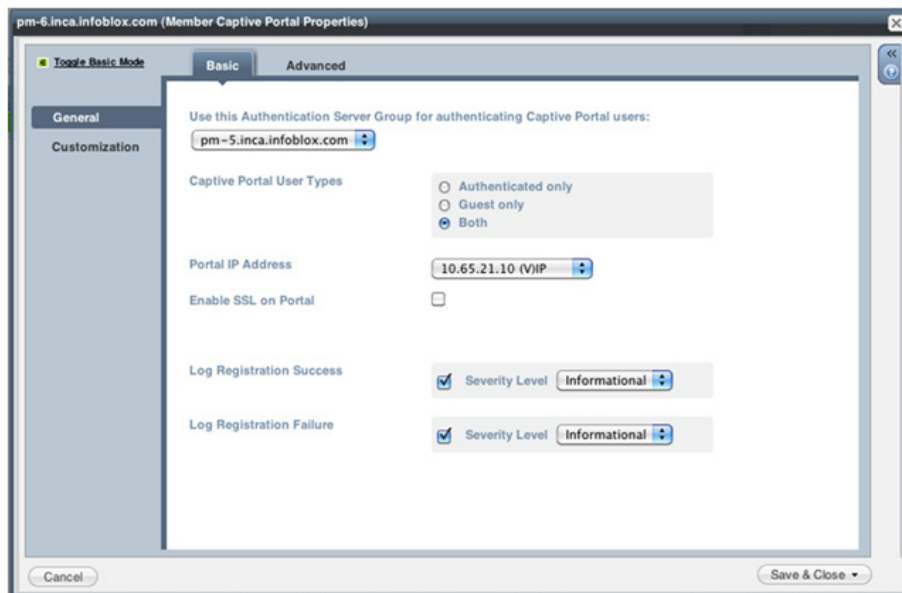
SOLUTION NOTE

- If the student authentication fails or simply logs on as a guest, the student will have limited internet access such as the ability to look only at the college web site

Deploying captive portal on a college campus will enable the implementation of a security policy that forces all students to be authenticated in order to access network resources which in turn leads to a better overall network security.

Benefit of using an Infoblox Captive Portal

- Captive Portal customization (configure Company Name, Welcome message, Acceptable Use Policy)
- Captive Portal provisioning (Run on a dedicated Grid member, supports either RADIUS or Active Directory servers)
- Captive Portal service configuration (SSL support to protect passwords, logging of success and failures)
- Captive Portal supports multiple DHCP servers
- High scalability and performance
- Included in NIOS (starting with version 5.1r3) at no additional licensing cost



Conclusion

Providing user registration and authentication through the use of a captive portal is of paramount importance in making sure that only authenticated users will have access to network services. Infoblox provides a captive portal solution that is customizable, configurable, scalable, and is included part of NIOS at no additional licensing cost.

Infoblox Product Warranty and Services

The standard hardware warranty is for a period of one year. The system software has a 90-day warranty that will meet published specifications. Optional service products are also available that extend the hardware and software warranty. These products are recommended to ensure the appliance is kept updated with the latest software enhancements and to ensure the security and availability of the system. Professional services and training courses are also available from Infoblox. Information in this document is subject to change without notice. Infoblox Inc. assumes no responsibility for errors that appear in this document.