Global Information Assurance Certification Paper

Enforcing Policy at the Perimeter

Derek A. Buelna

June 9, 2004

GSEC Practical Assignment 1.4b
Option 1: Research on Topics in Information Security

Table of Contents

Abstract

The rapid deployment of security patches and anti-virus updates has become a basic need within most IT organizations. The time between the disclosure of a vulnerability and its exploitation continues to decrease while vulnerabilities are becoming easier to exploit and are increasingly severe. Locally enforcing security policy on a large number of computers can be a challenge but keeping remote (VPN or dial-up connected) computers up to date can prove even more difficult.

This case study examines some options available to organizations for providing remote access to users without over-extending the perimeter. Five alternatives for enforcing policy on remote users *at the perimeter* are analyzed in order to determine if and how the following questions are addressed. Does the remote computer have up to date virus protection? Have the latest security patches been applied? Is a certain piece of software installed or not installed? Is the software firewall configured with the current rule set? The alternatives examined in this case study address most of these questions but they each have their pros and cons. Each product has a different focus and approach for addressing these questions.

Introduction

With the growing number of virus and worm outbreaks over the past few years, IT organizations are placing a high priority on the remediation of vulnerabilities and the timely distribution of anti-virus definition files. However, even organizations that have mastered this process are still getting hit, as anti-virus definition files are not always available before malicious code presents itself.

There are a number of methods, primarily reactive, that administrators can use to detect out of compliance computers on the network. In many cases these methods allow infected or unpatched machines onto the network for some period of time before detection and removal. With the speed at which viruses and worms can propagate, it can be problematic for organizations to allow computers on their networks for any period of time unless they're in compliance with corporate policy.

Traditional remote access solutions provide user authentication and were not designed to validate the state of remote computers connecting to the corporate network. Future remote access solutions will need to incorporate, or at least interoperate with, validation technology in order to enable policy enforcement at the perimeter.

Each of the following five sections examines an alternative to policy enforcement, providing the reader with an overview of validation technology. At the end of the case study, some conclusions are made about the functionality of the different technologies and some important issues are addressed.

Internet Security Systems

At a glance, policy enforcement is enabled using the capability of a VPN concentrator to determine if a software firewall is present on a remote computer attempting to make a VPN connection. This feature in conjunction with a software firewall is used to enforce policy. If a software firewall is present on the remote computer, the VPN concentrator will allow VPN connection establishment (assuming user authentication succeeds). If it isn't, the VPN concentrator denies access. The software firewall is in turn relied upon to enforce policy on the remote computer.

This alternative requires the use of a VPN concentrator such as the Cisco (Altiga acquisition) that can require the Internet Security Systems (ISS) BlackICE software firewall to be installed and running. We'll be referring to BlackICE as the Desktop Protector, which is the name of a newer version of BlackICE. Desktop Protector, in addition to providing a software firewall, provides host-based IDS functions and application protection capabilities[1].

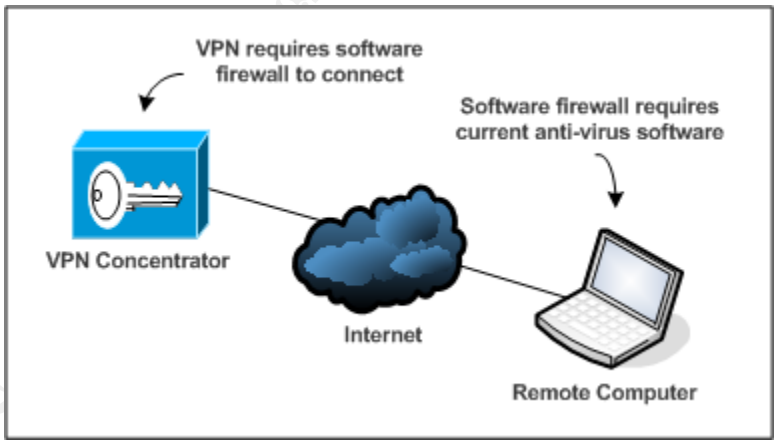

Figure 1

Does the system have current anti-virus protection?
The VPN concentrator allows remote computers with Desktop Protector installed to connect. Desktop Protector can determine whether or not anti-virus protection is up to date on the computer where it resides, and can isolate the computer (itself) if it is out of date, using the software firewall features.

Does the system have the latest security patches applied?
Desktop Protector does not have the capability to validate security patches, OS revision levels and application versions except for the features that are provided with application protection.

Is certain software installed or not installed on the system?
The Application Protection component of Desktop Protector can be configured to allow certain applications to execute and deny all others or alternatively it can be configured to deny certain applications and allow all others. This permit/deny functionality uses a checksum database. The Application Protection features can also control which applications are allowed to access the network. Application Protection can be turned on or off. Some organizations have opted to leave it off, due to the administrative nightmare it can create[2]. The option to only allow certain applications to execute can be particularly cumbersome in a large environment. However, this method can be effective in an environment where only certain applications are allowed and users are not allowed to install software on their own machines. Financial institutions and some government agencies come to mind. Application Protection will be going away in a future version of the Desktop Protector and it will be incorporating additional behavior based features.

Is the software firewall configured with the current rule set?
A check to determine if a system has a current software firewall policy is not executed as part of the authentication of a remote user. However, the Desktop Protector policy is centrally managed and distributed. A computer running Desktop Protector regularly checks with a central server to determine if there's a policy update. The frequency of these checks is configurable within the policy, while the default is once an hour.

ISS has a product called Desktop Enforcement for VPNs that provides a function similar to that provided by the Cisco VPN concentrator, the checking for a software firewall. The enforcement tool should be installed on a computer that is positioned between a VPN concentrator and the internal network, like a firewall. Its function is to validate that Desktop Protector is installed on a remote computer and that the latest policy has been applied. If the policy is out-of-date on the remote computer, it will be quarantined until it is up to date.

Cisco Systems

This section examines the policy enforcement features of the Cisco Security Agent (CSA) and those of the Cisco Network Admission Control (NAC) framework. CSA was originally developed by Okena, a Cisco acquisition, and is similar to the ISS Desktop Protector product. CSA is a host-based IDS, firewall

and application protection suite that intercepts all operating system, file system, configuration, registry, and network requests[3], being designed to prevent malicious activity from occurring. Cisco NAC requires three components, the Cisco Trust Agent (CTA), which is a software agent that runs on a client computer, a Network Access Device, which can be a router, switch, security appliance or a wireless access point, Cisco Secure Access Control Server (ACS), a policy server. Although the VPN/Security Management Solution is listed as a fourth component[4], this software is currently used to manage NIDS, Firewall and CSA policies and is not a requirement of NAC.

Does the system have current anti-virus protection?

Although still under development, NAC addresses this question. The function of the CTA is to validate whether the local anti-virus software is up to date on a computer requesting access and communicate this information to a Network Access Device. The Network Access Device communicates with ACS in order to determine whether or not the remote computer running CTA is compliant. If it is, the Network Access Device will permit the computer onto the network. If it isn't, the Network Access Device can deny access or quarantine the remote computer, depending on how it's configured.

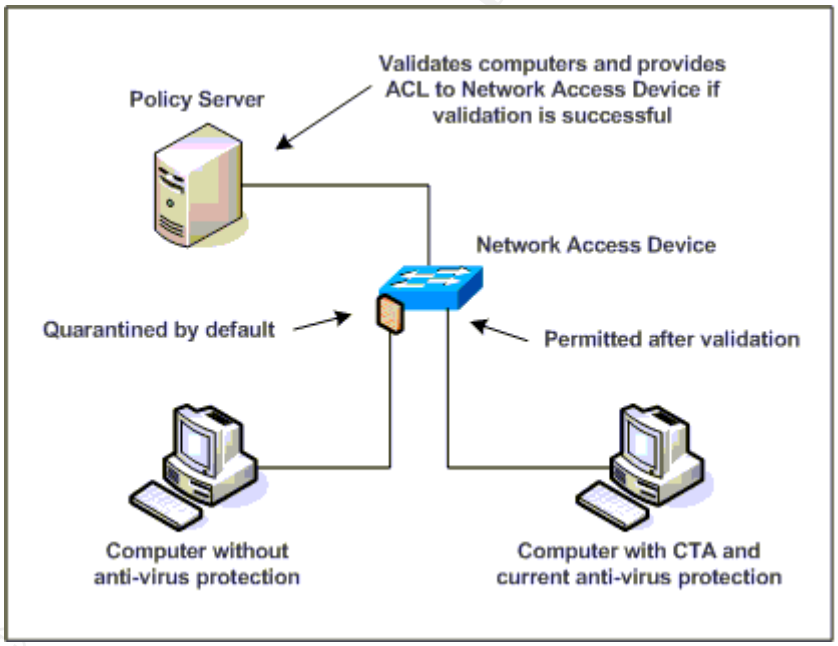

Figure 2

CTA currently works with three anti-virus vendors. These are Network Associates, Symantec and Trend Micro[5]. CTA will be available as part of the anti-virus software from these vendors in a future update. CTA will also be available as a free download from Cisco's web site. In fact, CSA software will even include CTA as part of a future update. Although it was noted that Network Access Devices could be routers, switches, security appliances, only certain routers are being initially supported while the rest of the devices should be supported later

this year. All of these devices will need a software upgrade in order to support the communication with computers running CTA and the policy server, ACS.

As an example of how this can work, consider a router sitting between a client computer and a set of servers. The router is configured with ACLs that block the majority of traffic from the client computer by default, except for DHCP, DNS, CTA traffic and so on. As part of the initial validation, CTA traffic, received by the router, is forwarded to ACS. Based on a permit response from ACS, a dynamic ACL is applied to the router for the client computer, allowing it full or partial access to the network. Based on a quarantine response from ACS, a dynamic ACL is applied to the router for the client computer, which will only provide the client computer with enough access to obtain anti-virus updates. Once the client computer is up to date, a permit response from ACS will cause the ACL to be updated, removing the quarantine.

Does the system have the latest security patches applied?
CTA does not have the ability to check for security patches at this time.

Using CSA in conjunction with the CSA profiler, administrators can identify remote systems missing critical system security updates, like service packs or hot fixes. This is not something done as part of an authentication or validation mechanism however. Note that CSA has buffer overflow protection, which serves to mitigate some of the risks associated with zero day attacks.

Is certain software installed or not installed on the system?
CTA can only check for anti-virus software at this time.

Similar to the ISS Desktop Protector, CSA can permit and deny applications from executing and from accessing the network. This feature is not part of remote user authentication or validation, it's part of a policy configuration. In order to enforce a software policy on remote users, the Cisco or other VPN concentrator can be configured to check for CSA, which handles this enforcement.

CSA Profiler can identify software installed or not installed on a remote system.

Is the software firewall configured with the current rule set?
CTA does not address this at this time.

As with the software enforcement features, checking for a firewall policy version is not part of remote user authentication or validation, it's part of a policy configuration. CSA checks with its management server to determine if a new update is available. If it is, it is automatically downloaded and installed.

Checkpoint

This section examines how the Zone Labs Integrity agent, a recent Checkpoint acquisition and the Checkpoint VPN solution (Firewall and VPN client) are able to enforce policy on remote computers. Most of today's VPN solutions, including Checkpoints, can be configured to check for a software firewall. In this example, the Checkpoint VPN concentrator requires Integrity to be installed on remote computer. When the remote computer attempts to connect using VPN, if Integrity is installed, it is granted access. If Integrity isn't installed, it is not allowed to connect. In turn, Integrity validates and enforces policy on the remote computer.

Does the system have current anti-virus protection?
The Integrity agent can check for anti-virus software[6]. This feature is not part of remote user authentication and validation. It is part of a policy configuration. In order to enforce a software policy on remote users, the Checkpoint VPN concentrator can be configured to check for Integrity, which handles the enforcement. If the remote computer is in compliance with the policy, it's granted access to the network. If it isn't, the remote computer can be provided access to a server where the appropriate software can be downloaded and installed (quarantined). Once the remote computer is up to date, it will again be granted access to the network.

Does the system have the latest security patches applied?
The Integrity agent is able to validate whether or not security patches or certain hot fixes have been applied. This feature is part of the policy configuration.

Integrity consists of an Integrity policy server and Integrity agents. The policy server is the central location where policies are created, stored and distributed. Administrators configure firewall rules and application protection settings to include rules regarding what software must be running or not running within a policy. The Integrity agent is essentially the ZoneAlarm product with some enhancements enabling centralized policy management and client validation and enforcement.

Is certain software installed or not installed on the system?
The Integrity agent can allow or deny applications from using the network and can run checks to determine what software in installed[7]. This feature is part of the policy configuration.

Centrally managing the application list with Integrity or another product that provides application protection features can prove challenging. A computer running Windows may have a large number of programs trying to use the network. These programs frequently change with software updates while crackers will try to disguise Trojans with names similar to valid executables.

Is the software firewall configured with the current rule set?
The Integrity agent checks with the management server to determine if there is a new policy to download and install, which addresses this question. This is separate from remote user authentication and validation.

The agent version of the Integrity client can be configured so even users that are part of the local administrators group on a remote computer are unable to easily disable it. Integrity enforces policies on the client by creating dynamic ZoneAlarm firewall rules. Using Cooperative Enforcement Technology, Integrity is able to interoperate with routers, switches, wireless access points and other devices.

Juniper

This section takes a look at the policy enforcement features provided by an SSL-based VPN. More specifically, we'll look at the product originally developed by Neoteris. NetScreen acquired Neoteris in October 2003, while Juniper acquired NetScreen in April 2004.

First, let's review how an SSL VPN differs from a normal VPN. A normal remote access VPN consists of an encrypted tunnel between a remote computer and a VPN concentrator. IP traffic can be configured to flow unrestricted through the tunnel including TCP, UDP and ICMP traffic. Thus, any application on the remote computer that is connected via a remote access VPN can access the network as if it were locally connected. In the case of an SSL VPN, an encrypted tunnel is created between a web browser and a VPN concentrator. In this case, VPN software is not required on the client, which is nice. Instead of running VPN software on a remote computer and connecting to a VPN concentrator, the user runs a web browser and connects to a specific URL.

The Juniper SSL VPN provides seamless access to web-enabled applications but it can also provide additional access using an ActiveX or Java plug-in for the web browser[8]. Port forwarding over SSL is supported while PPP encapsulation over SSL is available for applications with server-initiated connections like active FTP.

Does the system have current anti-virus protection?
The Host Checker feature can check for anti-virus software but it can also check for Sygate, ZoneAlarm and other end-point security products[9]. The Host Checker runs as part of user authentication so a remote computer is validated every time it connects. Many end-point security products can also check for anti-virus software so there are multiple ways this can be addressed.

Does the system have the latest security patches applied?
As part of release 4.1, the Host Checker feature is able to check for minimum versions of files. For example, this could allow an administrator to require a certain dll to be version 4 or higher.

Is certain software installed or not installed on the system?
The Host Checker feature can be configured to check for software or files on a remote computer. It can check for running processes and registry entries, basing the user authentication/validation decision on the results of these checks.

Is the software firewall configured with the current rule set?
The Host Checker feature is able to check for minimum versions of files as part of release 4.1. This feature could potentially be used to check for a current rule set. However, the Host Checker can be configured to check for a certain software firewall, validating that it is installed and running. This may be adequate as many of the software firewalls will automatically check for policy updates on a regular basis.

Microsoft

The Microsoft Quarantine features are focused on enforcing policy on remote computers at the perimeter and do not include firewall or IDS functionality. The Microsoft Quarantine features are designed to protect the corporate network from remote computers that are out of compliance with corporate policy. This technology allows organizations to enhance authentication of remote users with the ability to validate the state of the remote computer trying to connect using VPN.

The Quarantine components include quarantine-capable remote computers and a quarantine-capable VPN concentrator. The quarantine-capable VPN concentrator must be a computer running a member of the Windows Server 2003 family and Routing and Remote Access, which supports the use of a listener component and the MS-Quarantine-IPFilter and MS-Quarantine-Session-Timeout RADIUS vendor-specific attributes (VSAs) to enforce quarantine settings[10].

Quarantine-capable remote computers run operating systems that support connection entries created with the Connection Manager Administration Kit (CMAK), which is part of Windows 2000 and 2003 Server. These include Windows 98, ME, 2000, XP and 2003. CMAK allows for the definition of special actions as part of the VPN connection establishment.

By default, an ACL placed on the VPN concentrator restricts all remote computers to certain resources, Quarantine resources, until the remote computers are validated with a custom script. The Quarantine resources may

include DHCP, DNS and servers with software available for download so remote computers can become compliant. Once a remote computer is validated, the ACL is lifted and the remote computer is provided with normal access.

Does the system have current anti-virus protection?
Quarantine can check for current anti-virus protection as part of the user authentication process. The check requires the use of an administrator provided script[11], which is executed as part of the connection process, after a user successfully authenticates.

Does the system have the latest security patches applied?
Quarantine can check for security patches, application versions and other items, as the script that runs checks is customizable.

Is certain software installed or not installed on the system?
Quarantine can validate whether or not specific software is installed. Administrators should be able to check for virtually anything, as the script is customizable and can be a batch file or an executable.

Is the software firewall configured with the current rule set?
Quarantine may be able to check for this information, assuming it is made available to other applications on the system. The custom script performing this check can do virtually anything the administrator/programmer wants, including checking registry keys.

Conclusion

Organizations are beginning to understand the limitations of virus signatures and realizing the need to enforce policy on local and remote computers alike. They're looking for new ways to defend against zero-day attacks. Many products are being developed that allow IT organizations to enforce policy on local and remote computers.

The ISS Desktop Protector is not focused on enforcing policy at the perimeter but it can enforce policy on a remote computer when used in conjunction with a VPN concentrator that requires Desktop Protector to be installed. Desktop Protector can require up to date anti-virus software to be installed and it can allow or disallow certain applications. The ISS products also have features that are attractive to large enterprises. Desktop Protector events (IDS, firewall and others) roll up into a central database. Policy, including firewall rules is pushed down to computers with Desktop Protector. For example, a rule blocking outbound traffic on TCP port 25 can be quickly rolled out to many computers. Additionally, Xforce and ISS generally provide signatures/updates much faster than most software vendors. For example, ISS will usually have a signature for a vulnerability before

the vendor releases a patch. This is great because it allows Desktop Protector and some of their other products to block attacks using the HIDS to trigger an auto-block on the software firewall.

CTA is focused on enforcing policy where a computer connects to the network, locally or remotely. CSA, like the Desktop Protector, can enforce policy on a remote computer when used in conjunction with a VPN concentrator that requires it to be installed. Although NAC (and CTA) is still in development, it's appealing due to the integration with network and security devices. It's advantageous to have a single solution for enforcing policy on local and remote computers. Using CTA with CSA is also attractive as enforcement at the perimeter is coupled with a great deal of endpoint security, like buffer overflow protection. Note that although the CSA profiler can scan computers for security patches, this cannot be enforced at this time.

The acquisition of Zone Labs enabled Checkpoint to provide an end-to-end policy enforcement solution. As with Desktop Protector and CSA, the Integrity agent is replied upon to enforce policy on the remote computer. The Checkpoint VPN concentrator simply needs to require the Integrity agent to be running. Keep in mind that it's really Integrity doing the enforcement. Here we're using the Checkpoint VPN concentrator to require the Integrity agent but another VPN concentrator that supports requiring the Integrity agent could be used instead. Although the Integrity agent does provide considerable policy enforcement functionality, I've come to think of ZoneAlarm as more of a personal firewall. Managing one computer with ZoneAlarm isn't a problem but managing a hundred or more of them may be an administrative challenge. However, in teaming with Checkpoint, the Integrity product may very well be an alternative for large companies in the future.

The SSL VPN product available from Juniper has virtually limit-less policy enforcement capabilities as administrators can write their own dll in order to meet their needs. This enforcement is accomplished at the perimeter, every time a user makes a VPN connection. This may not be a viable option for companies already equipped with a satisfactory VPN solution. Those looking to reevaluate, however, may find this technology worth looking into. I also like how users can be assigned roles based on their Active Directory group membership. ACLs can be assigned to roles such that contractor x can only access server y on port z. Most VPN concentrators support ACLs but the Juniper product is very flexible. Roles also determine whether a user has full network layer connectivity or some portion thereof. As an example, one user may be authorized to use the Network Connect feature, which allows full TCP/IP connectivity using PPP over SSL, while another may only be allowed to access certain web applications. Additionally, the Juniper product supports remote computers running multiple operating systems, making use of Java. The other alternatives have a Windows focus.

As with the Juniper product, the Microsoft Quarantine technology is virtually limitless in addressing policy enforcement. It happens at the perimeter, every time a user makes a VPN connection, which is optimal. The validating of a remote computer is accomplished through an administrator provided script or executable, so there's plenty of flexibility in what you can check for. However, even though the enforcement capabilities are excellent, I would be uncomfortable running Windows 2003 Server as my VPN concentrator. I'm certain the 2003 family is more secure than previous versions of Windows, but I'd prefer to keep my Windows boxes inside the firewall and behind a reverse proxy. Additionally, I would rather use a VPN concentrator that supports IPSEC versus using L2TP/IPSEC[12]. The requirement that remote workstations must be quarantine-capable may also be an issue for some organizations as this means only certain versions of Windows can connect.

The following table depicts whether or not the alternatives examined in this paper can check for and enforce computers to have current anti-virus software, current security patches, certain software installed or not installed and a current firewall rule set.

Enforcement Capability Comparison

Vendor	Anti-Virus	Security Patches	Software	Firewall Rules
ISS	Yes	No	Yes	Yes
Cisco	Yes	No	Yes	Yes
Checkpoint	Yes	Yes	Yes	Yes
Juniper	Yes	Yes	Yes	Yes
Microsoft	Yes	Yes	Yes	Yes

A wide variety of products are available that can help organizations enforce policy at the perimeter. This case study examines some options but others including Sygate and Perfingo may be worth looking into. Also, the Trusted Computing Group is working on a specification entitled Trusted Network Connection[14], which quite a few vendors are participating in. You can expect a lot of activity in this space as the technology is fairly new and the vendor interoperability is still being developed.

References

1 – Internet Security Systems. “Complete Desktop Protection for the Enterprise.” iss.net. 2002. URL: http://documents.iss.net/whitepapers/CompDesktopProt.pdf

2 – Andrew Plato. “Customizing BlackICE Application Controls.” anitian.com 2003. URL: http://www.anitian.com/corp/papers/BI%20AC%20tweaking.pdf

3 – Cisco Systems. “Cisco Security Agent with Intrusion Protection for Remote Corporate Users.” cisco.com. 2003. URL: http://www.cisco.com/application/pdf/en/us/guest/products/ps5057/c1244/cdccont_0900aecd800ae54b.pdf

4 – Cisco Systems. “Cisco NAC, The Development of the Self-Defending Network.” cisco.com. 2004. URL: http://www.cisco.com/warp/public/cc/so/neso/sqso/csdni_wp.pdf

5 – Jennifer Hagendorf Follett. **“**Cisco Teams With Security Vendors To Thwart Worms, Viruses.” crn.com 2003. URL: http://www.securitypipeline.com/showArticle.jhtml?articleID=16101312

6 – Zone Labs. “Integrity for Checkpoint Datasheet.” zonelabs.com. 2004. URL: http://download.zonelabs.com/bin/media/pdf/Integrity_Checkpoint.pdf

7 – Cameron Sturdevant. “Integrity Lays Down the Law in Security.” eweek.com. 2003. URL: http://www.eweek.com/article2/0,3959,1229937,00.asp

8 – John Desmond. “Neoteris Extends Gateway Access.” esecurityplanet.com. 2003. URL: http://www.esecurityplanet.com/prodser/article.php/2245401

9 – Loring Wirbel. “Neoteris inks deals to broaden SSL service.” eetimes.com 2003. URL: http://www.eetimes.com/article/printableArticle.jhtml?articleID=16501836&url_prefix=story&sub_taxonomyID=2251

10 – Microsoft Corporation. “Microsoft Windows Server 2003 Network Access Quarantine Control.” microsoft.com. 2003. URL: http://www.microsoft.com/windowsserver2003/techinfo/overview/quarantine.mspx

11 – Microsoft Corporation. “Step-by-Step Guide for Setting Up Network Quarantine and Remote Access Certificate Provisioning in a Test Lab.” microsoft.com. 2003. URL: http://www.microsoft.com/downloads/details.aspx?FamilyID=fe902704-52dd-4bbe-8a75-f8fbb76cd28a&DisplayLang=en

12 – Microsoft Corporation. “Virtual Private Networking with Windows Server 2003: Overview.” microsoft.com. 2003. URL: http://www.microsoft.com/windowsserver2003/techinfo/overview/vpnover.mspx

13 – Ellen Messmer. “The Enforcers.” nwfusion.com. 2004. URL: http://www.nwfusion.com/weblogs/security/005122.html#005122

14 – Trusted Computing Group. “Trusted Computing Group Developing New, Open Trusted Network Connect Specification to Ensure Endpoint Integrity.” trustedcomputinggroup.com. 2004. URL: https://www.trustedcomputinggroup.org/press/TCG_Releases/2004/TNC_final_release_may_11_2004.pdf