Global Information Assurance Certification Paper

Secure Web Surfing; good or bad?
Michael C. Wisniewski
December 27, 2001
SANS Security Essentials GSEC Practical Version 1.3

Summary

This paper will cover secure web surfing through proxy or anonymous servers. This topic will probably become more popular in the future once people start hearing about it. This could be a problem in businesses where they monitor network traffic. This paper will cover what secure web surfing means, list a few examples, and how companies can detect if this it being used.

What is Secured Web Surfing?

There are a number of companies available that offer "secured web surfing". What this means is that there is a secure link between you and the company where you subscribe to the service. Then from the company where you subscribed the service from to the Internet, it hides all your information (for example, IP address and which URL's you visit).

There are multiple sites offering this service. Some sites are free whereas others you have to pay for. The free sites offer basic web surfing usage, whereas the more you pay, the easier and more secure it is to surf. The free sites offer a URL you originally go to. Once you are there, you are able to type in the web sites you would like to visit and your IP address is hidden; it will prevent tracking from web sites, hackers, and other prying eyes, and removes privacy threats from pages that you view. As you purchase different packages, you can get basic web browsing and encryption all the way up to a secure tunnel between your machine and the anonymous service that you are using.

How is this a good thing?

For the normal home user, they might be thinking that this is a great service! As we know with the advent of broadband, this can be a very useful service. If your neighborhood has cable modem access, your neighbor can sniff the network traffic and see which web sites you go to and get information you may not want the world to know. Digital Subscriber Lines (DSL) are more secure whereas it is not shared bandwidth. This means that your neighbor can not plug a sniffer in and see what you are doing on the internet. Dial-up is similar to DSL where it is a little more secure than cable modems, but there is still a chance that your ISP can monitor your traffic.

Since you now know that others can view your network traffic, there are many paranoid users that are out there that do not want this! If this is the case, all you have to do is install a client on your machine (or browse to a certain web page) and then your neighbors or ISP does not see where you are going since it is encrypted. In addition to that, all the destination web sites see are you coming from the anonymous service.

Some more benefits to subscribing to a service like this would be a reduction in viruses. Many of these sites claim that they neutralize hackers from running scripts and having others place files

on your computer. A lot of viruses today come from just browsing web pages. Usually a web page will contain a script (Java, JavaScript, ActiveX, and VBScript) and will execute this script without the user knowing. On the other hand, if you run up-to-date anti-viral software on your machine, it should detect these harmful scripts. By using services like this, it will prevent these viruses from running.

Another positive aspect that can be viewed is that it removes your IP address from destination web pages, along with neutralizing cookies. A lot of sites track where users come from by IP address and record information about this, without telling the user. The IP address is similar to your house address, and many people subscribe to unlisted phone service. One can assume that since this unlisted service by the phone company is so popular, people would like their IP's hidden as well. In addition to blocking your IP address, it will also manage your cookies. A lot of the programs will not stop cookies from being sent to your computer, but will just keep track of them for the different web sites that are viewed. Once you either end your session or change which web site you are viewing, it will erase or move the cookie so they can not be read by other sites. This is also a great thing because a lot of information can get stored in cookies, such as user names, passwords, addresses, phone numbers, etc.

How is this a bad thing?

Over all the positives that were just listed, this can also be a bad or abused service. There are many hackers, or kiddy-hackers, out there that want to become hidden and not be tracked down. If one of these users compromises a machine, the best and easiest way to track them down is by IP address. If the user hides their IP address, how can one track them down successfully?

This service can also be abused by employees at a company. In this day and age of efficiency, employers are starting to examine e-mails and web traffic of employees to see what they do all day. I do not think there is somebody out there that uses the company's internet strictly for work use. I am sure that people go to the Chicago Sun-Times, CNN, or the Weather Channel home pages at least once during working hours. However, companies are starting to track which web sites people go to and who goes to them, and if the employee is abusing their internet privileges. If the employee finds a service that encrypts all web traffic, then the company can not track where the employee is going.

For example, Joe goes out to www.weather.com twenty times a day to see what the weather is going to be like. Fred is viewing web pages through a secured browsing service and he visits www.weather.com thirty times a day, www.cnn.com fifteen times a day, and www.msn.com ten times a day. When Fred is done viewing the web pages, he disconnects from this secured browsing service, it stops encrypting his traffic and URL's, erases all his cookies, and deletes the cache. Now the cyber-security manager, Tom, sees Joe going out to these pages and sees this as an abuse of service. Joe will get fired while the secured surfer Fred won't. Even though this is not right, companies can have a hard time of tracking this and it does happen.

Another bad aspect of the above example can be found in a more realistic example. At some companies, viewing of pornographic sites can be founds for dismissal. One way to track this and catch users in the act is to sniff the network traffic. By encrypting the URL's and traffic, the

cyber-security technicians can not see what and when the user is doing this, making it impossible for them to be caught.

Finally, it may not be a problem now but could be in the future. By using a secured tunneling service, it bypasses the company firewalls and network devices that are placed there to protect the network. If the user is running a web server on a desktop, it can violate a cyber-security policy. If the user is running a web server with a secured tunnel on their desktop, the security technicians may never know about this since all traffic is encrypted. Although these services say they protect the user from viruses, one may get through and infect the web server that is connected to the secured tunnel. Once this machine is infected, it could set off an attack from inside the firewall and infect other machines on the internal network.

This could happen with a lot of other services, and this is why many companies choose to block outgoing ports and sites at the firewall. A few would be Gnutella, Napster, WinMX, and Morpheus. These programs allow file sharing and can work through firewalls. If a hacker finds a vulnerability in the program, it may give them access to the whole system running this. Once this is established, files might be placed and run from the machine running this service. This is why many companies choose to block programs and well known ports that these programs use.

How does this work?

You may be asking yourself how this technology works. There are a few different methods that can be used. The following paragraphs will go over the different methods and briefly describe them. One of the most popular services is called the Anonymizer. It can be found at http://www.anonymizer.com and will be used in this example.

The first and most basic method is a user stumbles upon a web site that they feel insecure about. They might not want the destination site to find information out about them or track them down. You can type in an address on the main page and then it will take you off and load the destination address web site. This will hide your IP information and it will not tell the destination web site what the source IP is. The destination IP will receive an anonymizer.com registered address. While this can be useful, it displays an annoying pop-up banner and an advertisement. On the other hand, it's free.

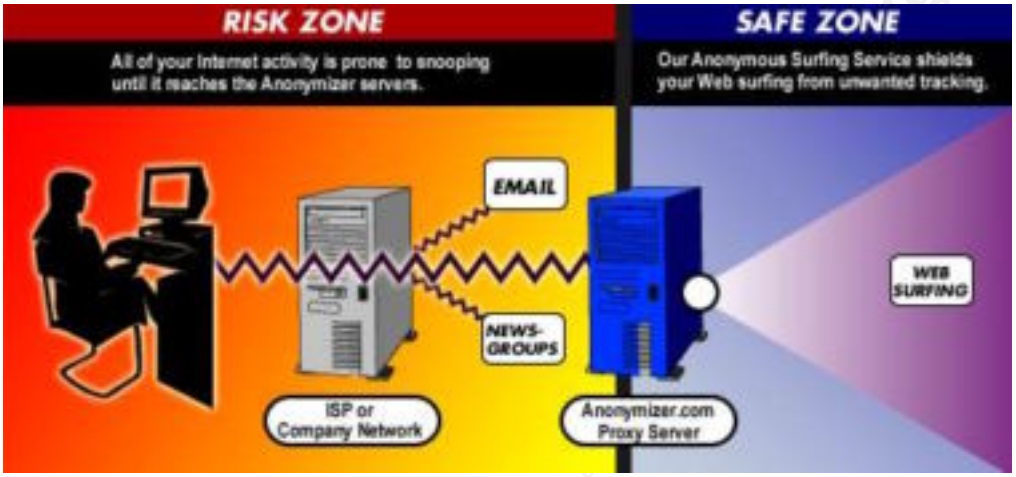
The next service step up from that is anonymous web surfing. In addition to the basic free service, it will also give you URL encryption, ad filtering, secure HTTP, and other features. This middle-weight subscription will give you enough power to browse the web "without your employers or ISP's seeing what you do."[1]

Then finally, the best package is called the "Anonymizer Secure Tunneling" package. This package uses SSH to encrypt traffic between the host computer and the Anonymizer's servers. In addition to the general subscription, you would need to purchase an SSH program, such as F-Secure's SSH Client.

[1] From the Anonymizer web site at http://www.anonymizer.com/services/paidSurf.shtml

Once you are connected to the Anonymizer servers, all your traffic from the host computer and the Anonymizer server will be encrypted. This also allows ISP's and employers not to sniff data and track where you are going. The below is a picture from Anonymizer that visually explains how this works.

Without SSH enabled and using the regular Anonymizer service…



With SSH enabled and using the Anonymizer service…

Hopefully with the above pictures, you can get a better view of what is actually going on. As you can see, the scale can fall both ways. One way this can be a really good thing for a cable modem user, but on the other hand, if you are a cyber security manager at a company, this can be an extremely scary situation.

How well DOES this work?

Now since you have been loaded with the knowledge, you may be asking yourself how well this technology works, if it even works at all. There is another program called Freedom //websecure[2] that I have used for this demonstration. I have taken the Freedom //websecure program (using the 15 day free trial) and installed it onto a test computer. After testing it for awhile and becoming familiar with it, I used windump 3.5 to capture traffic on where the web browser was going to. In the following captures, I have taken ten lines from the windump capture file and truncated the lines for easier reading. The following computer named "computer.dsl.att.net" is the machine opening the Internet Explorer web browser and visiting http://www.yahoo.com web site. This capture was also done as a normal user **without** using the Freedom //websecure program.

```
14:50:58.430755 computer.dsl.att.net.2837 > w8.snv.yahoo.com.80: S 2756567730:2756567730(0) win 65280 <mss
14:50:58.506343 w8.snv.yahoo.com.80 > computer.dsl.att.net.2837: S 1772405283:1772405283(0) ack 2756567731
14:50:58.506406 computer.dsl.att.net.2837 > w8.snv.yahoo.com.80: . ack 1 win 65280 (DF)
14:50:58.506821 computer.dsl.att.net.2837 > w8.snv.yahoo.com.80: P 1:335(334) ack 1 win 65280 (DF)
14:50:58.704833 w8.snv.yahoo.com.80 > computer.dsl.att.net.2837: . 1:1361(1360) ack 335 win 17680 (DF)
14:50:58.776718 w8.snv.yahoo.com.80 > computer.dsl.att.net.2837: . 1361:2721(1360) ack 335 win 17680 (DF)
14:50:58.776779 computer.dsl.att.net.2837 > w8.snv.yahoo.com.80: . ack 2721 win 65280 (DF)
14:50:58.847185 w8.snv.yahoo.com.80 > computer.dsl.att.net.2837: . 2721:4081(1360) ack 335 win 17680 (DF)
14:50:58.847275 computer.dsl.att.net.2837 > w8.snv.yahoo.com.80: . ack 4081 win 65280 (DF)
14:50:58.914988 w8.snv.yahoo.com.80 > computer.dsl.att.net.2837: . 4081:5441(1360) ack 335 win 17680 (DF)
```

The next ten lines will show the windump capture of the "computer.dsl.att.net" machine opening up the http://www.yahoo.com web site. In addition to that, the Freedom //websecure program **was** enabled.

```
14:52:02.783668 computer.dsl.att.net.2865 > ny-1.proxy.websecure.freedom.net.443: S 2774077398:2774077398(0)
14:52:02.826630 ny-1.proxy.websecure.freedom.net.443 > computer.dsl.att.net.2865: S 3001292010:3001292010(0)
14:52:02.826703 computer.dsl.att.net.2865 > ny-1.proxy.websecure.freedom.net.443: . ack 1 win 65280 (DF)
14:52:02.827528 computer.dsl.att.net.2865 > ny-1.proxy.websecure.freedom.net.443: P 1:79(78) ack 1 win 65280 (
14:52:02.884045 ny-1.proxy.websecure.freedom.net.443 > computer.dsl.att.net.2865: . ack 79 win 5840 (DF)
14:52:02.945203 ny-1.proxy.websecure.freedom.net.443 > computer.dsl.att.net.2865: P 1:1025(1024) ack 79 win 58
14:52:03.018373 ny-1.proxy.websecure.freedom.net.443 > computer.dsl.att.net.2865: . 1025:2385(1360) ack 79 win
14:52:03.018443 computer.dsl.att.net.2865 > ny-1.proxy.websecure.freedom.net.443: . ack 2385 win 65280 (DF)
14:52:03.067936 ny-1.proxy.websecure.freedom.net.443 > computer.dsl.att.net.2865: P 2385:2530(145) ack 79 win
```

Again, some of the above text has been truncated in order to make reading easier. The main point that I wanted to make here is to prove to the reader that this "secured web surfing" does work and can become a problem, or a benefit, depending on the audience. The person doing the surfing will be grinning right now and probably can't wait to get their hands on this. On the other hand, the security specialist's eyes are popping out over the above data and what it proves.

For those who do not understand the capture, here is a rundown of what it shows. The first capture we will examine is the one that is not using the secured web service. The first column (14:50: xxxxx) is the time that the packet was captured. The column shows the source followed by a period and then the port number that was used, which is 2837. Then comes a ">" sign followed by the destination address followed by a period and then the destination port, which is 80. The rest of the information is not important in this demonstration.

[2] http://www.freedom.net/

What the first capture shows us is that the machine named "computer.dsl.att.net" has gone to the web page of w8.snv.yahoo.com. We know this because the source address uses a high port number and the destination address uses port 80, which is regular unencrypted web traffic. As you can see, there are multiple packets exchanged between the two addresses, which are normal.

The second capture's syntax is the same as the first capture. What should be noted is that as you can see, the first line shows that computer.dsl.att.net uses a similar high port number as the first one. But instead of w8.snv.yahoo.com on port 80, it passes it thru ny-1.proxy.websecure.freedom.net. After that, you do not know which web page was visited, even though it was the same www.yahoo.com address that was typed into the browser. What is even more interesting is that even though the little "lock" was not displayed in the browser window, and the web site entered was not showed as https://www.yahoo.com, the destination port number is 443. If you have any experience with port numbers, you know that 443 is https, or the hypertext transfer protocol using the secure sockets layer. In comparison, many e-commerce web sites (http://www.amazon.com, http://www.cdnow.com, etc) use the https in order to encrypt information such as credit card numbers, names, and addresses. Since all of this information is going across port 443 and is being encrypted, a network sniffer can not be used to see which web sites the user is going to.

Some of you may be sitting there thinking "Oh well if I view the packet I can get more information out about it". Unfortunately, you can not. Windump was run with the –vvv –x –X switches and even with viewing the packets' data, you can not tell which web page a user is going to. Everything is encrypted.

What about non-web program?

A lot of people use instant messaging in order to keep them in touch with the outside world. This could be another issue where a user would like to encrypt the data and would like more information about this. Unfortunately, a lot of the services that were examined did not mention about other programs that are running and were vague in their descriptions. One would assume that if a "secured tunnel" was in place on a machine to the anonymous server, it would encrypt all the data going across and not web traffic. Although in order to receive this "secure tunnel" you would have to purchase the package (or service) that is a step up from the normal browsing package.

On the anonymizer.com web page, there is support on how to use mIRC with the anonymizer account. Since this can be done, one would assume you could setup America Online's Instant Messaging service, Yahoo's Instant Messaging service, or even ICQ and encrypt the messages that flow across those programs. The best bet is to check with the company before you purchase the package.

What can be done to detect this activity?

Unfortunately, there is no easy way to detect and stop this if you are the cyber security manager at a company. Unfortunately it does not use a specific port that you can block at the firewall, and there are so many different companies that are out that it is hard to block all of them. What can

be done though is identify as many different anonymous web browsing companies and block their web pages from being viewed from work.

You can also write a cyber security policy to discourage employees from using software like this. In today's world, it is becoming a necessity to have cyber security policies, and to list what software can and can not be run on the workstations. Even though you may not be able to stop users from visiting and using this software, the managers may be able to severely punish them if software is found on a machine.

The last way to detect this would be education. Since every company has computer technicians that go around and fix common problems with Microsoft products, you can also ask them to keep their eyes open for software such as this. I have seen time after time where a computer technician goes to a desktop to fix a simple problem. While fixing the computer, the tech comes across files of an unpleasant nature. The computer tech turns the user in and before you know it, the user is out the door for doing activity like this at work. The same can be done with these anonymous web browsing services. If a user does have this software installed, a warning can be issued and follow-ups can be done. Every company handles this differently, and it is up to them to decide.

What about web servers!

We don't want to forget about those evil people that compromise web servers, do we? Since the source IP is hidden with the anonymous proxy server's IP, the web page logs on the web server will show the IP address of the proxy server. Now again, this depends on which audience this is being presented to. On the one side you can have the hackers and paranoid people that want their information hidden. They are sitting there right now and can not wait to get their hands on some of this stuff. On the other side, you have the computer security technicians that are getting headaches just thinking about this.

What can be done to protect web servers from this "anonymous" IP traffic is just simply ban the IP's either at the web server itself or at the firewall. This may be hard to do since there are so many companies that offer this anonymous web surfing service. What the administrator can do is go through all the logs on a daily basis and see where traffic is coming from. If a site is found with repeated hits from one of these sites, further investigation is needed to see what kind of site it is and if it should be blocked or not. After all, the administrators should be going through the logs of the web server on a daily basis! We all do that, right?

How can others benefit from this?

One of the main purposes of this service is to hide your identity from the others. This might be your employer, your ISP, your neighbors, or maybe even the government. Believe it or not, a lot of government agencies also use this service! In this day and age of the Internet, there are government institutes that use software to hide their identity. A few examples could be a sheriff or FBI agent trying to set a sting up. The sheriff or FBI agent usually poses as a minor, and lures an adult into meeting them. The sheriff or FBI agent does not want to make it obvious that they

are from there (IE: xxx.fbi.gov) so they want to hide their identity so it appears as if they are from (xxx.anonymous.com) or elsewhere.

Another use would be for the above agencies to setup different stings with web sites. If a site is found that is questionable, the administrator might wonder and shut down the site if addresses have been coming from a government agency. By using an anonymous service, the web administrator does not see anything out of the ordinary and will eventually get caught.

How confidential IS this anyways?

You might be wondering if after all this and proving that it passes information over port 443 (HTTPS) that this thing is as secure as Fort Knox; there are ways to show who you are. When you sign up for one of these services you agree to a license agreement. Inside of this license agreement lists a number of things. One of them being the user will comply with export controls and a whole list of what you can't use it for. The list includes hacking, defamation, fraud, intellectual property and proprietary rights violations, harassment, threats, abuse, false pretenses, and disruptive activities.[3] If you examine the web page further, you will usually find a Privacy Statement. This explains that even though IP's and all the information is hidden, it is recorded on a server and can be accessed by the company's personnel. For example, if Bob uses an anonymous secured web service, hacks into a system or defaces a web page, the company or investigating agency would be able to view the logs on the defaced web page and see where this user came from. After that information is collected, they should be able to call the anonymous secured web service company up and get more information on who this user is and where this user can be found. In the end, it is not 100% secured browsing, but it's pretty close to it.

I run a company and like to protect the computers but don't want to use a service

Say you are a manager or CEO of a company and would like the fact that this service decreases virus infections, hides IP addresses, and neutralizes cookies and active content, but you don't want to be scared that users will do mischievous acts. You may be wondering what you can do. To answer that question, setup a proxy server! There is a product that is available from Trend Antivirus called VirusWall.[4] What this product does is provides virus protection, blocks dangerous Java and ActiveX codes, and acts as a proxy server. This is an excellent product that can be used as an option of going through an anonymous web browsing service. In addition to that, the administrators can track where the users are going more easily because the traffic is not encrypted from the workstation to the proxy server. There are other companies besides Trend that are out there that have products similar to VirusWall, although I am most familiar with it and that is why I chose it.

Is this service right for me?

After reading this whole paper, you may be wondering if you should subscribe to a service such as Anonymizer or Zero-knowledge. A few things to take into consideration are where you are browsing from and why are you using this. If you are using this service to browse web pages at

[3] http://www.freedom.net/trial.html?product=websecure
[4] http://www.antivirus.com/products/isvw/

work, it may just get you into more trouble than you would be if you weren't using a service such as the above.

On the other hand, if you are a home user and have a cable modem. I think it is well known that neighbors can sniff network data and find valuable information about the web sites you are visiting and what you are doing. By using a service such as the ones listed above, it will encrypt all the data from your computer, making it impossible for your neighbor to see what you are doing. This is the reason why companies have emerged offering this protection.

Conclusion

In conclusion, secured surfing is out there and people are using it. I can only imagine companies that offer this growing and this becoming more popular in the future. Even though it has some advantages, it has more disadvantages.

For example, think of a scenario where you do not want to be spotted. If you go out in public wearing bright orange colored clothes, some gigantic hairdo, or wearing a really big hat, you will stick out like a sore thumb. If you wear clothes like everybody else is wearing, or if you try to fit into the society or culture, you will blend in like everybody is and become hidden. Now think about this in the cyber-security arena. Using an anonymous IP address from anonymous.com and some IP address from dsl.att.net, which one is easier to stick out like a sore thumb? The one from anonymous.com!

My advice is to not use one of these services unless you have a specific need to. After all, if you are using a service to disguise your IP information and encrypt your traffic, what are you hiding?

Bibliography

Freedom //websecure Web site, "Protect your identity on the internet with Freedom internet privacy and security software", http://www.freedom.net/products/websecure/?product=websecure (December 27, 2001)

Zero-Knowledge Home Page, "Zero-Knowledge Systems." http://www.zeroknowledge.com/ (December 27, 2001)

Anonymizer Home Page, "Anonymizer.com – Online Privacy Services." http://www.anonymizer.com (December 27, 2001)

iNetPrivacy Software Home Page, "Anonymity 4 Proxy." http://www.inetprivacy.com/welcome.htm (December 27, 2001)

Perera, Rick, "Consumers Ask for Return of SafeWeb Service." http://www.pcworld.com/news/article/0,aid,75063,00.asp (December 11, 2001)

Mainelli, Tom, "Anonymous Browsing Gets Easier." http://www.pcworld.com/news/article/0,aid,57344,00.asp (August 7, 2001)

Trend Antivirus Home Page, "Trend Micro InterScan VirusWall." http://www.antivirus.com/products/isvw/ (December 27, 2001)

Jacobson, Van; Craig, Leres; McCanne, Steven, Lawrence Berkely National Laboratory, "WinDump: tcpdump for Windows." http://netgroup-mirror.ethereal.com/windump/docs/manual.htm (March 26, 2001)