SANS

WHAT WORKS™

Inspecting Encrypted Traffic with the Blue Coat SSL Visibility Appliance

SPONSORED BY

BLUE COAT®

WhatWorks is a user-to-user program in which security managers who have implemented effective Internet security technologies tell why they deployed it, how it works, how it improves security, what problems they faced and what lessons they learned. Got a story of your own? A product you'd like to know about? Let us know.

www.sans.org/whatworks

ABOUT NETTECTS

Founded in 2011, NetTects LLC provides solutions and consulting in the computer security, networking, and technology fields. NetTects specialties include network security (IPS, firewalls, application firewalls, remote access, forward and reverse proxies), network identity management (DNS, IPAM, & DHCP), network infrastructure (routers, switches, network management, logging) & high availability (load balancing of servers, sites, WAN links. NetTects partners with vendors of leading solutions in these spaces, including Blue Coat, Imperva, Infoblox, Fortinet , Juniper, Nimble Storage, PulseSecure, Radware, and Trip Wire. A full range of solutions to complement these technologies from other vendors (remote management, power, etc) is also available.

NetTects team members have many years technical, sales, and service experience in the industry. This experience is efficiently utilized to ensure that NetTects clients get best of breed solutions coupled with professional services providing secure, resilient, and efficient network architectures and quality deployment and troubleshooting.

ABOUT THE USER

Michael Weinstein, CTO of NetTects has been with NetTects since its inception in 2011. At NetTects, Michael works daily with clients and leading technology vendors to develop, deploy, and tune security and networking solutions in a variety of small, medium, and large enterprise environments across many verticals. He has worked on networks and supported deployments internationally for clients in many diverse verticals, including financial, media, health care, and retail. With over 15 years' experience in the Value Added Reseller space (ten years as CTO of a Value Added Reseller prior to NetTects), and five years at a manufacturer of security and load balancing solutions, leaving with a Director level position, Michael brings advanced networking and security skills along with a highly valued perspective to clients that fosters long term, trusted relationships with those clients.

Having had training and/or completed formal certification programs from a number of vendors (including Juniper, Blue Coat, Radware, Cisco, Network Appliance, Infoblox, APC, Nimble Storage, and Gigamon), Michael assists clients not only with the deployment of NetTects' vendors's solutions, but also the integration of the existing environment with those solutions. His understanding of enterprise environments, networking, security, and availability enables clients to quickly and effectively deploy new technologies, resolve security concerns, and provide a stable network for application resiliency. Furthermore, Michael's experience and understanding of complex integrations has also lead clients to rely on him to assist in remediation of networking and security issues, including service outages, DDoS mitigation, and forensic investigations.

SUMMARY

A large global media company saw both an increase in targeted threats and an increase in encrypted traffic on its Internet-connected networks. A system integrator tasked with increasing their ability to inspect encrypted traffic selected the Blue Coat SSL Visibility Appliance.

Q Tell us about the company you work for and what role you played in the deployment of Blue Coat's products.

A I'm the CTO of NetTects. My responsibilities include designing, deploying, troubleshooting, and training clients on networking and security solutions. NetTects focuses on a small number of vendors that are specialized in specific solution sets. We offer security gateways, proxy, anti-malware, SSL/TLS inspection solutions from Blue Coat. Our clients are a large number of verticals, including retail, healthcare, financial services and media. They range in size from about 100 users to enterprises with over 10,000. The specific client that we worked for on this deployment is a large client in the media space – multiple offices, different sized offices, from small branches to large facilities, a couple of large facilities across the world.

Q What was the customer's problem that you were looking to solve?

A Many of our clients have deployed proxies that can terminate SSL and have some visibility there, but the problem with that is there's not a lot of visibility that gets extended to the common tools that are used, like IPS's, data leak prevention solutions, etc. What we needed to do was have a solution that could also audit the security policy and have visibility into that traffic, especially as the traffic volumes for TLS and SSL increase on the Internet. We also saw that there were some applications that ran inside TLS that weren't really "proxy-able." Things like online meetings that we might want to have some visibility into; but if we proxied them, it tended to break them. So, the problem was to enable inspecting TLS/SSL traffic without disrupting business critical applications.

Q So, they had the usual web security gateway, web proxy requirements for a standard user-to-web type web security, but they also wanted to feed decrypted SSL traffic to other inspection tools, things like IPS and so on?

A Yes. IPS, anti-malware, things that are typically sitting out of path; and decrypting out of path is more difficult in this day and age, especially for individual devices to do it. We needed a solution that could go ahead and decrypt that traffic and present a copy of not only the plain text traffic, but also the decrypted traffic, from a single point to these devices that gave us the visibility we needed, so that the different departments within the organization could get what they needed.

Q Was there an incident or an audit report that triggered needing to fill this gap or was it that the gap was recognized and you moved forward to fill it?

A Over time there have been incidents for which we used the Blue Coat solution. As far as investigating what users are doing on some specific site or what a user is doing on specific environments that we needed to get that visibility on. It's very common, at least for the clients that I work with, to go ahead and decrypt things like web mail so we can stop attachments that contain viruses from the Internet. However, to decrypt the Internet as a whole becomes a layer eight issue, and you have to talk to legal, HR, etc. If you can isolate that and present it to just a certain set of security tools with limited access to those tools for the highest level of security and auditing teams in the company, it's much easier and much more palatable to legal and HR than decrypting and logging everything on the proxy.

Q For those key reasons, were you able to convince management to obtain the budget to move forward?

A Yes. It came down to the fact that the tools that they were using could no longer see much of the traffic. So, the budgeting was really driven from the top down – what do we need to get this done so that these tools that we have in place can get this visibility back? Even though we're doing all the enforcement on the proxy, it's nice to have that second set of eyes, on other things that the proxy is not focused on and being able to decrypt that traffic.

Q Can you walk us through the process you used to look at possible solutions and how you ended up with Blue Coat?

A There were a number of solutions that we looked at, and it was very interesting going through the process because topology was a big driver and a big differentiator for a number of other solutions we looked at. Some of them were very large in scale, and they didn't scale well to smaller sites. We looked at what they could do, and also had to look at how they managed the security side of SSL. Since a lot of what happens is when you start decrypting SSL as a man in the middle, you're destroying all of that security that's built into the browser. We needed to make sure that we were able to enforce that same level of security, in that every time you get that Chrome update or IE update that it's also on this device. The CA lists had to be manageable. The keys had to be protected as well as what cipher suites could be used, etc. So, that was a big problem for us to solve. The other big one was we didn't want another HTTP proxy. A lot of the solutions on the market said, "Hey, we're basically an HTTPS reverse proxy," but we already had that, and we didn't need to have this man in the middle HTTP proxy. We wanted something that was protocol agnostic. As long as it was TLS, whatever went inside, we could decrypt and view what was inside. We didn't want to terminate that as an HTTP transaction, for example. We had to look at all of those factors to determine what we were going to do and how it was going to fit into the environment.

Q **What is the solution you chose?**

A After a lot of consideration and looking at those solutions, we looked at Blue Coat SSL Visibility Appliance as well, and it was an in-line device. That always has some unique challenges, but what it did do very well was terminate SSL effectively and transparently. As long as the client had the certificate authority installed that it was using, it would just pick up on the fact that there was an SSL hello from the client which was really, impressive. It didn't matter what the protocol was running inside TLS, it didn't care. It just copied it off. It was also a nice benefit that it copied all the other traffic it saw. If there was HTTP traffic, it would copy that also. It just didn't do anything with it from the process perspective which was nice, because it meant we didn't have to have a ton of interfaces and different places to feed the tools from.

They actually generate the private keys on the fly; so your private key isn't at risk with the next SSL vulnerability that comes out. That was a big benefit for us...

Once we deployed this at that choke point, it was able to feed the security devices which worked well for us. They also have the unique feature amongst some of the vendors where they don't use the private key of the CA certificate that's deployed for the spoofed server certificate – they only use it to sign the spoofed certificate. They actually generate the private keys on the fly; so your private key isn't at risk with the next SSL vulnerability that comes out. That was a big benefit for us because it's always a concern when the whole enterprise is dependent upon the certificates and keys that are on these boxes. A lot of the other solutions we looked at did not do that, so it was a big benefit. Also, the CA list is easily maintained on the box. If we wanted to add CAs or remove CAs that were valid, we could do so easily. It's an interesting security device in that it does have a policy, but that policy is more action-driven as far as decrypt or not decrypt. I can do some enforcement, but my main enforcement is still the rest of the network. This is more of an enabler of my other security devices. So, it was really impressive in that regard that it was built with that in mind.

The largest solution single device has 40 Gbps of packet processing capability with 9 Gbps of SSL inspection and decryption.

It also has the filtering capabilities, so, the whole Internet, as Blue Coat categorizes it, is on here. It's very easy for us to say, "Hey, don't decrypt healthcare traffic," as an example. We don't want to see someone going to their insurance company and doing things like that or making a doctor's appointment, not of interest to the security group. So, it made it really easy for us to do that as well.

Q **To be clear, you're still using a separate web proxy approach for those things and then, the in-line appliance is just being used for this level of inspection?**

A Correct. In theory, I could tell it to send a reset, but it wouldn't be very user friendly. There'd be no custom error message that says, "Organization has denied your access to this site. Contact support if you feel this is incorrect." You wouldn't get any of that because it's not an HTTP proxy like the proxies are, but it could send a reset. That's not what we were looking for because we had that layer of security, as you mentioned. We wanted something that would at least just allow us to get that visibility. The "allows and denies" were done elsewhere. That's not to say we might do things like certificate validation in an emergency. For example, "Hey, we want to deny this certificate enterprise wide, anything signed by it, or this CN." We could certainly do that there or on the proxy.

Q **What is the scale and the scope of this. Roughly how many appliances were deployed?**

A For my largest client, we deployed under 100. There are many that were globally deployed and still deploying. Some of the sites have lots of bandwidth – in excess of gigabytes of bandwidth – for Internet access that we had to consider as a solution, which was also nice about the Blue Coat solution. The largest solution in a single device has 40 Gbps of packet processing capability with 9 Gbps of SSL inspection and decryption. That was impressive as an in-line device. It worked out very well to be able to drop that in and just go from that perspective once we decided to deploy. The smaller offices have a smaller box that can be spec'd for 250 Mbps, 500 Mbps, etc. So, that was another big differentiator.

Q **Roughly, how many users are behind all these appliances?**

A In excess of 10,000 at our largest client.

Q **Are there policies by Active Directory groups in place regarding who can go to places other people can't?**

A I'm a traditional security guy. When I deploy proxies, I really like to authenticate users. I'm not a huge fan of doing reverse lookups into AD and saying, "Okay, that guy's got this IP. It must be Dave or Mike."

Q So, basically, the CEO's traffic is going to get treated like everybody else's.

A Absolutely. That's what you want in an organization. Exceptions should be by group not by individual.

Q For typical use, you mentioned the CA list you have on the proxy. Is it transparent to the users?

A It's transparent to the users as long as they have a sub CA certificate on these devices, issued by your corporate CA that everybody knows about already. Then, they are able to, on the fly, spoof the certificate and sign it and, as I mentioned, generate a private key, generate a certificate, sign it, and then issue it to the client along with their own sub CA as the intermediate certificate. So, it presents all of that. Users don't see a thing. It's good to go.

Q The traffic that's decrypted is simply passed through to other inspection or controls? You're not storing traffic?

A There's nothing stored on the devices. They want to know when something's stored that could possibly be sensitive, that it's only on one device. However, as far as whether it can pass the devices in line, the box does have that capability. It's used primarily to feed passive devices or promiscuous devices on the network. But, this could be used in that fashion as well for an in-line deployment.

Q Did you measure any additional latency this causes, or was it essentially put in a test mode that nobody noticed and away it went?

A We didn't take millisecond measurements of the deltas compared with going direct. It's a proxied environment. So, some of the things are being decrypted already. They might even be decrypted twice now. Once by the proxy and then once by this device because it's feeding different tools and different goals. It was not noticeable by us when we were testing. We took the whole IT department and put it on the proxy that had this in line and everything was decrypted. It's pretty interesting when you look at the pcaps when you're testing it off of the security devices.

Q Once you made the decision to go with Blue Coat, how long did it take to roll out.

A Once we configured the networking perspective at each facility and each type of topology and how it was going out, they went in relatively easily.

Q As it relates to topology, the inspection appliance is inside or outside the firewall?

A I don't like to put anything that's decrypting outside the firewall. In addition, you may want to have client IP visibility. So, in all the cases that I worked with it, we've always put it inside the firewall so that you can see the internal IP address in your logs.

Q Anytime something goes in-line, there are worries not just about latency but, also about variability, and is it the reason something bad happened in the network? What did you do to make sure in-line behaved well?

A We did a good bit of fail-over testing where we did upgrades on the boxes and rebooted them and pulled them in and out of line and things like that. At some of the more critical locations to waylay those fears, we actually used a visibility device. In this case it was a Gigamon that we put in place there so that we could toggle traffic. It also gives us an external health check for that device, which is nice, so that we know that it is healthy. And if it's not, it can take action and either bypass or just alert us. We did test the port, the fail-open capability. Unplug the box, traffic just goes right through it. So, that's a nice advantage. Obviously, any sessions that were terminated, they have to be restarted because those keys are gone. But, it worked fine. The long and short of it is we got a lot of great management out of it. And as far as latency, most of this was Internet traffic. So, any latency that it added was negligible. We didn't notice.

Q You mentioned tens of appliances. How are they managed? Do you touch each box to manage it? Is there a management server? How you do that?

A Blue Coat has a central management server so you can push policy devices, back them up and things like that. If you're building your polcies based upon the Blue Coat categories, those are automatically updated. For example, if I choose healthcare, Blue Coat's going to maintain that list and feed rules through what they call the Global Intelligence Network.

Q For the global network, can you pre-configure the box and ship it out and they install, or is it that you essentially have to be on the local network getting it to work right?

A I'm a big fan of console ports, so for most of my customers, I'll say to them "if you're going to ship it out and it's not preconfigured, just put a console server on it. We'll log in and get it up and running, and then plug in the network interface and will be good to go." They can also be pre-configured. Some of the devices have an on-box screen as well, so even a hands-on site could do it if we give them instructions, walk through and give it a base IP; plug in the management port for us. It's not my favorite method. I'd much rather have a console server that I can log everything and see what's going on; but, in a pinch, it works in an emergency.

Q **How long has it been operational?**

A We started the process about two years ago. So, we've been up and running for almost a year now.

Q **Where are you now? You went through the deployment and a year of operation. Any lessons learned? Things you know now you'd do differently that you could pass on?**

A I can tell you, I know more about SSL than I thought I knew, and I know how much about SSL I don't know. It's ever evolving, and it's obviously a very complex topic. A lot of really smart people put together how this is supposed to work, and even they missed a few things, which makes it always a challenge when the new vulnerabilities get rolled out at protocol level, things like, Heartbleed – there's been a year of these. And this device can help with that as well. So, that's nice, because I know they can automatically detect a Heartbleed attack and log it and stop it. Another benefit is that you can control cipher suites. Even just logging them is nice. I've also used the device to help validate other security solutions. For example, I happened to notice that one of the other security solutions we were using when it went through this box was logged as using a less than optimal cipher suite, so, I contacted that vendor and said, "Hey, you know, this is a security device. Why aren't we using high-end modern cipher suites in the communication with your cloud services?"

...this type of device, depending upon what type of vulnerability you encounter, can absolutely help because it's in position to do so. So, it's really nice.

I've used it to validate that security devices are not validating the CA certificate. There's been plenty of CVEs from vendors where they fail to validate a certificate. So, they're basically all subject to man-in-the-middle attacks. Well, that's what this box does. So, if I can break open a communication from device X going to that company's cloud system, I know that it's a problem, right? I want to know that it's validating. That it can't be intercepted. Or, if it's intercepted, it's by me when I deployed the certificate on it. It's been really good in that regard.

For me, as a VAR, when I evaluate new solutions and I pop them into my lab, I can now crack open any communications they're doing and see what they're vulnerable to, even just log the cipher suites if I'm not cracking them open - all transparently, it's been a real boon. It really does an amazing job of all that. It's pretty impressive.

Q **I think that's an interesting topic. I was actually going to bring up Heartbleed. What did it mean operationally when Heartbleed came out? What did it mean to the operation of the appliances?**

A Well, from this perspective, a lot of this stuff is what sites are the end users internally accessing? So, Heartbleed was a little bit less of a risk in that regard in that you count on the web servers/service providers to fix their servers. Obviously, we wanted to make sure the clients weren't vulnerable. But it's a tough thing to enforce. IPSs can definitely pick up that type of traffic. I helped write some signatures to detect it when it was being executed on some DDoS devices at a couple of clients. I know how it works and and I was amazed by it when I saw it and ran it against my own systems to see how I could extract information and see cookies and things like that that were supposed to be encrypted, dumping out of memory. But this type of device, depending upon what type of vulnerability you encounter, can absolutely help because it's in position to do so. So, it's really nice.

Q **Any features or requirements you either asked or hope to see come from Blue Coat?**

A One of things that I hope Blue Coat can take advantage of as the box grows – what's the next protocol vulnerability, and how can I use this box to address it? Log jam – if the browsers are denying that and this box passes on that same parameter so the browsers continue to deny, it will log that the cipher is being used, but the prime size is not logged. I'd like to see that as well.

There's a lot of things that'd be really great to get more granular with for troubleshooting, additions to some authentication protocols and things like that. But, otherwise, it's pretty well rounded, and it's done a great job. For me, as a VAR, when I evaluate new solutions and I pop them into my lab, I can now crack open any communications they're doing and see what they're vulnerable to, even to just log the cipher suites if I'm not cracking them open – all transparently, it's been a real boon. It really does an amazing job of all that. It's pretty impressive.

Q Since you said you rolled this out globally, were there issues in certain countries where you couldn't inspect or were there different privacy rules and employee union rules about what traffic can be inspected? Did you run into that?

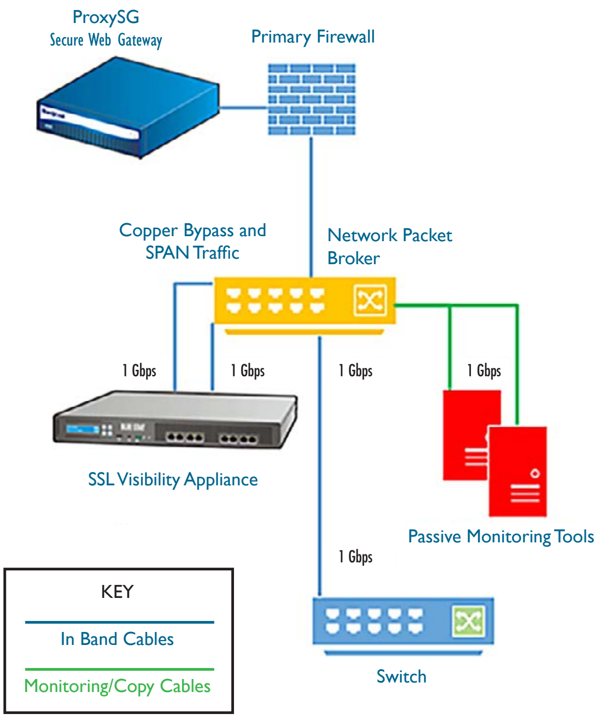
A Yes. I run into that, not only with this, but with other solutions and other clients as well. I've worked in the past with companies that are not U.S. based, and there are rules for filtering, even for what they can block are different than what we would consider a block. A lot of what the acceptable-use policies you have in the U.S. are, "Hey, it's our network. Anything you can do that's beyond work is by our good graces." But, that works different over in Europe. I don't understand the full ins-and-outs of it, but it was definitely what I refer to as "layer-eight issues." My job is to enforce what you tell me to enforce and make recommendations to protect the enterprise. And then, there are countries that this type of solution is tough to even get into. Countries have their own specific laws about encryption and things of that nature, so there are definitely some challenges there. With most of my clients being U.S. based, it's pretty straightforward. If we're looking to protect the enterprise, it's the enterprise network. There's an expectation of privacy from the perspective that information will not be used for anything that it shouldn't be, but it doesn't mean we're not going crack open the web mail to make sure you're not downloading something malicious whether you intended to or not as an end user.

Q Any additional comments?

A This is really an interesting space to be in and what you can learn in it is tremendous if you take the time.

SANS bottom line on the Blue Coat SSL Visibility Appliance:

- Legitimate business use of encryption is increasing due to growing Cloud, Mobile and web applications, making it harder to detect potential threats.
- Minimizing network disruption requires any encrypted traffic inspection solution to be a true network device.
- To effectively inspect SSL/TLS traffic, inspection solutions must transparently handle ceritificates and related issues.
- SSL/TLS inspection must be supported on all TCP ports, not just HTTP/HTTPS ports, for both inbound and outbound traffic.
- Integrating with Web Security Gateway policies simplifies development and deployment of encrypted traffic inspection policies.


ProxySG
Secure Web Gateway
Primary Firewall
Copper Bypass and SPAN Traffic
Network Packet Broker
1 Gbps
1 Gbps
1 Gbps
1 Gbps
SSL Visibility Appliance
Passive Monitoring Tools
1 Gbps
KEY
In Band Cables
Monitoring/Copy Cables
Switch