

Using a Network Admission Control System to Secure Your Network

Michael Lavengood
Assistant Director of IT Services – Network Services
Franklin College
101 Branigin Blvd.
Franklin, Indiana 46131
317-738-8148
mlavengood@franklincollege.edu

Introduction

As users become more mobile on more powerful machines that attach to faster networks it makes it harder to keep an organizations' network and data secure and operational. This trend has been occurring since wireless networks and wireless devices have become more affordable. We can assume that this trend will continue in the years to come, probably at even a faster rate than in the past. By utilizing a network admission control (NAC) system, we can require that the devices that connect to the network are secure to a level that is acceptable by that organization.

Cisco.com defines a network admission control system as a system that “allows noncompliant devices to be denied access, placed in a quarantined area, or given restricted access to computing resources, thus keeping insecure nodes from infecting the network.” If a device is deemed compliant then the computer is allowed onto the network just like when they are not checked by a NAC. This type of system pushes security to the connecting device, not on the network.

To fully gain all the capabilities of a NAC you will need to install a piece of software, known as an agent, to the connecting device. This allows the network and system administrators to check for very specific items on the desktop, be it a registry key, or a piece of software is running, etc. You can use a NAC without installing the agent; this still gives you the option to put a user into a role that has ACL's attached to that role. With Cisco's Clean Access system, you can use Nessus, a vulnerability checking software, to check for unsecured systems. This could lead to many false positives or may not be an option at all since most devices now have a firewall installed, which disables these types of checks.

We are going to specifically look at Cisco's Clean Access. Cisco bought out Perfigo to acquire this technology. Franklin College purchased the software from Perfigo and we have not seen a significant change in the product since Cisco has taken over the development. We will also discuss a web site that has been developed by Franklin College to work in conjunction with Clean Access to provide users documentation on how to fix their computer when it is in quarantine.

Cisco Clean Access Components

The Cisco Clean Access consists of three different components. The Clean Access Server (CAS), the Clean Access Manager (CAM), the Clean Access Agent (CAA). The agent is an optional piece but is strongly recommended to get the full functionality. With just the Clean Access Server and the Clean Access Manager, you will be able to use ACL's based on roles, but

you will not be able to check a device for installed applications or running applications to name a few.

The Clean Access Manager is the front-end for the system's administrators. This is where they set up the Clean Access Servers, configure user roles, set up the default web page for users to log on to, and view which users are logged onto the system. The web interface is not very intuitive at first, and it does take some time to figure out where everything is since there are so many different items that can be configured.

The Manager gives you the ability to see all users that are currently logged on to the NAC based on role. For each user you can view the IP address, MAC, and OS of the device that they have connected to the system, as well as when they logged on. If you have implemented new checks you can kick all users or specific users off the network very easily. If you are using the agent then you can also see what requirement a device does not meet. If you start to get a lot of calls with people needing help on how to get past this requirement, you should look at your help documentation to see if you can make it more descriptive.

The Clean Access Server is where all the enforcement is done. Depending on how your network is set up you may need more than one CAS. Here at Franklin College since we have two core routers, we had to purchase two CAS's. These servers are installed between the router and users. All traffic from networks managed by Clean Access is routed through the CAS. These devices can be the DHCP server for all devices managed by Clean Access.

To enforce Clean Access on specific virtual local area network (VLAN) you enter the VLAN(s) into the specific Clean Access Server that you want to manage that traffic. Everything that is a part of that VLAN is then considered untrusted. The Microsoft Encyclopedia of Networking defines a virtual LAN as, "A network technology that allows networks to be segmented logically without having to be physically rewired." You then must change your gateway address on your routers to point to the trusted network interface on the CAS. This forces all traffic from that VLAN to be routed through and managed by the Clean Access system.

The Clean Access Agent is a small piece of software that is installed on most devices that will connect to the network. This software works on Windows 98, ME, 2000, and XP. This piece of software is where the end-users log on to get onto the network. It then communicates with the CAS to determine what role and requirements this user must meet. It then begins to check to determine if the users' computer meets the requirements by checking if applications are running, if a file exists, or if a registry key exists, etc. If the computer does not meet a requirement, then the computer is put into quarantine. Once in quarantine the user is given either a link or a file to allow them to meet the requirements. They are not able to go past this point until the requirement is resolved. Once all the requirements are met, the user is allowed onto the network. If there are any ACL's for the role that the user is assigned to, the user will be limited by them, but that is the only thing based on the Clean Access system.

Why Franklin College Implemented Clean Access

Franklin College has been requiring that students install a managed version of Symantec Anti-virus. Initially, this was done by sending all students an email with the link to install it included and trust that they installed the software. We soon discovered that this method was not effective; our network was being slowed to a crawl because student computers were still being infected. We then implemented the NetReg system (<http://www.netreg.org>) that was developed at Southwestern University. That system allowed us to make sure that all student machines had to register before it was allowed onto the network. This solved a lot of our virus issues since during the registration process we had students install Symantec. Yet, we still had to manually verify that all students had Symantec installed. Toward the end of the school year we were planning a large network upgrade and heard about Perfigo, now Cisco Clean Access. After some research and talking to other colleges using this system, we determined that this would help solve these issues.

How Franklin College implemented Clean Access

Since we already had our network setup with VLANs for our student switch ports and different VLANs for our faculty and staff ports, moving to Clean Access was easier to move to without major network changes. However, adding the NAC to our network was still a major network change since it is a completely different way of thinking about the network.

We setup a test VLAN in our offices with every type of computer that we thought we would see on our network. This lab had at least one machine with the following operating systems: Windows 95, 98, ME, NT, 2000, and XP as well as Mac OSX and a wireless access point. We included a wireless access point so that we could test to see how wireless devices would connect to the network behind the NAC.

Next we change the gateway of this VLAN to the trusted network card of the CAS and added that VLAN to the Clean Access Server. We then needed to setup the roles that we used. We determined that we only needed three roles for users: a student role, a role for faculty and staff, and a role for guests to the campus. To do this we had to add an authentication server, so the system could authenticate users and then add mapping rules to an LDAP attribute for each role. Since we have a different information store in Microsoft Exchange, we mapped the homeMDB attribute to determine the roles.

We then setup different log on pages for each of these operating systems. This allowed us to give a specific message to Windows 95, 98, ME, and NT machines since we do not allow them on our network. This page informs the users that they need to upgrade their machine to a required operating system. For Windows 2000 and XP machines the users get a logon page (see Figure 1), once they logon to this page it requires the users to download the Clean Access Agent. MAC OSX computers are not required to download the agent since it does not run on that operating system. So once they logon they are allowed to access the network.

Figure 1.



After we determined that this worked and that Windows users could log on using Clean Access, we needed to setup what requirements to check for on the Windows machines. This part can get very confusing and requires a lot of testing so below I'm going to explain each part in detail. The Cisco Clean Access system comes with several checks, rules, and requirements already created that you can use out of the box. Most of these are to check for certain Windows updates.

There are four different categories for a check. The first category is a registry check. With the registry checks you can check if a registry key exists or you can check for a specific value of the registry key (Figure 2). The second category is a file check. You can check if a file exists, or you can check the file for its file version or date, either creation or modification date. A Service check is the third category, and with this category you can check to see if the service is running or not. The last check is an application check. This check is a lot like the service check but it checks if an application is running or not.

Figure 2



A rule is a way to group related checks (Figure 3). If you have only one check that you need to look at, then the rule might have only one check but it can have more than one. You specify which operating systems that the rule is for and then using operators (“&” (and), “|” (or), and “!” (not)), you add what checks you would like that rule to check for.

Figure 3

Device Management > Clean Access

Certified Devices | General Setup | Network Scanner | Clean Access Agent

Distribution | Rules | Requirements | Role-Requirements | Reports | Updates

Check List | New Check | Rule List | Edit Rule | New AV Rule | Agent-AV Support Info

Rule Name:

Rule Description:

Operating System: Windows All Windows XP Windows 2000
 Windows ME Windows 98

Rule Expression:

Use checks and operators to create an expression. If a rule condition is true, the client is considered in compliance with the rule.
Operators are "&" (and), "|" (or), "!" (not), and "()" (eval priority parens).
Ex: *check1 & (check2 | check3)*

Next we need to create a requirement (Figure 4). A requirement will have one or many rules associated to it. You can set the requirement to succeed only if all rules are met, any rules are met, or no rules are met. Within the requirement you give the user a way to resolve the issue that they have not met. For example, if students do not meet our registration check, they are displayed a link which will take them to a registration page. You can use either distribute a file, a link, or an antivirus definition update. We have found that it is best to give the user a link and give them step by step instructions on how to resolve their device's issue. Now that we have a requirement created, we need set what roles will have to meet this requirement before they are allowed onto the network.

Figure 4

Device Management > Clean Access

Certified Devices | General Setup | Network Scanner | Clean Access Agent

Distribution | Rules | Requirements | Role-Requirements | Reports | Updates

Requirement List | New Requirement | Requirement-Rules

Requirement Type: (dropdown menu open showing File Distribution, Link Distribution, Local Check, AV Definition Update)

Do not enforce

File to Upload:

Requirement Name:

Description:

Operating System: Windows All Windows XP Windows 2000
 Windows ME Windows 98

(This file is placed on Clean Access Manager. For Clean Access Agent to download this file, HTTP/HTTPS access to Clean Access Manager should be allowed.)

This school year we implemented Clean Access in all of the residence halls as well as on our wireless network. After thorough testing we determined that only student computers need to be checked and that less is actually more when it comes to requirements. We knew that we needed to guarantee that Symantec Antivirus was installed and up to date. We also need students to reg-

ister with us for two reasons. When they register they accept our acceptable use policy and we use this information to bill them for network access. We tested several other requirements such as, making sure that Windows Update is turned on and running, as well as checking for other versions of antivirus software.

After setting up all of this and checking that the checks work, we found one problem where Cisco Clean Access was lacking. How do we provide the user with detailed instructions and files to fix their computer to meet our requirements? Without a vehicle to do this our support calls would go up and we would still have to work on most of the students' computers. We determined that the best way to do this was to create a web application. This application is on a dedicated server since we do not want untrusted devices touching the network. This application had to be easy to use so that if we had a virus outbreak we could quickly put up documentation and files for the user to use to clean their computers.

This web application that we call Enforcer, allows for any member of our IT staff to provide help documentation for the users. They enter the information; it can be text, a file, a link, or images and give them priorities in a form. The information is displayed on the web page based on the priority the item was given. We then take the web address of this page and add it to the requirement. When a user does not meet a requirement they are presented a link to the documentation and they have all the information that they need to fix their computer.

The next part that we needed to figure out was when a student registered their computer with IT Services we needed to record their MAC address. We record this in case we ever have a need to investigate what a user was doing from a specific computer. Unfortunately there is no way to pull this information via an Internet browser, so we had to come up with another way.

We are able to pull the user's username and IP address from their browser. Since Clean Access runs on Linux we knew that it was using ISC's DHCP server (<http://www.isc.org>). This stores the MAC address for every IP address that it hands out to a device. We then created a cron job (scheduled task) that runs a script that copies file that contains all of the IP address leases to a new file. Then that file is sent to the Enforcer server. This script is run on both of our Clean Access Server once a minute. The registration page then checks these files for the IP address that we received from the browser to get the MAC address.

The student then enters in their student ID number and states that they accept the Franklin College Acceptable Use Policy. The system then creates a file that the user runs that enters information into their computers registry.

Conclusion

Cisco's Clean Access system is a very powerful and robust system, that has unlimited possibilities. What it does best is check that applications that you require a user to be running to gain access to your organization's network, or to check for unauthorized applications such as peer-to-peer file sharing software. This system does require a lot of planning and testing. You can not just put it on the network and expect it to be up and running in a day. We spent around 8 months testing and developing the help document system.

References:

Cisco Systems, Inc. Documentation. Last Accessed: April 23, 2006. URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cg/hsec_c/schoverv.htm#wp1000871

Tulloch, Mitch. Microsoft Encyclopedia of Networking. Redmond, WA: Microsoft Press, 2000.