

## SOLUTION NOTE

### A Joint Solution from Infoblox and Juniper

#### Dynamic Network Access Control

Network access control (NAC) is a term that has come to mean many things to many people. For the purposes of this discussion, NAC refers to the ability to apply policies dynamically to grant and maintain (or terminate) endpoint access to networks and applications. While this sounds simple enough in concept, implementing NAC has proved problematic for many organizations. The devil is in the details: Implementing NAC can be straightforward if all of the networking and security equipment in the network is from a single vendor, all endpoints are known and have endpoint security software installed, and if all devices are smart enough to support username/password or a similar type of authentication. In practice, these “ideal” conditions rarely exist:

- Even organizations that have a primary supplier for their networking equipment often use equipment from multiple vendors—for example, many organizations use security equipment such as firewalls and IDP/IDS from “best of breed” suppliers that are different from their network equipment vendor.
- Unmanaged endpoints, such as laptops owned by contractors or joint venture partners, are commonly found in today’s corporate network.
- Increasingly, the devices on a network are things such as sensors or machines that don’t have an interface or the intelligence to support end-user authentication.

These complexities typically make it necessary to either implement a highly restrictive network environment in which only known devices can connect, or else to implement an environment that leaves many security holes open in order to accommodate unmanaged devices and guest users.

The example below describes a dynamic network access control scenario that leverages IF-MAP to support fine-grained security policies for both managed and unmanaged endpoints, both pre and post admission:

A global organization, call it ABC Co., operates small remote sites around the world, often in spaces shared with competitors. End devices at each remote location, which can include PCs, laptops, printers, bar code scanners and others, connect to a local switch which is in turn connected to a local firewall that provides a VPN tunnel back to the organization’s main datacenter. On occasion, users at the remote sites need to “swap” locations with a competitor, who will then plug their devices into the remote firewall. Of course, the competitors should not be granted access to ABC Co’s datacenter. ABC Co. needs a way to dynamically establish firewall policies at the remote locations for the managed and unmanaged devices that periodically connect.

The local switches are from several different vendors, so using a single-vendor solution isn’t possible. Each of the switches is configured for 802.1X port authentication. Managed PCs and laptops have an 802.1X supplicant and support end-user authentication. Unmanaged devices—either guest PCs without 802.1X supplicants or “dumb” devices (like bar code scanners) authenticate via MAC authentication (i.e. their MAC address is passed to the RADIUS server in response to the 802.1X challenge).

The solution uses three IF-MAP compatible products: A Juniper Infranet Controller (IC) which provides RADIUS-based authentication for 802.1X and also provides a policy engine; an Infoblox Core Network Services appliance with an IF-MAP client integrated with the DHCP server; and an Infoblox Orchestration Server appliance that provides an IF-MAP server.

## SOLUTION NOTE

The Juniper IC has the ability to dynamically configure firewall policies; however, to do so it requires the IP address of an attached device (because firewall rules are based on IP address). This is where IF-MAP comes in. First, the end device plugs into the 802.1X switch, which challenges it to authenticate. In this case the device is a PC with a RADIUS supplicant. The user provides their login credentials via the supplicant and the switch provides the login information to the Juniper Infranet Controller as part of the RADIUS request, which also contains the end device's MAC address. The Infranet Controller does a lookup in a backend authentication system and retrieves the user's role and rights as part of the authentication. Based on successful authentication, the Juniper IC communicates with the switch and enables the port. It also publishes the MAC address and a session ID to the IF-MAP server, and posts a subscription on the MAP server asking for notification of any changes associated with the session ID address just published.

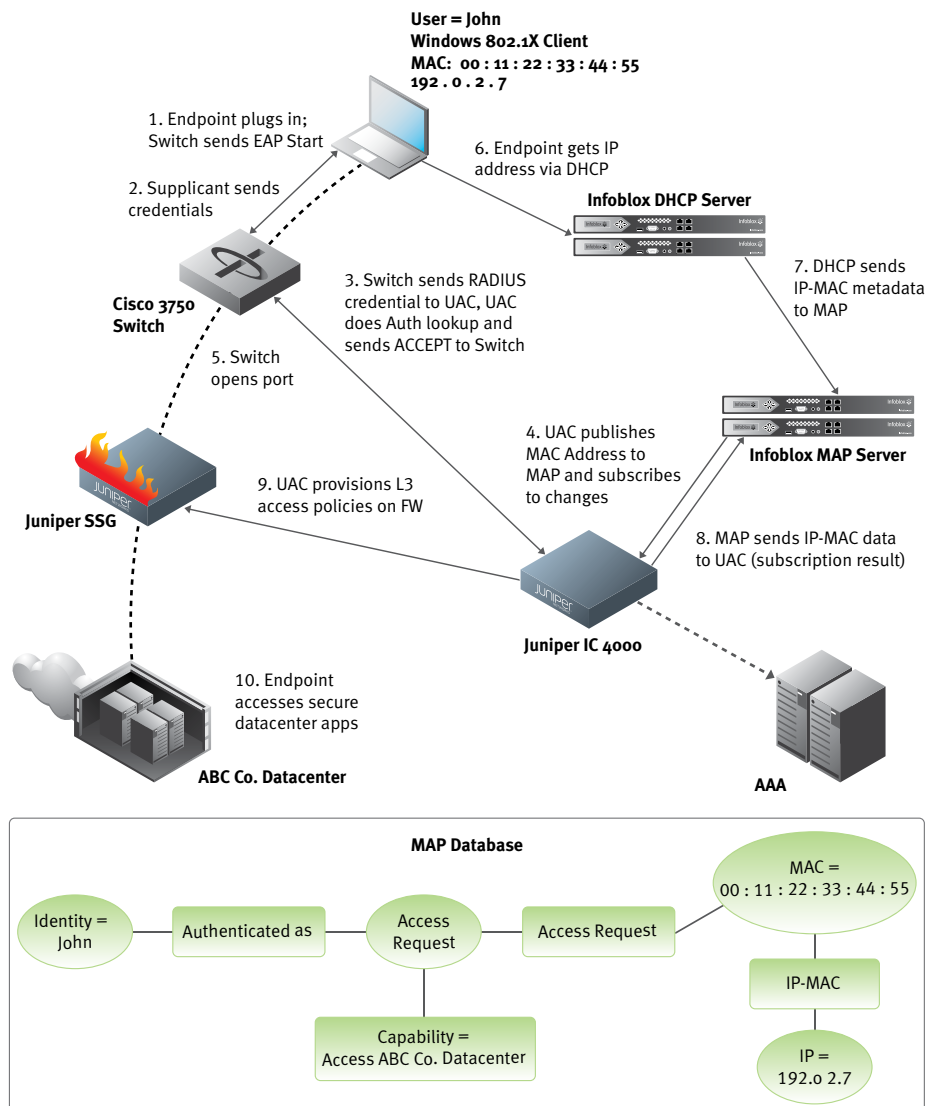


Figure 1: IF-MAP enables the Juniper IC and the Infoblox DHCP server to update one another without direct integration between the two systems.

## SOLUTION NOTE

With the switch port enabled, the end device issues a DHCP request, which is fulfilled by the Infoblox DHCP server. The Infoblox DHCP server publishes the IP-MAC address link to the IF-MAP server with metadata indicating that this represents a DHCP lease.

Publication of the IP/MAC link to the IF-MAP server triggers the subscription that had been posted by the Infranet Controller, so the IF-MAP server sends the IP address associated with device's MAC address to the Infranet Controller (along with the session ID). Now, with the IP address known, the Infranet Controller can automatically provision the firewall (and other devices, such as intrusion detection systems) with policies appropriate for the endpoint. The Infranet Controller also posts a subscription on the IP address, so that it can be advised immediately if something happens with that IP. If at some point another IF-MAP enabled device, like an IDS, detects virus or worm traffic from the device's IP, it can publish an event to the IF-MAP server, referencing the IP address. That will trigger the IF-MAP server to send the event to the Infranet Controller, which can then send an update to the firewall, cutting off the endpoint from the rest of the network.

### Physical Access Control/Logical Access Control Convergence (PAC/LAC)

The scenario above can be taken a step further with the addition of an IF-MAP compatible physical access control (PAC) system, such as the one available from Hirsch Electronics. The Hirsch system can publish metadata to the IF-MAP server that associates a user's location with their identity based on the last door that they badged through. With this additional information, a policy server can dynamically enforce a policy that requires a user to be in the room with their PC in order to get or maintain access to the network. By subscribing to changes in user location, the policy server can receive instant updates when a user changes location, and cut off access to the network or specific applications if a user leaves their PC unattended.

### TNC, IF-MAP, and Other Standards Bodies

IF-MAP is a component of the TNC architecture that provides a standardized infrastructure for sharing information. The TNC architecture is built around three entities—an access requestor (AR), a policy enforcement point (PEP), and a policy decision point (PDP). An AR is any endpoint, such as a laptop, initiating a connection. The 802.1x environment would call the AR a supplicant. Client hardware and any software supporting authentication and assessing endpoint security are included in the AR. A PEP is any device or system, such as a switch or firewall, performing an enforcement action, such as blocking network access. The PEP also controls the level of access granted to the endpoint. The PDP is typically a policy server or management system where IT defines and distributes the policies implemented by the PEPs. The PDP also communicates with the authentication server and to pass verification information to ARs.

IF-MAP's MAP Server and MAP clients extend the TNC architecture for communication with other systems. The MAP Server, or simply MAP, stores state information about devices, users, and traffic flows in a network. MAP Clients are the network systems or applications that publish information to a MAP Server, search the information in a MAP Server, and subscribe to notifications from a MAP Server when information stored in the server changes.

IF-MAP is an open standard that can be adopted by communities of related vendors, service providers and end users in applications beyond network security. IF-MAP can thus be used by other standards bodies in much the same way as it's used by TNC: Specifically, as a component that extends the standards to enable easy integration with previously unrelated systems.

#### 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.