

**Intrusion  
Prevention  
Tools for  
Defense  
In-Depth**

**SANS WhatWorks  
in Internet Security**

**TippingPoint  
at  
The American  
Red Cross**

**2006**



# TipingPoint at The American Red Cross



## About The American Red Cross

The American Red Cross, a humanitarian organization led by volunteers, will provide relief to victims of disasters and help people prevent, prepare for, and respond to emergencies. Each year, in communities large and small, victims of some 70,000 disasters turn to neighbors familiar and new -- the nearly 1 million volunteers and 35,000 employees of the Red Cross. Through more than 800 locally supported chapters, more than 15 million people gain the skills they need to prepare for and respond to emergencies in their homes, communities and world. As part of the International Red Cross and Red Crescent Movement, a global network of more than 180 national societies, the Red Cross helps restore hope and dignity to the world's most vulnerable people. The Red Cross is not a government agency and relies on donations to do its work.

## About the Speakers

Gordon Bass is the acting chief information security officer for the American Red Cross. He is responsible for the security of the information used daily to perform the Red Cross mission, including that of blood donors, financial donors, volunteers and victims of disasters.

Michael Cokenour is the senior information security engineer/analyst. Within IT and the OCISO at The American Red Cross, he is responsible for assessing vulnerabilities, threats and gathering research on malware, exploits and mitigation.

## SANS Summary

When Hurricane Katrina made landfall on the Gulf Coast, The American Red Cross realized that it would be handling a nearly unprecedented volume of new, temporary networks, systems and shelters. Those networks would serve as a major communications link between hurricane survivors and their families and friends, as well as between the numerous shelters and the main office. Ensuring the confidentiality and availability of the information traveling through those networks prompted The Red Cross to look for an intrusion prevention system (IPS).

~~~~~

To hear Gordon Bass and Michael Cokenour expand on the answers below, view their presentation slides, and listen to their answers to many more detailed questions asked by other users from around the world, go to <http://www.sans.org/webcasts/archive.php>.

~~~~~

**Interview**

**Q. What was happening at The Red Cross that led you to look for an intrusion prevention system?**

A. There had been malware incidents that had consumed us for hours or days. We knew that when Katrina hit, we would be so busy responding to the hurricane crisis that facing another malware outbreak would have been like the "Perfect Storm" and we could not withstand that. The availability and confidentiality of those using the shelters was terribly important. Microsoft Tuesday was also right around the corner.

***"It was the only product where user feedback substantiated that it truly was plug-and-play and as easy to use as the vendor advertised."***

Because we also have biomedical regulated devices on our networks, we cannot patch until we complete rigorous assessment of the patches. Using an IPS would give us a protective layer to guard all of our networks.

**Q. What process did you use to look for a solution?**

A. It was on the SANS list of WhatWorks and so we used that information and the opinions of others in the infosec community. We didn't have a lot of time to look into this because of Katrina, so user feedback was very important. This was the only product where user feedback substantiated that it truly was plug-and-play and as easy to use as the vendor advertised.

**Q. What product did you select?**

A. We are using TippingPoint Intrusion Prevention Systems.

**Q. Did you consider any other IPSes?**

A. We talked to people in the industry, and it was very clear that this product was head and shoulders above the rest. We had some experience with other products, but they were not what we wanted. We did consider Cisco's IPS, but they could not guarantee that it would be "plug-and-play" so we had to pass on their offer, even though Cisco is a trusted partner and was a key asset in the hurricane response efforts. Cisco had a complementary product called Cisco Clean Access, which we decided to implement as well, but we realized this product would take some time to put into service. Time was not on our side at this point.

**Q. What were the key criteria you decided were most important?**

A. Effective, trouble-free and quick. These three criteria were paramount and without all three we would not move forward at this point in time.

**Q. How long did it take to get the IPS and put it in place?**

A. We told TippingPoint we wanted it, and the box arrived the next afternoon. The TippingPoint engineer installed it that day with our network and IT security folks. Everyone involved in the process pushed to get it in quickly because of what was happening with Katrina.

We set it up with a default install and then made some tweaks, like permitting instant messaging (IM) because the people in the shelters might need it to reach out to friends and family. We did elect to block IM file transfers so we would not have security issues involved with that vector.

**Q. What level of manpower does it require?**

A. Extremely minimal. I was really thorough about monitoring for the first 48 hours, but after that I realized I didn't need to do that much with it because

*"We have plans to purchase additional TippingPoint IPS devices in the near future."*

what it blocked by default was pretty good and the reporting seemed accurate.

**Q. What kind of tweaks did it require after the initial setup phase?**

A. We activated blocking for the spyware category, as well as for IM file transfers we mentioned.

**Q. Where did you deploy the technology?**

A. We first put the IPS device in line with the Shelter Network as they were just getting connectivity. This provided a “buffer” of sorts to keep our main network from adversely affecting communications at the shelters and from anything they might do that could harm our internal networks. We had a good test bed that allowed us to watch packets being blocked from the time the first couple machines came up to the time that the shelters were fully up and running.

***"We saw spyware and adware blocked as well as IM file transfers."***

We then configured an interface to also filter our remote dial-up traffic. This was a good test prior to deploying the IPS in front of our VPN concentrators that see similar traffic, but are more fully utilized.

After the shelter, RAS and VPN were protected, we then, at the time of the Microsoft WMF vulnerability, decided it was time to consider installing it at our Internet gateway. On day one as we were making this decision, TippingPoint put out a signature to catch the first WMF exploit seen in the wild. That sealed the idea of putting it at the gateway. TippingPoint followed with another signature a couple days later and we started seeing blocks of malicious code from the WMF exploits on our TippingPoint IPS.

**Q. Your network is rather complex because of the temporary networks you need to add. Can you describe how the organization and shelter networks interact and what kind of traffic passes through them?**

A. This has been a first for us due to the sheer size of the area affected and the great number of people devastated by the disaster. Shelters had to be erected in various geographic locations and the use of various vendors' equipment for communications had to be put up quickly and professionally. Luckily, all the vendors put aside competitive rivalries and acted for the good of the victims. We were able to have people use e-mail, IM and eventually a database to connect with those who did not know where they were. People in the shelters were also able to contact those they might not have known what had happened to. We also have our client assistance traffic that traverses some of the shelter networks. That data contains private and sensitive information and we must maintain its confidentiality. And again, we also move biomedical data through these networks as well as Armed Forces emergency communications.

*"Hearing such honesty from the sales rep really built trust. The TippingPoint sales engineer was very forthcoming, which increased our confidence in his product and support."*

**Q. I understand you received many offers of help from the IT community during Katrina. How did that play into your choice of product?**

A. Well, where do we start on this one? The outpouring of help from vendors that we had partnerships with to vendors that we had never done business with was amazing. Everyone was working for one cause -- the evacuees and victims down South. Not only donations of hardware, but many companies sent employees to help on whatever we needed. I hate to bring up vendor names as I will leave someone out and there were so many. The IT and infosec vendors really put those devastated by the hurricane first.

In the first couple of days, we tried to anticipate the problems that might arise. We thought of all of the fraud and phishing we would begin to see. We knew after the tsunami in December 2004 that where there is a disaster, the bad guys aren't far behind. I sent an e-mail to the SANS Internet Storm Center pleading for help from handlers and others to keep an eye out for anything phishy or fraudulent looking.

Well, I learned that if you ask for help from SANS or the Storm Center, the cavalry shows up. Marc Sachs and others e-mailed wanting to do more than just monitor the Internet. That led to Alan, Marc and Erik Fichtner showing up the next day and asking what we needed and what could they do to help. Volunteers from SANS ISC started to e-mail us asking where we needed help. Many ended up in far-flung shelters, our distribution center in Austin and here at NHQ. Others took the call and kept watchful eye on the Internet for us, along with help from the US-CERT folks. Alan and SANS were extremely generous to give us a substantial donation to help shore up security for our enterprise so that we may protect the victim and donor data now and in the future.

**Q. I understand TippingPoint gave you the product. How did that come about?**

A. After hearing what its users had to say, we told TippingPoint we wanted the IPS and they gave it to us for free. It is not unprecedented for a vendor to

***"Amazingly, we have yet to have an identified false positive."***

provide us with a free product so they can introduce us to new and beneficial technology. TippingPoint wanted to help in the wake of the hurricane relief effort and was generous enough to donate two devices. These types of donations, while ensuring availability, integrity and confidentiality during the

response, also allow us to utilize the funds the American public donates directly in the field helping the evacuees.

We do have plans to actually purchase additional TippingPoint IPS devices in the near future.

**Q. Did the device pass the network guys' tests?**

A. The network guys were a little gun shy, but all their questions were answered skillfully by TippingPoint. They didn't really have any concerns when everyone began working together. At first, there were questions of blocking legitimate traffic and of creating choke points. However, all our concerns were allayed with what we saw in the prior SANS webinars and the case studies, as well as in the information provided by TippingPoint's staff. Of course, we had a failover so that we were prepared if we plugged the IPS inline and packets didn't flow. Packets did flow and as mentioned, monitoring allowed us to rest easy after the initial days. All went as planned and explained.

**Q. What level of senior management approval did you need?**

A. We were required to get sign-off all the way up to our CIO, Steve Cooper. Steve very much understood the concerns about security and was a big proponent of getting the system in place.

*"The absence of complaints and concerns speaks for itself. Our network people are really onboard with TippingPoint and are trying to find other uses for the product."*

**Q. How do you know it actually works?**

A. The IPS logs identified that some Zotob worm traffic was being blocked by the IPS soon after it was brought online. The infected PCs that were the source of the Zotob traffic were removed from the remote networks and rebaselined.

**Q. Any more proof it works?**

A. We saw spyware and adware blocked as well as IM file transfers. We currently are seeing an average of approximately 15,000 hits on the spyware signature a day. Now admittedly, many of those are from repetitive attempts by the same machine. You must go in and actually remove the spyware once alerted or you are going to see it continue to hammer away.

**Q. What problems arose and how did TippingPoint respond?**

A. As part of due diligence, we looked at a lot of the WhatWorks case studies and asked TippingPoint about potential problems. The only notable problem was in a revision to the firmware. The sales rep told us TippingPoint had corrected an improper RFC, but because it wasn't followed consistently it caused some issues. Hearing such honesty from the sales rep really built trust. Many vendors tend to downplay or not admit to their mistakes. The TippingPoint sales engineer was very forthcoming, which increased our confidence in his product and support. Since then, he has followed up frequently just to make sure we haven't had any issues.

**Q. How was technical support?**

A. I have not had to call TippingPoint tech support in the many months we have had it deployed. I should also add that they followed up several times to make sure everything was working well.

**Q. Did you consider a host-based intrusion prevention alternative?**

A. We would view HIPS as a complimentary product. As we were pressed for time, a network IPS was a quicker fix. Anything being installed on our

***"...it was very clear that this product was head and shoulders above the rest."***

servers and desktops that changes our baseline image would require further testing with all our biomedical applications. We just did not have the

time to pursue that option.

**Q. Did you have any problems with false positives?**

A. Amazingly, we have yet to have an identified false positive. Since implementation, we haven't had a case where a user has identified any issues that related back to the IPS configuration.

**Q. Any features you would like to see added?**

A. The reporting could be a little more robust and it can be a little cumbersome to create custom reports. Don't confuse this with the actual alerting or the viewing of what is happening; I am only speaking of going back and trying to create reports for trending and the like.

**Q. How do you feel about the TippingPoint IPS?**

A. The absence of complaints and concerns speaks for itself. Our network people are really onboard with TippingPoint and are trying to find other uses for the product. I love the product, company and people we work with.

*"I love the product, company and people we work with."*

We have such a fluid environment because of our need for temporary networks that typical security controls would have required a Herculean effort. It was really simple to let TippingPoint identify bad traffic and take care of it.

~~~~~

**SANS Bottom Line on TippingPoint at The Red Cross:**

1. Very quick delivery and install;
2. Good default block settings;
3. Requires limited adjustments and monitoring -- truly plug-and-play;
4. Reliable;
5. And most importantly, it stops the bad stuff cold.

**For more information on TippingPoint:**

**Visit: [www.tippingpoint.com](http://www.tippingpoint.com)**

**E-mail: [info@tippingpoint.com](mailto:info@tippingpoint.com)**

**Phone: 888-TRUE-IPS**