ADVERTISEMENT

NETWORKWORLD

by **Tim Greene**
Executive Editor

Burning NAC questions – Part 2

News
Oct 17, 2007 • 7 mins

Cisco Systems Networking

Part 2 of 2. In second part of our look at important network-access control issues, we take a look at important questions surrounding Cisco, NAC implementation and NAC policies. Review part 1 here.

Shouldn't I just wait for Cisco?

Should I deploy a NAC appliance in-line or out-of-band?

What is the best method of enforcing NAC policies?

Shouldn't I just wait for Cisco?

There's really no need to wait because depending on what you want out of NAC, Cisco may already have it.

And if Cisco doesn't yet offer what you want, there is still no need to wait because you can get alternatives from other vendors.

Cisco has a NAC appliance that can check devices before they get network access for virus software that it is updated and turned on and whether patch levels meet policy.

That said, the device is criticized by some for what it cannot do. "Cisco remains behind many of the other vendors in this space because of the inability to perform assessment checks beyond initial connection," says Mandy Andress in her recent review of the appliance for *Network World*.

For example, the device does not perform periodic rechecks of devices once they have been admitted to the network to make sure they maintain their security posture.

The Cisco NAC Appliance does afford multiple enforcement methods, including placing the device inline with traffic where it can restrict traffic directly, having it work in tandem with 802.1X authentication or running it out of band where it controls an access switch. It can also enforce NAC for devices attaching via SSL or IPSec VPN through Cisco gear.

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 1 of 6
INFOEXPRESS, INC. - EX2525

There are other appliances from other vendors that do more, and if Cisco's appliance comes up short, these others can fill the bill.

Cisco also has a scheme that builds NAC into its network architecture, a design that scales better for large rollouts. One of the problems all NAC customers face is that NAC appliances in general don't scale large enough to accommodate a major corporate-wide deployment without relying on many appliances, says Rob Whiteley, an analyst with Forrester Research.

Cisco's network-based NAC requires certain switch specifications that may mean upgrades for some customers. As a result, some are holding off until they need to upgrade.

One problem customers see with Cisco NAC is that it has two separate designs that don't have interchangeable parts. Currently Cisco NAC Appliance and its network-based NAC Framework have separate clients to evaluate the security posture of network endpoints.

Also, the NAC Framework relies on Cisco's Access Control Server (ACS) to determine which access policy to apply while the NAC Appliance relies on its own management server to determine if endpoints are in compliance.

Cisco has a migration strategy called OneNAC to simplify the transition between appliance and network-based NAC with interchangeable clients and a single server. But that plan still has some details to be ironed out.

Regardless of its comparative merits, Cisco's NAC has a solid base of loyal customers, according to Current Analysis' latest annual NAC study. The report says that 67% of current Cisco NAC Appliance customers and 68% of Cisco NAC Framework customers would consider buying more Cisco NAC gear.

The flip side is that the numbers imply that about a third of these customers would not consider more Cisco NAC products, but the survey doesn't state their reasons.

Should I deploy a NAC appliance in-line or out-of-band?

Neither answer is right for every case.

Ultimately for large deployments, out-of-band NAC that uses some form of edge enforcement such as access switches will be more practical because it scales better, Whiteley says. In-band NAC requires more and more devices as the rollout grows.

But for smaller networks or for targeted NAC enforcement, in-line NAC appliances can serve just as well, says Joel Snyder, a senior partner in Opus One and a member of the Network World Test Alliance. "In-band I think of more for the occasional guest access — drop one of those boxes in between your guests and let it handle that load," Snyder said in a recent Network World online chat about NAC.

Out-of-band NAC relies on existing network mechanisms to enforce policies, such as 802.1X authentication, ARP and MAC tables and DHCP assignment. It gets its name from the fact that the NAC device does not sit directly in the flow of traffic – usually it hangs off a switch port – without any direct means to restrict traffic.

In-band NAC includes devices that traffic must pass through, usually placed between access-layer devices and distribution layer devices, although some can sit between distribution and core layers of networks. In some cases, vendors have incorporated NAC capabilities in access switches themselves.

There are many arguments in favor of both methods. *Network World* asked two vendors — one selling inline gear, one selling out-of-band — to come up with the best reasons for their positions.

Quick deployment without interrupting business use of the network, no single point of failure and lower risk of creating network latency are cited as advantages of out-of-band deployment by Grant Hartine, CTO of NAC vendor Mirage Networks.

He also says out-of-band NAC gear finds devices when they send ARP packets that may be missed by in-line devices, depending on their placement.

By contrast, in-band NAC provides better control of traffic and can monitor and restrict traffic after devices are admitted to networks if they violate usage policies, says Jeff Prince, CTO of NAC vendor ConSentry Networks. In-band deployment also supports enforcement of user-specific policy rules about what resources a person can access without creating extensive virtual LANs to address each case, he says.

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]

INFOEXPRESS, INC. - EX2525

"Out -of-band is what I like to call 'edge enforcement," Snyder says. "It scales, it handles the load and it doesn't depend on a single point to do enforcement. [In-line] is really where I think we want to go for big enterprise deployments.

"Of course, that doesn't mean that the in-band guys can't handle the load, but you really want to aim for edge enforcement if it fits, and go for in-band if it doesn't."

What is the best method of enforcing NAC policies?

Nothing's perfect, NAC enforcement included.

There are a variety of methods to choose from, with the choice dependent on how much effort, cost and disruption are acceptable and whether the method is deemed secure enough.

NAC policies can be enforced at the edge of networks by access switches, firewalls and VPN gateways and inside the network also by using firewalls as well as in-line appliances between access and distribution switches. They can also be enforced by manipulating DHCP IP address assignments and by resetting a device's ARP tables to block network access.

A critique of enforcement methods presented at a Black Hat conference by the CTO of Insightix helped put the security of these methods in perspective.

For instance, in the case of DHCP, proxying DHCP servers to enforce security policy cannot address devices that somehow obtain static IP addresses and therefore don't need to deal with the DHCP server. That can makes significant portions of some networks free of NAC enforcement, said Ofir Akin, CTO of Innsightix.

In another example, enforcing NAC policies via switches relying on 802.1X can provide tight policy controls but only for devices that support 802.1x via client software. Devices that don't – such as printers an phones – could be spoofed, circumventing NAC altogether and giving access to an unauthorized machine that can then do damage.

The critique was meant as a heads-up to potential NAC users so they are aware of possible vulnerabilities and can take steps to fill whatever gaps exist, he says. "As long as users understand these solutions are not perfect and take other measures, then I've done my job right," Arkin says.

Users should balance the security of the enforcement method of NAC products with the amount of money and time they will take to implement. For instance, if the best method for a customer is 802.1X authentication, that requires an 802.1X client on every device that will be screened. Users have to ask whether distributing the clients and upgrading the switches that will enforce the policies are worth it.

Burning NAC questions – Part 1

Who needs NAC anyway?

Will NAC help meet regulatory compliance?

Shouldn't I just wait for Microsoft?

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 3 of 6
INFOEXPRESS, INC. - EX2525

by **Tim Greene**
Executive Editor

Tim Greene was executive editor of Network World.

More from this author

Show me more

POPULAR ARTICLES PODCASTS VIDEOS

01

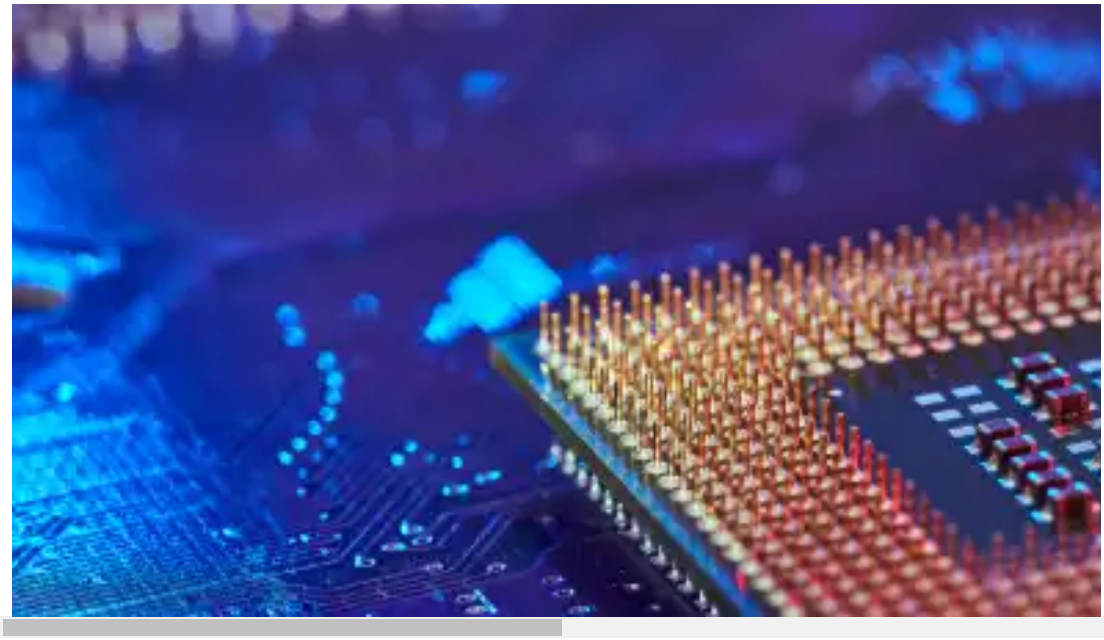
NEWS ANALYSIS

Nvidia Blackwell chips face serious heating issues

By Andy Patrizio

Nov 18, 2024 • 3 mins

CPUs and Processors Data Center



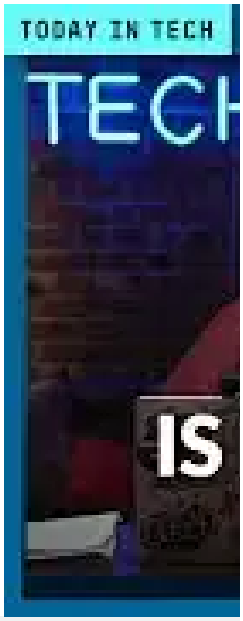
02

PODCAST

Has the hype around 'Internet of T

Apr 18, 2024 • 36 mins

IoT Platforms IoT Security



CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 4 of 6
INFOEXPRESS, INC. - EX2525

About

About Us

Advertise

Contact Us

Foundry Careers

Reprints

Newsletters

BrandPosts

Policies

Terms of Service

Privacy Policy

Cookie Policy

Copyright Notice

Member Preferences

About AdChoices

E-commerce Affiliate Relationships

Your California Privacy Rights

Privacy Settings

Our Network

CIO

Computerworld

CSO Online

InfoWorld

Copyright © 2024 IDG Communications, Inc.