

NETWORK ACCESS CONTROL TECHNOLOGIES

Benny Czarny
 OPSWAT Inc., 640 2nd, 2nd Floor
 San Francisco, CA 94107, USA

Tel +1 415 543 1534 #301
 Email benny@opswat.com

ABSTRACT

Cisco, Microsoft and the Trusted Computing Group are battling to control the keys to locking untrusted endpoints out of networks. Whether you call the approach network access control, network admission control, network access protection, network node validation or trusted network connect, the premise is identical – systems should grant access to the network based on factors such as anti-malware protection level, personal firewall assessment, host and user authentication, location, and even time of day. This paper will:

- Review network access control technologies delivered by Cisco, Microsoft, Trusted Computing

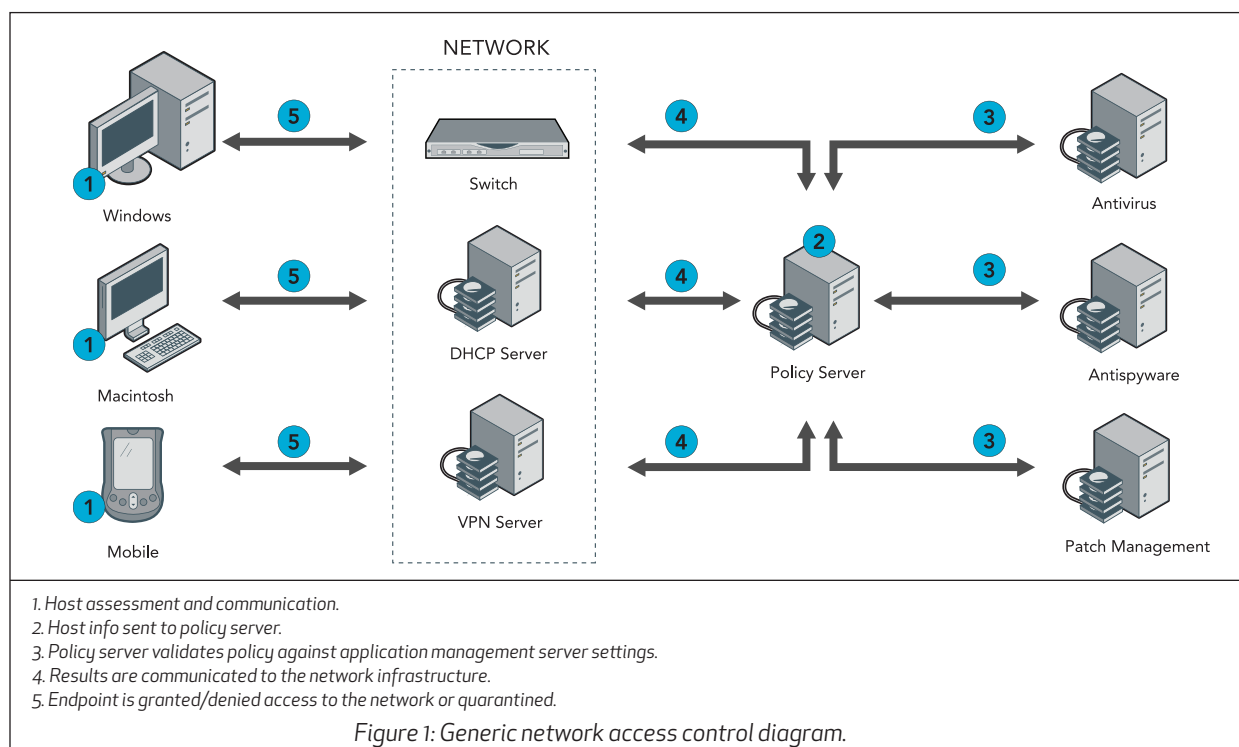
Group and selected non-standard-based solutions such as Nevis Networks and ConSentry Networks.

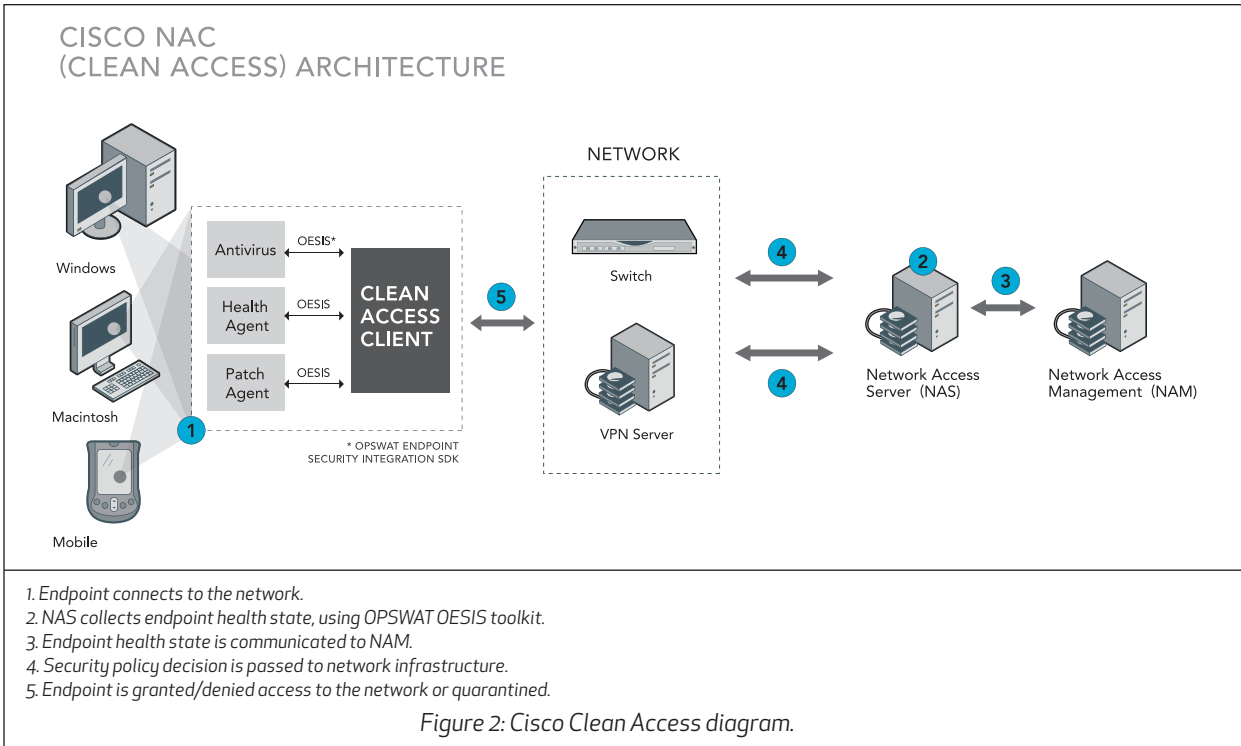
- Outline the partnerships between anti-malware companies and each one of the technologies, it will then outline the partnership process and the resources that would be required for each initiative.

- Compare the processes and list the technical, business and marketing advantages and risks of implementing each network access technology partnership.

INTRODUCTION

Over recent years the increase in the number of mobile workers, the number and types of mobile devices, and in the number of non-employees requiring access to corporate networks has dissolved the network perimeter. Access requests can come from anyone and anywhere, which is why organizations are turning to network access control (NAC) technologies. This paper discusses Cisco NAC, Microsoft NAP, Trusted Computing Group TNC and other programs that offer a solution to the problem. This paper also outlines the benefits of anti-malware companies partnering with these programs.





The approach has many names: network access control, network admission control, network access protection, network node validation or trusted network connect. But whatever it is called, the premise is the same: systems should grant network access based on factors such as anti-malware protection level, personal firewall assessment, host and user authentication, location, and even time of day.

Network access control is not a new concept. *Microsoft* released its Remote Quarantined Service with *Windows 2003 Server*

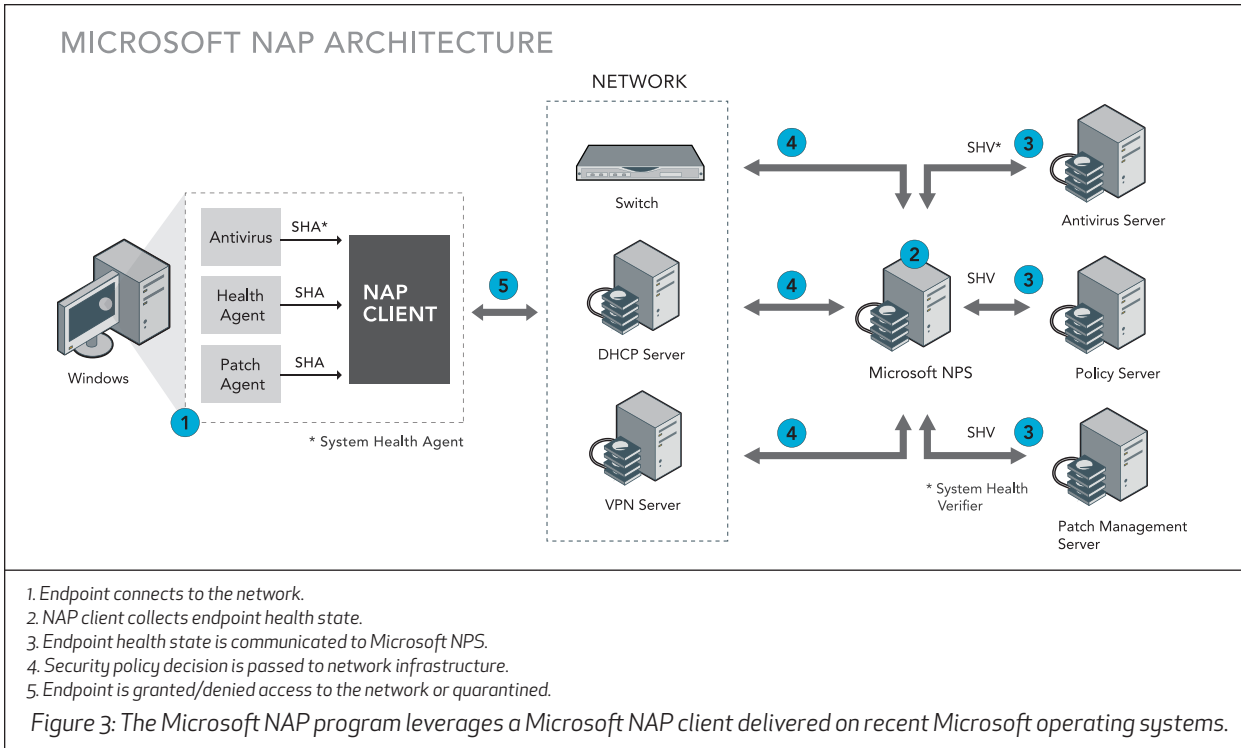
- this solution enabled system administrators to write scripts that would check the health of machines trying to access a network remotely. Now, *Cisco*, *Microsoft*, the Trusted Computing Group and many other vendors are battling to control the keys that lock untrusted endpoints out of networks.

Although endpoint security applications do not always play an active part in this battle, they have a significant influence on this market, given their mission to protect endpoints from malware, vulnerabilities and other security threats.

CISCO NAC

Cisco was the first to define the technology. In 2003 it launched the NAC program. In fact, *Cisco* coined the term NAC (for Network Access Control), which is the term most commonly used today. In its initial approach *Cisco* and its partners provided live client policy information to *Cisco's* NAC client, through written Posture Plug-ins (PP). *Cisco* also defined the term Posture Validation Server (PVS). PVS is a partner policy server that allows administrators to define the health of endpoints – the PVS instructed *Cisco* network devices as to the level of network access allowed based on the health of the endpoint communicated by the PP. This program extended to anti-virus, patch management, vulnerability scanners and other security technologies.

However, *Cisco's* original NAC framework not only failed to solve the problem of unmanaged endpoints, it was also hacked. It had two additional drawbacks. First, it worked only with upgraded *Cisco* LAN equipment. Second, the program depended on the vendors of anti-malware and other security products to alter their binaries in order to work with the *Cisco* Trusted



Agent platform. Furthermore, some of the prospective partners (e.g. Symantec and McAfee) had – and still have – competing NAC solutions.

The acquisition of Perfigo in 2004 enabled Cisco to overcome these drawbacks. Perfigo's solution was able to work with nearly all of Cisco's switches, by creating dynamic virtual networks. And once Perfigo agreed an OEM licence for OPSWAT's OESIS (OPSWAT Endpoint Security Integration SDK) Framework, Cisco no longer had to rely on security vendors modifying their products.

MICROSOFT NAP

Microsoft launched a program that was similar to Cisco's NAC, named NAP – Network Access Protection. It supports a few more authentication protocols and has a similar client/serverbased integration. Cisco's PP was replaced by a System Health Agent (SHA) and PVS was replaced with a Network Policy Server (NPS).

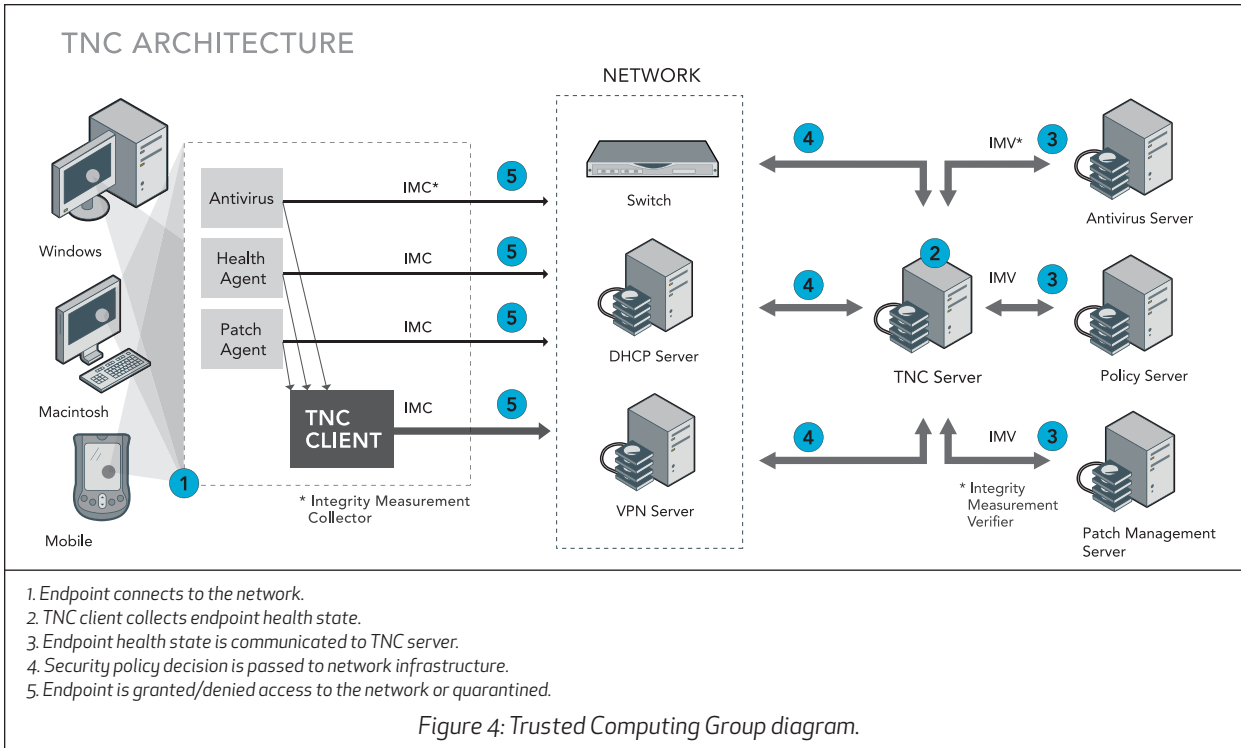
Though similar in concept, one major difference sepa-

rates the first NAC and NAP programs. While Cisco's program supports any operating system that works with Cisco's equipment, Microsoft's solution works with any Microsoft operating system and with any networking equipment, as long as Windows 2008 Server is part of the network health decision-making process.

TRUSTED COMPUTING GROUP TNC

The Trusted Computing Group (TCG) is a non-profit organization whose purpose is to define and promote open standards for hardware-enabled trusted computing. TCG formed a work group (the Trusted Network Connect (TNC) Work Group) that has released an open architecture and a set of standards for determining endpoint integrity before and during network activities.

Similar to NAC and NAP, TNC defined a protocol for gathering a client computer's security state in the form of integrity measurements. Called Integrity Measurement Collector (IMC), this protocol is the equivalent of Microsoft's SHA or Cisco's PP. TCG defined an Integrity Measurement Verifier (IMV) as



the interface between the network enforcement point and the network policy server (TNC server). It is similar in concept to Microsoft's System Health Validator (SHV) and Cisco's PVS. However, unlike SHV and PVS, the TCG program was designed to support any operating system and any networking equipment.

NAC PRODUCTS

There are many network access control products produced by dozens of companies, including: Most companies deliver an appliance or software

- Cisco Systems
- Sophos
- Microsoft
- AEP Networks
- Nortel Networks
- Mirage Networks
- Bradford Networks
- Insightix
- McAfee
- Forescout Technologies
- Avenda Systems
- SonicWALL
- ConSentry Networks
- Aruba Networks
- Bluesocket
- Blue Ridge Networks
- Check Point Technologies
- InfoExpress
- StillSecure
- Trend Micro

- F5 Networks
- Array Networks
- Symantec
- Nevis Networks
- 3COM Corporation
- Tipping Point Technologies
- And others

solution that integrates with existing network infrastructures and enforces some sort of network access control. Nevis Networks and ConSentry Networks, the two NAC/switch vendors, took an all-in-one approach and delivered a network access device (switch) with NAC capabilities. The rest of the NAC vendors enforce network access by using technologies that include:

- Virtual networks
- SNMP
- ARP poisoning
- 802.X
- DHCP
- Other technologies and techniques
- The frameworks: NAC, NAP and TNC

The goal of almost any NAC vendor is to collect information about the health of an endpoint and/or to trigger a healing action on an 'unhealthy' endpoint. Health checks include checking for the state of endpoint security applications by verifying the definition time of the anti-virus application, the engine version, the last time the anti-virus application triggered a scan, when the last definition file update occurred and other checks.

Healing actions include triggering a definition file update, updating the engine and triggering a full system scan.

Non-compliant endpoints are usually notified, denied access to the networks or put in a separate LAN that has fewer network permissions.

There are several methods by which NAC vendors monitor endpoint health:

1. Running a one-time or a persistent client on the endpoint.
2. Calling RPC (Remote Procedure Calls). This can be done from *Windows*, which some NAC vendors permit products and users to leverage.
3. Monitoring network traffic, which enables vendors to monitor endpoint activities, such as anti-malware application updates on given ports and protocols, virus outbreaks, bots and peer-to-peer applications.

WHY ANTI-MALWARE COMPANIES SHOULD PARTNER WITH NAC VENDORS

For any anti-malware company, partnering with NAC vendors makes business sense. Partnering enables joint packaging and joint solutions. Partners can co-market and co-brand, which enables companies to be detected and inter operate with many NAC vendors, get listed on their websites and on their management consoles. Partners can provide mutual defence and anti-malware companies partnering with NAC providers can avoid uninstallation of their products. If a NAC

product does not detect a supported endpoint security application on the endpoint machine (whether that is because there is none or because the application installed on the machine is unsupported), the product will typically instruct the network access device to quarantine the endpoint and install a security application that it supports. Since many anti-malware applications cannot inter-operate, the supported security application will typically trigger a uninstall of the unsupported application. For security vendors, uninstallation of their application means:

- Virtual networks
- SNMP

HOW TO PARTNER WITH NAC VENDORS

- For NAP, NAC, TNC and other NAC solutions, anti-malware vendors should join OESISOK. OESISOK is a certification program that verifies the integration to the *OPSWAT OESIS Framework*, which powers most NAC devices. The program permits the submission of betas, release candidates and generally available releases for certification testing.
 - To partner with *Microsoft*, anti-malware vendors should join the NAP program. Integrate your system health agent with the *Microsoft* NAP client. Develop SHV and integrate your policy and system health verifier. Maintain the solution for every application you deliver.
 - To partner with TNC, anti-malware vendors should implement IMC and follow the TNC guidelines. Develop and test an IMV and IMC solution. Market the solution with every relevant TCG vendor and maintain the solution for every application you deliver.

REFERENCES

- [1] Cisco News Room. <http://newsroom.Cisco.com/dlls/index.html>.
- [2] Cisco CTA. http://www.Cisco.com/en/US/solutions/ns340/ns394/ns171/ns466/ns617/net_de/sign_guidance0900aecd80417226.pdf.
- [3] Hacking Cisco CTA. <http://www.ernw.de/con->

- tent/
e7/e181/e566/download568/ERNW_nacattack_10_dr_20070307_ger.pdf.
- [4] <http://mediaproducts.gartner.com/reprints/juniper/vol3/article4/article4.html>.
- [5] <http://www.opswat.com/>.
- [6] OESISOK Antimalware Interoperability Certification Program. <http://www.oesisok.com/>.
- [7] Cisco-Microsoft Interoperability white paper. Cisco Network Admission Control and Microsoft Network Access Protection Interoperability Architecture. http://www.Cisco.com/application/pdf/en/us/guest/netsol/ns617c654cdccont_0900aec8051fc24.pdf.
- [8] Cisco CNACF deployment guide: Network Admission Control Framework Deployment Guide. http://www.Cisco.com/application/pdf/en/us/guest/netsol/ns617c649cdccont_0900aec80417226.pdf.
- [9] Cisco CNACF configuration Best Practices: NAC Framework Configuration Guide. http://www.Cisco.com/application/pdf/en/us/guest/netsol/ns617c649cdccont_0900aec8040bbd8.pdf.
- [10] Cisco CNACF partners info. <http://www.Cisco.com/web/partners/pr46/nac/partners.html>.
- [11] Cisco NAC portal. <http://www.Cisco.com/go/nac>.
- [12] Cisco CNACF switch support list. http://www.Cisco.com/en/US/netsol/ns628/networking_solutions_package.html.
- [13] Cisco NAC 2.0 (Framework) Release Notes. http://www.Cisco.com/en/US/netsol/ns617/networking_solutions_release_note_09186a0080652b06.html.
- [14] Cisco CNACA Release Notes page (includes current list of CNACA partners). http://www.Cisco.com/en/US/products/ps6128/prod_release_notes_list.html.
- [15] Cisco CCA (CNACA) page. <http://www.Cisco.com/go/cca>.
- [16] Cisco CNACA data sheet. http://www.Cisco.com/en/US/products/ps6128/products_data_sheet0900aec802da1b5.html.
- [17] Cisco Switch Support for Cisco NAC Appliance. http://www.Cisco.com/en/US/products/ps6128/products_device_support_table-09186a008075ff6.html#wp60598.
- [18] Microsoft TechNet on Network Access Protection. <http://www.Microsoft.com/technet/network/nap/default.aspx>.
- [19] Network Computing article, Cisco NAC vs. Microsoft NAP. <http://www.networkcomputing.com/showArticle.jhtml?articleID=60401143>.