GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at http://www.giac.org/registration/gsec

Changing Firewalls for the Better

Joseph Tucker

Sunday, 2 May, 2004

GSEC Practical Version 1.4b
Option 2 – Case Study

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Abstract

I work at a small investment company (Company Z). For a while, Company Z had been using a managed service provider to manage the company's CheckPoint 4.1 firewall. Using the managed service provider was supposed to relieve Company Z from the routine monitoring of the traffic traversing the firewall. Due to a chain of circumstances, however, I discovered that the service provider did not monitor the firewall, nor did the service provider have vendor support for the firewall product they had given us. With a poorly configured firewall on our perimeter network, we were not providing confidentiality to our users since our corporate information and data were available to unauthorized people. We also could not assure network availability to our end-users because unauthorized traffic coming into our network was taking up network bandwidth.

In this paper I will illustrate how I helped Company Z become aware of the managed service provider's limitations, how I helped Company Z change to a new managed security service provider, and how doing so increased the perimeter security of Company Z.

Background

Company Z had outsourced the management of the company's only firewall to a managed service provider for about the last seven years. Because there were limited in-house IT resources to constantly monitor the firewall, it was only logical that Company Z would look to outsource their firewall management. After the original setup of the firewall, however, the IT staff never reviewed the firewall policies when rules were added or modified. Company Z relied solely upon the service provider to determine the validity of the policies.

Throughout the winter of 2002 and spring of 2003, Company Z was working on a Disaster Recovery plan than included setting up a second facility to use in the event of a disaster. Since we would need to have a firewall at that location, a colleague and I went to a CheckPoint firewall training class. (The CheckPoint firewall at the second facility was not managed by a service provider.) My colleague and I were responsible for configuring the new CheckPoint firewall for the second facility. Because the policy for the second facility was relatively simple, we had no need to reference the primary facility's firewall policy. After the second facility was set up, my colleague and I thought it would be advantageous to look at our primary facility's current firewall policy for comparison. As well, we wanted to document both policies and note any differences between the primary and secondary facilities. I learned that, up to that point, we did not have readily available access to view the firewall policy or the log viewer of the primary firewall. In the summer of 2003, we contacted the managed service provider and they e-mailed us a copy of the firewall policy. The policy had several rules that conflicted with one another, along with many

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

outdated rules. We were completely shocked to see some of the rules that were in the policy. It was blatantly obvious that no one had reviewed the firewall policy for a very long time. It was equally obvious that the service provider did not take notice of questionable rules within the policy.

When we challenged the managed service provider about the firewall policy and the rules that were set up, the service provider's response was short and simple: it was not their responsibility to determine which rules were "appropriate" for our environment. The service provider claimed that their responsibility was only to add/modify rules as our Company requested them.

When my colleague and I brought up this issue to IT senior management, we were told that the firewall was apparently working, and we (the Company) were not having any issues, so nothing was to be done about it. Our initial efforts to illustrate the dangers of our firewall policy were rebuffed with other projects that had supposedly “more importance.” When pressed to at least consider changing managed service providers, my colleague and I were again told that the issue could wait until a later date.

In order to attempt to convince the senior-level management that this situation required immediate attention, I went back to the managed service provider and asked if I could have access to the firewall logs. I wanted to see the traffic at the firewall level to observe what was coming in and going out of our network. With a little reluctance, the service provider allowed me to see the logs (after several failed attempts to grant me permission due to technical difficulties on their end). Unfortunately, the logs locked up regularly- at least once and hour. Entries in the log that occurred while the log viewer was locked up became unavailable once the log viewer was reset. After keeping track of the logs for just a week, I had enough raw data to illustrate the dire need to improve the perimeter firewall.

The limited logs that I could view showed a few important items that I could show to the senior management. There was a plethora of e-mail trying to relay off of our e-mail server. There was erroneous Internet traffic that was able to enter our network because of outdated rules. Some ports were allowed promiscuously which were allowing worms into our network. And, most discouraging of all, unrestricted remote access software was able to enter through our network.

It was very clear that the service provider was not monitoring the traffic that was going through our firewall. I confirmed this by calling and asking the service provider directly. The service provider admitted that they do not routinely look at the logs or monitor traffic unless there is an outage or disruption of service of some kind. I also obtained a copy of our signed contract with the service provider. The service provider’s description of services for which they were responsible included only two items: maintenance of the hardware, and adding routes and rules to the policy as our company requested. Neither traffic monitoring nor log auditing was not a part of their services.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

While my initial reaction was to try and convince management that this was all quite serious and warranted immediate action, I acknowledged that my opinions and influence to this point were not enough to get the attention of senior-level management. So my approach was to encourage a network security audit to be performed by an outside 3rd party vendor.

My intentions were to have the auditors validate the problems that we had already mentioned with our firewall, and hopefully gain a little attention to the need for more stringent IT security practices. Rather than present a case singling out the firewall, I encouraged a full audit of the IT core services to determine all vulnerabilities that may exist. Other people within the department help a little more influence, and they were interested in an audit of their group, so getting support for a full audit was more openly received. My proposal to have an audit was accepted, and throughout the fall of 2003 we interviewed several companies to perform the audit. In the end, one particular vendor stood out among the others, so they were chosen to perform the audit in February 2004.

Service Provider

Strike One: The CheckPoint vulnerability alert from ISS

On Wednesday, 4 February, 2004, Internet Security Systems (ISS) released an alert stating that CheckPoint VPN connections were vulnerable to a possible ISAKMP exploit[1]. The alert that was published at the time claimed that the vulnerability affected CheckPoint version 4.1. Included in the vulnerability alert was mention that CheckPoint, however, had stopped supporting version 4.1[2]. ISS released a second alert that was published saying that there was an HTTP parsing vulnerability in 4.1 as well[3].

I contacted our managed service provider to find out what they were doing regarding these vulnerabilities and what was required on our end. Again, their answer was short and simple: nothing. The service provider contended that, because we had a CheckPoint version that was no longer supported by CheckPoint, our only option was to upgrade to the newest version of CheckPoint's software or else be exposed to both high-risk vulnerabilities. The service provider never mentioned that we were not using the HTTP Security Server (which was exposed to the HTTP parsing vulnerability), so we were technically only exposed to the VPN vulnerability. But the service provider's immediate reaction was for our company to disable VPN access over the

[1] Internet Security Systems X-Force Advisory. "Checkpoint VPN-1/SecureClient ISAKMP Buffer Overflow." 4 Feb, 2004. URL: http://xforce.iss.net/xforce/alerts/id/163 (2 May 2004)
[2] Insomniac, "CheckPoint 4.1 Vulnerability." 6 Feb, 2004. URL: http://neworder.box.sk/explread.php?newsid=10580 (2 May 2004)
[3] Internet Security Systems X-Force Advisory, "Checkpoint Firewall-1 HTTP Parsing Format String Vulnerabilities." 4 February, 2004. URL: http://xforce.iss.net/xforce/alerts/id/163 (2 May, 2004)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

weekend. During that time, the service provider would wait and see if CheckPoint may (or may not) release a patch. Posed no other alternatives from the service provider, we acquiesced and notified our users that VPN access was being disabled for the weekend due to a security issue with our VPN product.

Strike Two: The fall of an outdated firewall appliance

Over the weekend during which VPN connections were disabled, the firewall appliance at our location (that was managed by the service provider) malfunctioned and was no longer working. In other words, our Internet access had been interrupted. Around noon on Sunday, 8 February, 2004, I went into the office to get on the phone with the service provider to attempt to rectify the problem. By 2am Monday morning, the service provider had tried to remotely manage the firewall, modify configurations, and change policy all through a serial modem connection without success. We were still without a working perimeter firewall.

At this point, the service provider conceded that the appliance must have malfunctioned and would need to be replaced- which could happen within 48 hours. It was at this time that I was told that our service provider could not get direct support from CheckPoint because the service provider had let their CheckPoint vendor support contract expire. I arranged to have a new firewall shipped out to us, and then hung up the phone with the service provider.

I configured an off-the-shelf DLink firewall for a temporary solution. I had the list of rules that existed in our previous policy, so I made an effort to only create rules that were absolutely necessary for immediate Internet communication. My goal was to provide Company Z with limited-yet-functional Internet access until we could implement a properly working firewall. With the exception of a few static routes that had to be added later in the morning, the Internet connection was up and working by the start of business Monday morning.

Strike Three: Where's the management???

Coincidentally, Monday, 9 February, 2004, was when the 3rd-party Network Security Audit was to begin. When I explained to the auditors what the situation was, they agreed to elaborately detail the firewall issues. I wanted to make certain that they placed strong emphasis on it given the current state of affairs.

On Wednesday, 11 February, 2004, the "new" firewall appliance showed up from the service provider. It was a CheckPoint 4.1 firewall loaded on a Nokia appliance. During the day we went ahead and set up the “new” firewall in the equipment room and attached a monitor to it just to see what the firewall reported while booting up. Already it was giving error messages that the Licensing was out of compliance. Cutting short our losses for the time being, we went ahead and proceeded with implementing the “new” firewall. That evening we put the

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

"new" firewall in place, connected it to our network, and tested everything successfully (meaning simply that traffic was passing through the firewall to and from the Internet for basic services such as e-mail).

Thursday morning I asked the service provider for a copy of the policy that was installed on the "new" firewall, along with the entire configuration of the firewall appliance itself. At the same time, I had the auditors perform a thorough scan against the firewall. I wanted to see what condition the firewall was in, and what traffic was able to penetrate through the firewall.

While the firewall was routing traffic between the DMZ and the Internal network properly, the policy showed a rule that completely misused the negation option. Rule number twenty stated:

> Source: Any IP Address that is NOT in the "Blocked_IP_Address" group
> Destination: ANY
> Service: Anything other than HTTP
> Action: Accept

18	Blocked_IP_Addresses	Exceptions-HTTP	http	accept	Long	Gateways	Any	Allows Active-X from certain IP addresses
19	Blocked_IP_Addresses	Exceptions-HTTP	http	accept	Long	Gateways	Any	Strips Active-X from all html not originating from the exception addresses
20	Blocked_IP_Addresses	Any	http	accept	Long	Gateways	Any	Anything outbound from IP addresses other than those being blocked

The rules immediately above rule twenty give a little indication of what purpose the rules were meant to serve. There is a firewall object called Blocked_IP_Addresses. The IP Addresses contained within that object are IP Addresses assigned to temporary employees and consultants. These temporary employees and consultants are supposed to be restricted from unnecessary Internet access. Rules eighteen and nineteen apparently intended to say that any IP Address that is not in that Blocked_IP_Address group is allowed to use HTTP for Internet access. Rule twenty was probably intended as a (poorly chosen) default rule whose purpose was to allow any traffic from the Internal LAN to the Internet. However, by using the negation feature improperly, the service provider unfortunately allowed all traffic through the firewall.

I immediately caught this rule by reviewing the policy that was sent to me from the service provider. I contacted the service provider to see if we could change the rule to appropriately reflect our environment. Their response was that, because it was a default rule for outbound traffic, it might disrupt other services. Unless we (the company) knew specifically what we wanted opened on the firewall, the service provider actually encouraged us to leave that rule alone.

The auditors then found that the management ports of the firewall were open to any IP Address. They had successfully connected to the firewall remotely from an External IP Address as well as from a non-authorized Internal IP Address. (Note: The auditors were given permission to perform such a scan. In this

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

context, “non-authorized” means an Internal IP Address that should not have been allowed to do something.) With this information, and with the events of the previous weekend, it did not take much to convince senior IT Management that we needed to switch service providers.

No looking back: A new MSSP

Selecting the MSSP

There were three main criteria for getting a new managed service provider to work with us: quality of services, cost of services, and the ability to quickly migrate from our current service provider to the new service provider. There was a number of Managed Security Service Providers (MSSP) that would meet our needs. After getting information from a number of companies and interviewing several of them over the phone, I narrowed the search down to three companies. We brought these three companies in for a more thorough interview and to give each a chance to explain their services at length. We made our decision and went with a company called Lurhq. Given our recent experiences, we selected this MSSP based on their ability to allow us full access to view and change our firewall policies as needed. They refer to such a service as “Open Service Delivery.”[4] I contacted Lurhq to inform them that we would like to use their services.

We arranged for a conference call between myself, the project coordinator at the MSSP, and the engineer from the MSSP who would be working with me on the implementation of new firewalls. We went over the needs of my company's network and came up with a perimeter network design that involved two firewalls- creating a physical DMZ- and segmentation of some of our Vendor routers off of the LAN.

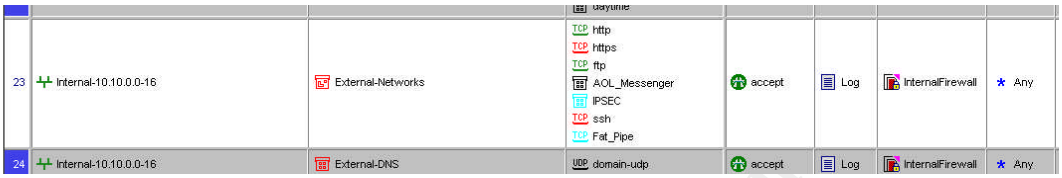
To implement this design, I had to evaluate and recommend the purchase of hardware and software for the firewalls we were going to use. With encouragement from our senior-management to stay with CheckPoint (the investment was already there with the training some IT staff had already received), I researched the most appropriate hardware and Operating System (OS) platform for the firewalls. Staying with the same hardware vendor as our current servers seemed to make the most sense. The OS decision came down to two choices: CheckPoint's Secure Platform (SPLAT), or a secure version of Red Hat's Linux. In the end, since our MSSP was going to be working with us on the firewalls, their recommendation of Red Hat's Linux distribution over SPLAT was the deciding factor.

Implementing the new firewalls

[4] “OPEN™ Service Delivery: The Foundation For A Trusted Security Partnership.” Delivering Superior Managed Security Services. URL: http://www.lurhq.com/why.html (2 May, 2004)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

I worked with Lurhq to come up with an efficient firewall policy. I made sure that we were using a defined object for the Internal LAN as opposed to using "Any" as a default catch-all. The only inbound request allowed through the firewall from the Internet was for e-mail. There were services restricted for our DMZ that deal with Vendor networks. Those were locked down to allow only specific ports to the necessary IP Address. I restricted all outbound requests to the Internet to only eight necessary services (seven in one rule and DNS in another):



Once the configuration was finished, I notified our company that we were going to be replacing our firewalls on a Saturday and that Internet accessibility would be disrupted for 24 hours. That seemed like a sufficient window for switching out the firewalls. In our preparations, we had planned out specific timelines for the migration to occur.

There were several issues that were unavoidable- many of the static routes that were on the previous firewall (and not documented anywhere else) were not included in the information given to me by the former service provider. It took a little while to get the necessary information by evaluating dropped traffic at the firewalls. Once that information was obtained, it took a little longer to add routes and configure the new firewalls accordingly. However, come the following Monday morning, a new perimeter network was in place and more efficiently protecting our network.

Results speak for themselves

Immediately after putting in the new firewalls we were able to see a dramatic improvement in performance with our vendor routers. We also noticed improvements in our Internet connectivity. We were able to isolate some of the problems we were having with network traffic by isolating our company's content filters within the DMZ.

Courtesy of the reporting available from Lurhq, we were able to see the amount of traffic that was now being dropped by the firewalls compared to what was penetrating our network before. By changing our service providers, we are now in a better position to ensure the confidentiality and availability of our network resources than we were before. Because of stricter firewall policies, we have eliminated the vulnerability of having the firewall management ports exposed. This will help prevent an attack against the firewall from the outside that would disrupt the availability of network resources from legitimate users.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Conclusion

The security that did not exist at all with our old firewall was damaging to our network. Our User Services Group had been fending off worms, viruses, and spam for a long period of time. In the afternoon, our Internet connection would slow to a crawl. Despite all of that, we were receiving no support from our service provider.

It was difficult to get management buy-in to an idea early on. Senior management was finally able to see the severity of the issue once the firewall malfunctioned. The Chief Information Officer actually worked with me while I was configuring the DLink firewall at 4:00am. The realization that we were greatly exposed made a lasting impression. So from a very bad experience came a great benefit to our company. Most notably, there was a mindset that "if it is not broken, do not fix it." Well, spending thirty-five hours in the office fixing a broken firewall is not my ideal way to spend a weekend!

After the fact, CheckPoint came out and said that the ISAKMP vulnerability did not exist in version 4.1 as ISS had stated.[5] The irony is that it took the firewall reaching its breaking point for our company's senior-level management to notice. With a little coincidence, the need to replace our firewall was driven by the failure of a prior service provider to actually provide us with a service. With ironic timing, the security auditors were able to give validation to the urgent need for a stronger firewall presence on our perimeter network. By addressing the firewall problem, I have had the opportunity to raise the visibility of security in our company. The network security audit- originally intended to stress the need for a new firewall- has also exposed other areas that we need to address. And, most importantly, the MSSP that we have gone with has surpassed our expectations by alerting us to events and keeping in regular contact with us regarding new threats and vulnerabilities. Overall, improving our firewall has greatly improved the security of our company from where it was just months ago. Now, we are able to provide with confidence a high level of confidentiality from external sources and network availability to our end-users.

[5] ISAKMP Alert. 7 Feb 2004. URL: http://www.checkpoint.com/techsupport/alerts/41_isakmp.html (2 May 2004)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

References

[1] Internet Security Systems X-Force Advisory. "Checkpoint VPN-1/SecureClient ISAKMP Buffer Overflow." 4 Feb, 2004. URL: http://xforce.iss.net/xforce/alerts/id/163 (2 May 2004)

[2] Insomniac, "CheckPoint 4.1 Vulnerability." 6 Feb, 2004. URL: http://neworder.box.sk/explread.php?newsid=10580 (2 May 2004)

[3] Internet Security Systems X-Force Advisory, "Checkpoint Firewall-1 HTTP Parsing Format String Vulnerabilities." 4 February, 2004. URL: http://xforce.iss.net/xforce/alerts/id/163 (2 May, 2004)

[4] "OPEN™ Service Delivery: The Foundation For A Trusted Security Partnership." Delivering Superior Managed Security Services. URL: http://www.lurhq.com/why.html (2 May, 2004)

[5] ISAKMP Alert. 7 Feb 2004. URL: http://www.checkpoint.com/techsupport/alerts/41_isakmp.html (2 May 2004)

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Last Updated: July 26th, 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
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
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
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
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
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
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
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
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
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 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
Community SANS Indianapolis SEC401	Indianapolis, IN	Oct 09, 2017 - Oct 14, 2017	Community SANS