Global Information Assurance Certification Paper

Controlling a network

GIAC Security Essentials Certification (GSEC)
Practical Assignment

Version 1.4b
Option 1

John J Mondello Jr
3 August 2004

Introduction

One of the biggest problems a company faces today is maintaining control over a network. The ultimate goal of service network control is to balance customer satisfaction with high network utilization. But how can you strike harmony between these two different classes of metrics?[1] How exactly does one maintain control over a Wide Area Network (WAN) that is located statewide or nationwide geographically? Control is a very broad term with all sorts of different meanings so I'll start by defining what the definition of control will be for the purposes of this paper.

Below is a sample of an enterprise network service growth:[2]

Time Frame	Devices	Users	Applications	Connection Types	Max. Relationships Requiring Mgmt.
Today (Year 1)	25,000	3,000	100	3	**22.5 billion**
In 3 Years	40,000	4,350	145	6	**151.4 billion**
Per-Year Increase	5,000 (20%)	450 (15%)	15 (10%)	1	**25.1 billion** (Year 2 over Year 1) **66.2 billion** (Year 3 over Year 1) **128.9 billion** (Year 4 over Year 1)

Of the networking technologies available today, there still lacks a convincing strategy to lock down ports to prevent users from plugging a machine into an available drop. Strategies are discussed throughout this paper and will include both pros and cons of each possibility.

The Scenario

Bob: Good morning, Jim. How's everything running today?

Jim: Typical Monday morning, Bob. Network problems seem to be preventing our connection to our sites at Chicago and Denver.

Bob: What do you think the problem could be? Have you checked the routers?

Jim: Yes, and our pings are only going through about half of the time.

Bob: Hmmmm. OK, I'll put a call in to the security guys to see if they can tell me anything.

---

[1] Ratkovic, Aleksandar. "Controlling your service network." 11 February 2002 URL: http://infocus.telephonyonline.com/ar/telecom_controlling_service_network/

[2] Bailey, Stewart. "Gaining Control of Your Network Identity Infrastructure." URL: http://www.infoblox.com/solutions/whitepapers_identity.cfm?CMP=SFS-701300000000HcJ

(Bob calls Fred, the security manager)
Fred: Fred speaking, can I help you?

Bob: Hey Fred. It's Bob from the Network Control Center. Would you know of anything that would be causing connectivity issues?

Fred: I don't think so. I pushed out patches last week but that shouldn't have had any affect. That's about it. Let me check out the Intrusion Detection System logs.

Bob: OK.

(Fred checks IDS logs and finds the possible problem)

Fred: WHOA! I see a ton of ICMP traffic flooding devices everywhere!

Bob: Where is it coming from?

Fred: It looks like most of it is coming from IP address 10.10.20.50. That sounds like a subnet in your building Bob.

Bob: OK. Can you resolve the name or see who is logged on?

Fred: Nope. It is a machine called *FUMANCHU* and someone is logged on locally.

(In walks Jethro, the entry level Network Administrator)

Jethro: What's up Bob?

Bob: (Bob puts Fred on hold) Not now Jethro. We have enough issues right now.

Jethro: Tell me about it. I was just down the hall and Mr. Seabass from HR said that he brought his laptop in from home, plugged it into our network and couldn't get to the Internet or access any of his files on the network.

Bob: What did you say? He brought his laptop *from home* and plugged it into the network?

Jethro: Uhh…I guess. He also mentioned something about some welchia message he saw that popped up on his screen. I was going to look into it in a minute.

Bob: (taking mute off of the phone, Bob begins to speak to Fred again) Fred, I think I've found out who the culprit is. See if you can block that IP address on the local subnet and if the issue clears up.

(Fred does so and the problem clears up almost instantly.)

Fred: Well, my IDS looks like it stopped ringing and I can now ping all the way through to Chicago and Denver.

Bob: Well done, Fred. It looks like that IP address was the problem. So how can we stop that sort of problem in the future?

Fred: (a blank look on his face, even through the phone.): Umm……Good question.

The End

As you can see in this quick case, herein lies the problem. There isn't a sufficient way of locking down what machines can be "plugged" into a network. In the case above, the HR chief, Mr. Seabass, brought his laptop from home because he wanted to download something from his work PC to his laptop so he'll have it on the road with him upon traveling. Upon plugging the little blue cable from his laptop into the wall, his machine infected others across the WAN with the welchia worm, causing a series of Internet Control Messaging Protocol (ICMP) messages to flood the network resulting in a denial of service across the entire company network. Currently, if there is a vacant drop or open jack on a wall, one can simply plug a machine in and without having to worry about providing any domain credentials, can still retrieve an IP address from the good old, reliable DHCP server.

This case demonstrates the importance of control and what its definition is in respect to this discussion. Control is NOT software or commercial off the shelf (COTS) products. It is more of a process that must be maintained by management.

Security is not a product; it's a process. It's the process of paying attention to vendor updates for your products. Not only network and network security products -- browsers, firewalls, network operating systems, Web server software -- but every piece of software you run. Vulnerabilities in your word processor can compromise the security of your network.[3]

Managing remote sites is not about specialized products, but about maintaining standards and extending your organization's core infrastructure, policies and

[3] Schneier, Bruce. "Security is not a product; It's a process." 15 December 1999 URL: http://www.schneier.com/crypto-gram-9912.html - 1

systems. Companies that let remote sites implement one-off technologies lose the cost benefits of standardization.[4]

The Problem

How many times has your boss asked you, "How many machines are on the network?" Can that question really be answered? Well, at that particular moment in time, a ping sweep can be performed, netbios names resolved and a very accurate number can be given. But what if machines were off during the time the ping sweep was performed? Is there connectivity throughout the entire WAN? The question must be asked: Does a network administrator really know a hard, concrete number of machines that are on his/her network?

So why exactly is that question so important to ask? Let's look at it from a security standpoint. I've come up with a motto: "One can only secure what one knows about." The problem is started with not knowing what one has. If you can't see it, certainly you can't secure it.

The "Other" Problem

OK, so you say that you have a good quality control program in place where ALL machines needing network access are required to come from one designated in-house shop. These designated shop personnel are the only administrators that can add/remove machines to the domain and a log is kept so forth and so on. There is still the problem of having unused drops all over the various physical locations of a business area. How exactly can you tell which drops are being used and how it corresponds to the incoming patch panel # it was given? Is that even possible or manageable?

Let's regroup for a minute here. The first problem we ran across was the lack of knowing precisely how many machines were on a given network. Remember, we can't possibly secure what we don't know about. Once a quality control program has been developed and machines are "ran through the mill" (though this may still only be a 95-98% solution), the continuous problem of unused drops still presents an issue that needs to be resolved. How can a company secure LAN drops out in the field without knowing which patch panel numbers to secure and if legit machines are being used?

Solutions?

There are, however not really acceptable, a couple of possibilities out there to combat such a problem:

[4] Brown, Richard J. "Branch Office Management." 22 July 2004. URL: http://www.nwc.com/showArticle.jhtml?articleID=23900506

- Port Security on switches and routers
- VLAN Management Policy Server (VMPS)
- Manual process of matching patch panel to PC.

These possibilities are about the closest thing technology has to offer when it comes to securing ports at the Layer 2/3 level of the OSI model. Let's examine these topics individually and look at both pros and cons to see what we can expect from each technology.

Port Security

What is port security? Let's bring back our case for just a minute and take a look at what happened when old Mr. Seabass brought online his trusty laptop from the house. Unknown to him, his laptop had contracted a virus at some point, a bad one at that, prior to plugging into the network. Almost instantly, the welchia worm took over. According to Trend Micro, the Welchia worm came into existence around February 4th and immediately had an impact on the world infecting over 95,000 machines to date.[5]

The worm was designed to take advantage of a flaw found in the Microsoft operating system. An attacker could exploit this known vulnerability and cause disruption to a network, known as a denial of service attack. Not only did the infected machine cause a series of ICMP messages to flood the network, it also took advantage of the machines that were not patched to protect this known flaw. Basically, the machine came online and said, "I'm going to ping every machine on this network and I won't stop until you fix me. Oh, and by the way, if I come across a machine that isn't patched, I will tell it to do the same thing that I'm doing."

Could port security have prevented this? Is it cost effective? What other business impacts will it cause? Below will be a brief summary of the good and ugly of port security.

Pros

- ✓ *An assumption is made that a company is using up-to-date equipment that includes Layer 2 technology to connect a number of devices on a Local Area Network*

Port security is the act of securing ports on a switch or Layer 2 device by telling it what machines or devices will be able to connect. The primary and most practical way to accomplish this is to involve a one to one media access control (MAC) address assignment. Every device, to include routers, switches, PC's,

[5] Trend Micro "Worm_Nachi.B" 20 July 2004. URL: http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_NACHI.B

laptops, contains a MAC address. This address is hard coded or burned onto the device by the manufacturer of the product.

You can use the port security feature to restrict input to an interface by limiting and identifying MAC addresses of the workstations that are allowed to access the port. When you assign secure MAC addresses to a secure port, the port does not forward packets with source addresses outside the group of defined addresses. If you limit the number of secure MAC addresses to one and assign a single secure MAC address, the workstation attached to that port is assured the full bandwidth of the port.[6]

Once a MAC address is obtained, that address is configured on the port to be assigned to use the port's connection, ultimately allowing connectivity to the LAN indicated by a little green light. Below is an example configuration of port security being used on a Cisco 2950 switch:

router>enable
(enters privileged mode)
router#configure terminal
(enters configuration mode)
router<config># interface fastethernet0/1
(enters interface mode)
router<config-if>#switchport port-security
(turns port security on interface)
router<config-if>#switchport port-security violation restrict
(no other machine can connect to this interface other than the specified Mac address)
router<config-if>#switchport port-security mac-address 1234.5678.1234
(only this Mac address will be able to use this port)

The above configuration will restrict anything from access unless the machine's MAC address is equal to 1234.5678.1234. Turning on port security not only prevents illegitimate machines to connect but it also can prevent legitimate machines from connecting as well. The user may simply think that since his jack is "turned on" that he has a connection and he can just plug anything into it. Wrong answer. Port security denies connection to anything other than the stated MAC address.

Cons

After the forty man-hours it took to set up port security on our switches throughout the campus, Mr. Seabass cannot just bring his hand me down laptop

[6] Cisco "Configuring Port Security." 20 July 2004 URL: http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/12_1e/swconfig/port_sec.htm - wp1042596

from home and all is well right? It sure seems that way. Let's throw a "wrinkle" into the mix.

The boss calls the Network Operations Center one fine Monday morning and informs them that they are due to receive a shipment of 500 computers within the month to replace the existing computers that are pretty much out of there 3-year life cycle. No problem. A team is set up to replace existing machines and remove the old ones and then someone brings up, "What about port security? Will replacing machines have an impact?" The blank stare is back, the empty thoughts appear and the forty man-hours it took to set this up suddenly comes to mind again.

As you can see, a logistical nightmare is at hand. Someone has to manage to get the new MAC addresses, find out where they are plugged into the switch, remove the old MAC address and input the new one. The best part is that it has to be done for every single new machine that is put out into the field.

The management piece of port security is undoubtedly a tough assignment to keep up with. For what is does, is it really worth that much attention? These are the questions management must answer.

Summary of port security

In summary, port security provides a working answer to solve the issue of unknown machines showing up on the radar; however, it comes at a price. The price is paid in the managing aspect of it rather than the literal meaning of price. Add that with the manpower needed to produce such efficient results and you can surely guarantee a headache daily.

Pros

- One to one mapping of a device
- Prevents unauthorized use
- Highly secure
- Inexpensive

Cons

- Not scalable
- Logistical nightmare
- Extremely difficult to manage

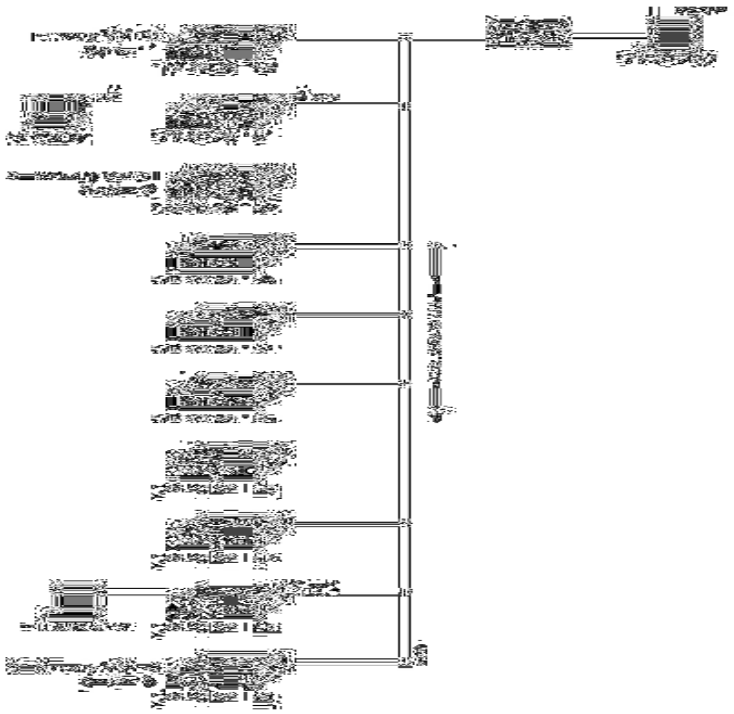
VLAN Management Policy Server

VLAN Management Policy Server (VMPS) works very similar to the way that port security works. The concept of locking ports down applies to VMPS as well. The

biggest difference between port security and VMPS is the way the MAC addresses are handled. Given our same case study with Mr. Seabass, we will examine the features of VMPS and see if it may produce technology better suited for an environment needing to secure connectivity within a WAN.

VMPS, proprietary to Cisco, allows you to assign switch ports to VLANs dynamically, based on the source MAC address of the device connected to the port. When you move a host from a port on one switch in the network to a port on another switch in the network, the switch assigns the new port to the proper VLAN for that host dynamically.[7]

Below is an example of how VMPS works:



1. User's machine on Ethernet segment port 3/1 requests IP address
2. Local switch points back to primary VMPS server for approval
3. Primary VMPS server checks machine running tftp server for the text file containing MAC address to VLAN mappings
4. The Trivial File Transfer Protocol (TFTP) server responds to the primary VLAN server with which VLAN machine belongs to
5. Machine is given IP address in its corresponding VLAN.

[7] Cisco "Understanding how VMPS works." 20 July 2004 URL: http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_guide_chapter09186a00800c65e4.html - 1019855

Pros

When compared to port security, VMPS has an advantage in the way that the ports can be centrally managed through the VMPS server. MAC addresses are input into a text file and assigned a Virtual Local Area Network (VLAN). This becomes useful when legitimate machines must move around within the office or building. As long as ports on the switch are set up in the text file, it doesn't matter where the machine is plugged in. In addition to its mobility, VMPS also accomplishes the same counteraction as defined in port security to defend the network of Mr. Seabass.

Cons

Though VMPS offers a little more than port security, the logistics of managing what MAC addresses are active or not active still resides. Computer turnover and the process of new machines coming online will present a nightmare when trying to differentiate which MAC addresses are legit vs. the older ones in the appropriate text file.

The constant communication between primary VMPS server and TFTP server leads to the issue of processing power and bandwidth. Depending on the type of switch and hardware specifications, the switch load will increase substantially which can affect performance. The TFTP server also serves as a single point of failure. If the file that resides on the TFTP is down, the primary VMPS server will not be able to find out VLAN info for devices.

Summary of VMPS

In summary, VMPS is another working solution that offers a little bit more enhancement compared to port security, but still not a viable method.

Pros

- Mobility
- Centrally Managed

Cons

- Turnover of devices
- Single point of failure
- Processing power on switch

Manual Process

Any time the word "manual" is used in technology, the words manpower and time come to mind. In this case, that is just what this solution entails: a manual

method of knowing which patch panel numbers match with what machines are actually legit.

Paula Lea, the Academic Registrar of Cumbria Institute of the Arts, speaks about a product that has shown to improve their business by eliminating the need for manual processes. "SITS has provided us with an efficient and accurate reporting tool, and has given us the ability to automate many processes and returns which previously had to be done manually. This saves us substantial amounts of time and resources, which we can now channel into making other IT processes more efficient."[8]

Countless hours will be spent figuring out that: Mr. Smith of public relations is plugged into jack that is labeled 100, so we'll just check that one off as being legit. Even once all legit users are accounted for, there is no way of checking if Mr. Smith brings his laptop from home and plugs into the jack labeled 100. As you can see, the manual method offers very little, is very painful, requires huge amounts of time and manpower and does not provide any way of checking legit machines vs. non-legit machines.

Pros

- Computer jacks are turned off and require higher authority to "turn them on"

Cons

- Not scaleable
- Manpower intensive
- Excessive time spent
- No way of checking for legit machines

SUMMARY

Of the three choices, the VMPS solution would appear to be the best of the three, though at a price. Thought management intensive, it is centrally managed with appealing features that could help in controlling the network.

Part of the inspiration in choosing such a topic was brought about by an idea. That idea involved a DHCP server only giving out leases to netbios/machine names that meet certain criteria. For example, when conducting a search for excel files, one would put in *.xls. This would return all excel files. Apply the same concept but for DHCP giving out leases to certain machine names. If a company implements a special naming scheme that is unique to them, you could

[8] Lea, Paula. "Thoughtful solutions for Cumbria Institute of the Arts." 20 July 2004 URL: http://www.sits.co.uk/pdf/SITS-case-study-Cumbria.pdf

simply say only give out a lease if the machine name begins with LANO*. This would prevent unknown machines from just plugging in.

When trying to decide a way of locking down unused ports, the technology and tools are limited. One must assume the worst-case scenario and prepare. It is vital that a process be put in place to secure what is and is not on the network in the best way possible.

Reference List

Ratkovic, Aleksandar. “Controlling your service network.” 11 February 2002 URL: http://infocus.telephonyonline.com/ar/telecom_controlling_service_network/

Bailey, Stewart. “Gaining Control of Your Network Identity Infrastructure.” URL: http://www.infoblox.com/solutions/whitepapers_identity.cfm?CMP=SFS-701300000000HcJ

Schneier, Bruce. “Security is not a product; It’s a process.” 15 December 1999 URL: http://www.schneier.com/crypto-gram-9912.html - 1

Brown, Richard J. “Branch Office Management.” 22 July 2004. URL: http://www.nwc.com/showArticle.jhtml?articleID=23900506

Trend Micro “Worm_Nachi.B” 20 July 2004. URL: http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_NACHI.B

Cisco “Configuring Port Security.” 20 July 2004 URL: http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/12_1e/swconfig/port_sec.htm - wp1042596

Cisco “Understanding how VMPS works.” 20 July 2004 URL: http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_guide_chapter09186a00800c65e4.html - 1019855

Lea, Paula. “Thoughtful solutions for Cumbria Institute of the Arts.” 20 July 2004 URL: http://www.sits.co.uk/pdf/SITS-case-study-Cumbria.pdf

Last Updated: July 23rd, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor