Network Access Control Testing

26601 Agoura Rd
Calabasas, CA 91302
(Toll Free US) 1.877.FOR.IXIA
(Int'l) +1.818.871.1800
(Fax) 818.871.1805

www.ixiacom.com

White Paper

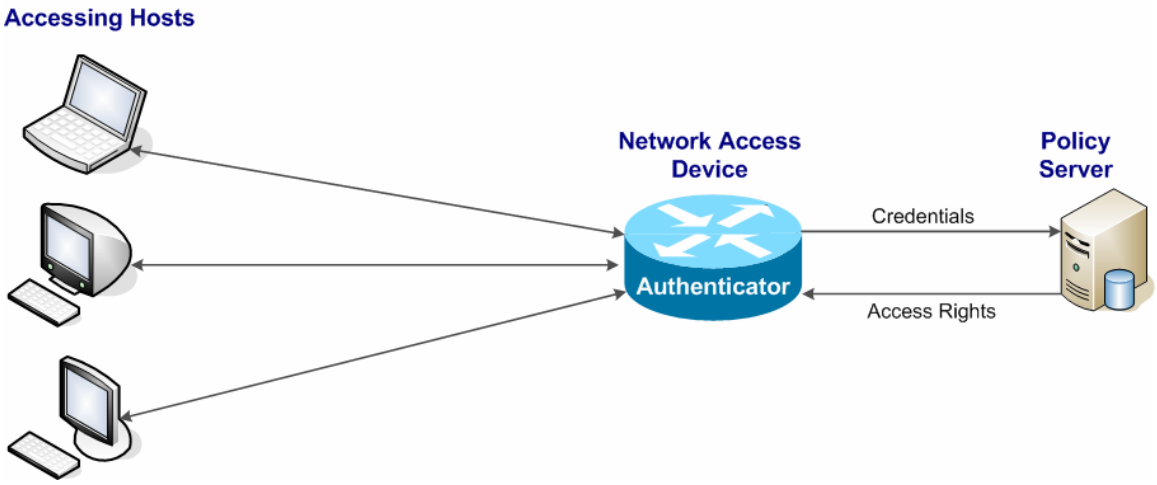
Network admission control (NAC) is an industry term encompassing a set of technologies and solutions that work synergistically to offer enhanced network admission control. NAC uses network infrastructure components to enforce compliance to security policies on all devices seeking to access network resources in order to limit damage from emerging security threats.

This white paper discusses Ixia's NAC test solution, which permits network equipment manufacturers to test the performance of their NAC devices before bringing them to market. This paper will also discuss how both enterprise users and system integrators can cheaply and efficiently test their network designs before deployment. Using Ixia's leading NAC test solution will lead to savings in time, effort and cost. Ixia's NAC test software provides detailed performance statistics that make it easy to compare and quickly determine the suitability of various NAC offerings for a particular environment.

How does NAC work?

The NAC framework involves three network elements:

1. Hosts requesting access to the network.
2. Access device these hosts are connecting to.
3. Server making authentication and authorization decisions based upon an access policy set by the user.



The function of a **network access device** is to act as the enforcement point of policy that is implemented on the policy server for hosts trying to access network resources.

Each of these hosts has a software agent that reports to the network access device the current status of various software components installed on the host. The reported data may include information about the operating system installed, e.g., Windows XP or Linux, plus the particular version of the operating system, and the anti-virus patch version. Based upon this information, the policy server can decide whether the host requiring network access meets the configured criteria for granting access.

Based upon the status information received, if the requesting host is out of policy it may be placed into "quarantine," where it will have the opportunity to redress the security weakness detected. In the case where it complies with the access policy, it is declared "healthy" and allowed access to the network. If it is found to be a threat to other hosts on the network, it is declared "infected" and denied network access by the network access device.

Why Ixia NAC testing?

Ixia's NAC test solution builds upon Ixia's market leading test software.

- Reduction in time to market – using Ixia allows the user to go through their test cases in significantly less time, which leads to faster development, validation, and testing cycles.

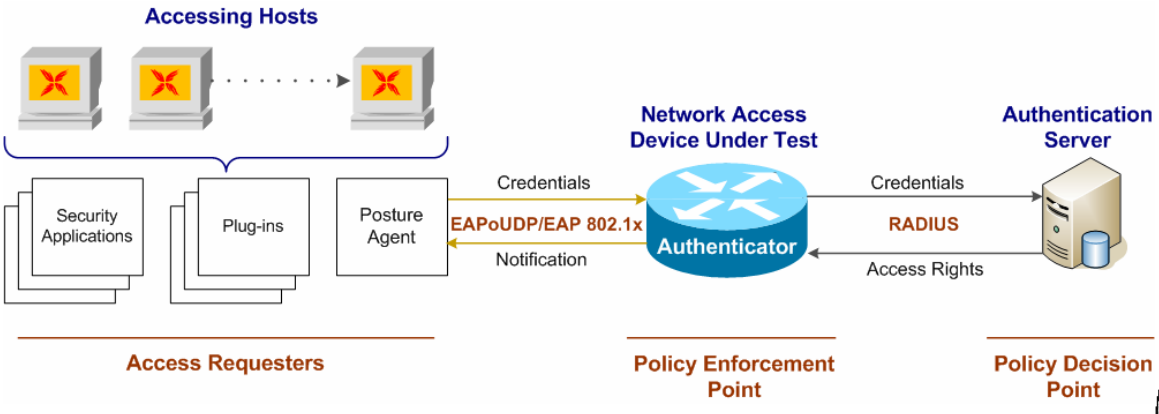
- Reduced testing CAPEX – using Ixia the NAC test solution makes it unnecessary to buy thousands of servers to do the same testing achieved by just a few ports on an Ixia chassis.
- Faster deployment – efficient testing of a NAC implementation before deployment in a production network will ensure easier and faster deployment.

- Reduced operational costs – validating a NAC design before its actual design will help to diagnose problems before they occur, resulting in significant savings in operating costs
- Ease of use – users can test large network designs, using the market-leading IxNetwork™ GUI with only minimal training.

Ixia NAC solution overview

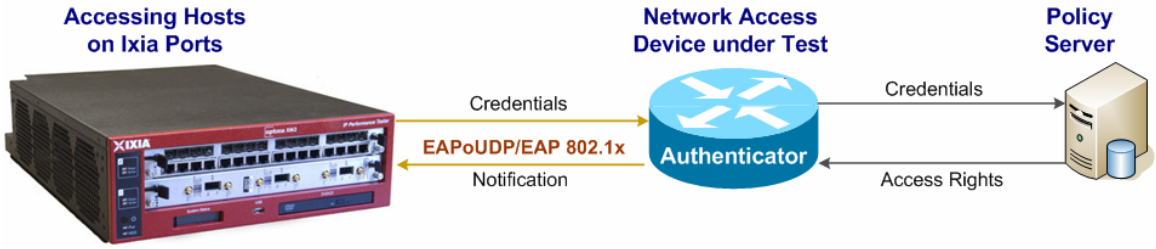
Architecture

The ports on the Ixia chassis emulate hosts requiring network access. All security-related information on the host that is relayed to the network access device is emulated on the Ixia ports – from installed security applications, to plug-ins, to the posture agent, which report security data to the access device, using either EAP or 802.1x authentication protocols.



Ixia ports can simulate thousands of these hosts, which makes it possible to test more realistic performance characteristics of network access devices and authentication servers, while at the same time achieving reduced time-to-market and CAPEX goals.

Ixia's unified test platform makes performance upgrades easy and protects investments in software and hardware. Any Ixia load module (line card) can be installed on any Ixia test chassis. And Ixia's NAC software will run on the resulting hardware platform as well as future configuration of Ixia components.



Ixia NAC Solution Test Scenario

In the following simple test scenario, the user wants to test the performance of their access device and authentication server. The Ixia-emulated hosts, running Windows 2000, accessing the network are assigned three different tokens by the policy server, depending upon based upon security applications and plug-in data conveyed to the network access device by the posture agent.

The user has configured the expected token that the network access device and authentication server should return, based upon the configured access policy.

EAPoUDP Posture Sequence List

	Name
1	Win2k_Infected
2	Win2k_Quarantine
3	Win2k_Healthy

EAPoUDP Posture List

		Name	Expected System Token
1	☑	Win2k_Healthy	Healthy
2	☑	Win2k_Quarantine	Quarantine
3	☑	Win2k_Infected	Infected

Import Export

EAPoUDP Application State List

		Name	Vendor	Application	Attribute	Value Type	Value
5	☑	Cisco:PA:OS-Type	Cisco	PA	OS-Type	String	Windows 2000
6	☑	Cisco:PA:OS-Version	Cisco	PA	OS-Version	Version	5.1
7	☐	Cisco:PA:PA-User-Notifi...	Cisco	PA	PA-User-Notific...	String	
8	☐	Cisco:PA:OS-Release	Cisco	PA	OS-Release	String	
9	☐	Cisco:PA:Kernel-Version	Cisco	PA	Kernel-Version	Version	

26601 W. Agoura Road Calabasas, CA 91302 • Tel + 1-818-871-1800 • Fax + 1-818-871-1805 • www.ixiacom.com

Based upon this configuration, Ixia will verify if the incoming hosts are assigned the proper tokens: “healthy” for emulated hosts that comply with the policy, “quarantine” for emulated hosts that need to be moved to a remediation network, and “infected” for those hosts that are an active threat to other hosts in the network and need to have their network access severely restricted or even denied.

Summary

Ixia’s NAC testing solution affords the user the ability to conduct testing with Ixia’s leading test software, which provides ease of use with real-world emulation, while at the same time reducing time to market, CAPEX and OPEX.

The Ixia’s solution is suited for network equipment manufacturers, system integrators and enterprise users seeking to qualify technologies for their networks.

For more information, please contact Ixia at http://www.ixiacom.com/contact_us/

About Ixia

Ixia is a leading provider of performance test systems for IP-based infrastructure and services operating in over 30 countries worldwide. Service providers, network and telephony system vendors, semiconductor manufacturers, governments, and enterprises use Ixia's test systems to validate the capability and reliability of complex IP networks, devices, and applications.