Surfing the Web Anonymously -
The Good and Evil of the Anonymizer

GIAC (GSEC) Gold Certification

Author: Peter Chow, chow_pete@yahoo.com
Advisor: Hamed Khiabani

Accepted: July 9, 2012

Abstract
Companies of all sizes spend large amounts of time, resources, and money to ensure that their network resources and Internet connections are not being misused. They hire the best Information Technology professionals, however, even the most technically challenged end user, with very little technical skills can find creative ways to circumvent firewall rules and bypass blocked websites. This paper will describe how an anonymizer or an anonymous proxy can bypass firewall rules and weaken the ability to enforce Confidentiality, Integrity, and Availability (CIA triad) in a network infrastructure. On the other hand, an anonymizer can be used for good, and is a useful way to hide IP addresses to surf the web anonymously.
1. Introduction

1.1. The Dilemma

Companies of all sizes spend large amounts of time, resources, and money to ensure that their network resources and Internet connections are not being misused. They hire the best Information Technology professionals, however, even the most technically challenged end user, with very little technical skills can find creative ways to circumvent firewall rules and bypass blocked websites. This paper will describe how an anonymizer or an anonymous proxy can bypass firewall rules and weaken the ability to enforce Confidentiality, Integrity, and Availability (CIA triad) in a network infrastructure. On the other hand, an anonymizer can be used for good, and is a useful way to hide IP addresses to surf the web anonymously.

1.2. Background Information

Anonymizers (anonymous proxy) are products and services that can be used for both good and malicious acts. They can provide users with Internet privacy to surf the web anonymously, by masquerading the person’s real Internet Protocol (IP) address and substituting it with another IP address. Anonymizer’s tools can also bypass security filters set by firewall rules (i.e. Access Control Lists) and access unauthorized websites or transfer information without corporate consent and thereby reduce the CIA model’s effectiveness.

All a user needs to do is install a proxy application and configure the web browser to point to a proxy website. Thereafter, when accessing websites, the computer will connect to the proxy server, circumvent the firewall ACL rules, and retrieve blocked websites.

In 1997, while studying for his Ph.d in Astrophysics at the University of California, San Diego, Lance Cottrell created the first anonymizer which was Anonymizer.com. Cottrell is an advocate for privacy and established the Kosovo Privacy Project which enabled users to use anonymizer services to report on the 1999 Kosovo war zone without discovery or penalties (Cottrell, 2011).

Peter Chow, chow_pete@yahoo.com
As the Internet continues to grow in popularity, more users are going to the web as their primary source of information. This information includes communication like email, chat, instant messaging (IM), and social networking sites like Facebook and Twitter. Ecommerce and online banking are other areas in which the Internet has influenced the way users are doing business and managing their personal information. Many websites today collect personal information about how users are surfing their websites. They gather information on just about everything, from the surfer’s IP address to how many times they visited a certain website. Just about every click of the mouse on a website can gather valuable and marketable information that can be sold to interested companies. Many people are now more aware of this and are learning about how their information is gathered, stored on internet cookies and then sent to marketing and advertising companies like DoubleClick and other adbot affiliates. Cautious users are now turning to anonymizer software and services to maintain their privacy and to masquerade their true location, IP address. Another reason for masking one’s IP address is that it adds a layer of security from malicious attackers while surfing on a public network. However, a side affect of using an anonymizer, creative users have found out, is that anonymizers have been found useful in circumventing corporate firewalls and accessing websites that should have been blocked. Figure 1 illustrates when firewall rules are applied and the intended website is blocked.

![Figure 1: Warning Message](image)

Peter Chow, chow_pete@yahoo.com
Surfing the Web Anonymously – The Good and Evil of the Anonymizer

Figure 2 illustrates how the firewall rules are circumvented by the use of an anonymizer.

2. How It Works

2.1. Example of an Anonymizer

In a typical network, access by workstation is connected to a switch and then on to a router that may have a firewall or proxy server to prevent unauthorized connections. Figure 3 is an example of a workstation opening a web browser to www.youtube.com URL, being inspected by the firewall and allowed passage thru based on its access control list or rule sets.

![Diagram of firewall and anonymizer](image_url)

Figure 2: Bypassing ACL’s rules

Figure 3: Permitted websites

Peter Chow, chow_pete@yahoo.com

© 2012 The SANS Institute

Author retains full rights.
Figure 4 illustrates when the Firewall access control list is set to deny passage to the www.youtube.com website. It will block the connection and prevent access and return an access blocked message to the workstation’s web browser.

Figure 4: Blocked website

Figure 5 illustrates when the workstation directs its web browser to an Internet anonymizer (proxy server) to connect to the www.youtube.com website. It then bypasses the Firewall access control list and circumvents the rules that prevent it from connecting. How this works is when the computer is set up with an anonymizer it will establish a secure connection allowing access to surf websites normally blocked by the firewall, and as a result unauthorized access is undetected.

Figure 5: Access a denied website via anonymizer

Peter Chow, chow_pete@yahoo.com
2.2. **How to do it**

There are many types of anonymizer applications and associated services. Some are free of charge like proxify.com and others are commercial grade, such as JonDonym and have a monthly subscription price based on the volume of data used. In this example, a free version of the JonDonym Anonymous Proxy Server called (JAP) AN.ON has been selected because it is free.

(JAP) AN.ON is a research project and is free of charge. This application is written in the Java programming language and can be installed on a number of different operating systems, which include Windows, Macintosh, OS/2, Linux/UNIX and other types of operating systems. JAP allows surfing the Internet anonymously and undetected by connecting to the JAP proxy servers located all over the world (JAP, 2012). JAP can be downloaded at [http://anon.inf.tu-dresden.de/index_en.html](http://anon.inf.tu-dresden.de/index_en.html) (see Appendix A). After downloading JAP, follow the installation process (see Appendix B).

2.3. **Blocked websites**

Corporations configure their firewall rules (ACL’s) based on a number of factors which include preventing malicious attacks to their network resources. Another factor is to prevent internal users from accessing unacceptable or harmful websites.

In this example, the corporate firewall is set to prevent access to the website [http://www.anonymizer.com](http://www.anonymizer.com). When a web browser tries to open this website, a warning message is displayed indicating “Security risk blocked for your protection” and the website is not accessible, Figure 6.

![Figure 6: Blocked website’s warning message from Firewall](image-url)
Check your IP address setting by opening Windows Internet Explorer web browser and entering www.whatismyip.com in the address box. It indicates that Your IP address location is 45.112.164.5 (made up IP address for security purposes), Figure 7 (Whatismyip.com, 2012).

2.4. **Launching JAP**

To masquerade your IP address, start and configure the JAP application.

Step 1: Click on the JAP application icon to launch the program, Figure 8.

![JAP application icon](image)

Figure 8: Launching JAP application

Step 2: Turn on JAP Anonymity service by clicking on the “On” radio button, Figure 9.

![JAP application interface](image)

Figure 9: JAP application interface

Peter Chow, chow_pete@yahoo.com
Surfing the Web Anonymously – The Good and Evil of the Anonymizer

Step 3: Select the location and service by clicking the down-arrow tab and selecting the “FreeBee – Bolzano”, Figure 10.

Step 4: Configure Windows Internet Explorer web browser to use proxy. Open Internet Explorer and click “Tools” then “Internet Options” Figure 11.

Step 5: In Internet Options, click on “Connections” and then click on the “LAN settings” tab, Figure 12.

Peter Chow, chow_pete@yahoo.com
Step 6: In the Proxy server box, check the “Use a proxy server for your LAN”. Enter “localhost” in the Address box and “4001” in the Port box. Click the “OK” button to finish and close “Internet Options” Figure 13.

![Figure 13: Entering Proxy Server IP address and Port number](image)

**Note:** Uncheck when not using Proxy server, otherwise normal connections may not work.

Step 7: Testing Proxy settings, open Internet Explorer and enter **www.whatismyip.com** in the address box again. Now your IP Address is 178.33.255.188 (real IP address assigned by the proxy) which is coming from France and not your real assigned IP Address of 45.112.164.5 which is located in the United States, Figure 14 (Whatismyip.com, 2012).

![Figure 14: Checking IP address with Proxy services enabled](image)

**Peter Chow, chow_pete@yahoo.com**
2.5. **Accessing a blocked website**

Now, in Internet Explorer enter [http://www.anonymizer.com](http://www.anonymizer.com) URL in the address box. Now the Security risk warning message is not displayed and the website is accessible and not blocked by the firewall, Figure 15 (Anonymizer.com, 2012).

![Figure 15: Accessing a blocked website with Proxy services](image)

3. **Anonymizers – The Good, the bad and the ugly**

3.1. **The Good**

There are many benefits that would cause common and professional users to use an anonymizer. For the common user, it allows them to hide their true IP Address and have the capability to masquerade their actual location while surfing the Internet, allowing them to keep their privacy. Professional users working offsite or on the road would want to use an anonymizer to enhance their security and confidentiality. While connected to an unsecured LAN or Wireless LAN that is connected to the public Internet, an anonymizer adds a level of encryption and stealth connection. Couple this with a VPN connection back to a corporate network to add another layer of security on top.

Another benefit both common users and professional users can all utilize with the use of an anonymizer is that while overseas in countries where there are limitations, restrictions, and censorship that prevents access to websites that are blocked by the government or by local authorities, an anonymizer can get around this. As addressed by Carolyn Pearson in her SANS GIAC Security Essentials Certification (GSEC), Practical

Peter Chow, chow_pete@yahoo.com
Assignment, title The “Great Firewall” of China, A Real National Strategy to Secure Cyberspace? “Sites such as Anonymizer.com, known as “circumventors,” allow users to access sites blocked by their governments via a proxy server.” (Pearson, 2004).

3.2. The Bad

Anonymizers and Proxy servers are used to circumvent Acceptable Usage Policies (AUP) by crafty users who bypass the firewall rules set by administrators. It creates a challenging endeavor for those who are tasked to enforce company policies and to mitigate the risks of violating Confidentiality, Integrity, and Availability in a network infrastructure. Enforcers need to restrict the users from having administrative rights on company owned assets, not allow installation, modification, and configuration capabilities on company systems, and prevent usage with anonymizers. Since companies have no control over personally owned computers, the AUP should include limiting the use of personally owned computers connecting to the corporate network.

3.3. The Ugly

Hackers and crackers have been reaping personal glory by using anonymizers and proxy servers. All the good in an anonymizer is turned to evil when it is being misused. Bypassing, circumventing, hiding, masquerading, and many other benefits are a powerful tool for those who wish to misuse this technology. The list is too long; therefore it will not be addressed in this paper.

4. Countermeasures

The first line of defense in combating anonymizers is awareness. Having knowledge and understanding of these applications and/or services is the beginning of creating lines of defense. This paper addressed how simple it was to use and how easy it was to breach the network’s integrity and circumvent the network firewall’s ACL, allowing websites that were not authorized or approved to be accessed. While there are no solutions in preventing an attacker from outside the network from using an anonymizer, there are solutions from within the network where legitimate users can be prevented from using anonymizers. While there can be many possible solutions, it

Peter Chow, chow_pete@yahoo.com
should start with having a well defined and enforceable Security Policy and Acceptable Usage Policy. It may also include limiting users from installing applications on their systems, and preventing users from modifying web browser option settings that direct to an external Proxy Server. Instead, create an internal Proxy Server and require them to point to the corporate Proxy Server in order to gain access to the Internet. Regardless of what methodologies are used, they should include user awareness training. Educating the end users is exercising due diligence and applying best practices towards enforcing effective security practices. However, if there are anonymizers being used, the network administrators need to know what types of tools are available, how to use them, and how to detect and identify types of anomalies in traffic that have the signature of an anonymizer.

5. Detection

5.1. General Practices

Because there are so many anonymizer proxy servers and services available, it is difficult to apply general best practices in detecting them all. However, there are some strategies that can be applied in trying to prevent them from being used. Some methods include applying Blacklist filters or creating ALCs to deny PHP and CGI proxy servers and scripts.

In the following section, a scenario will illustrate first, a host trying to access a blocked website without using an anonymizer. Then, trying again, after turning on the anonymizer to bypass the firewall and gain access to this blocked website. By comparing, contrasting, and analyzing the two captured files, can a thesis be concluded in identifying anonymizer usage?

5.2. Wireshark Software

The Wireshark open-source packet analyzer can capture and detect traffic (Wireshark, 2012). In this scenario, a host is attempting to access a website (www.anonymizer.com) and is blocked by the firewall. Wireshark, starting with frame Number 13, captures the host’s IP address (Source 10.210.205.92, port 40389) trying to
open a TCP connection (SYN) to the URL (Destination 209.143.153.58, port 80), see Figure 16.

Right-clicking on frame No. 13 (Time stamp 29.603.54) and looking at the “Follow TCP Stream”, shows that there was a SYN request, but there wasn’t any data sent back to the host (Source), as displayed in the “Stream Content”, see Figure 17.

Continuing at frame No. 14 (Time stamp 10.210.205.92), another SYN request was sent by the host. This can be identified by the source port, now 40390, and is captured by the Wireshark protocol scanner. The host is continuing to send SYN requests and still trying to attempt to gain access to the blocked website, see Figure 18.
Surfing the Web Anonymously – The Good and Evil of the Anonymizer

Right-clicking on frame No. 14 and opening the “Follow TCP Stream” again shows that the stream content has a GET / HTTP 1.1 sent from the source to destination host (www.anonymizer.com) and was intercepted and Moved to Location: http://192.168.116.101:15871/cgi-bin/blockpage.cgi?ws-session=2483493383, see Figure 19.

This is because the firewall is running on a Websense V-Series appliance (IP address 192.168.116.101) that provides web security and email security (Websense 2012). It blocks access to unauthorized websites and responds back with a “Security risk blocked for your protection” message to the source’s web browser, in this case the host who requested the connection to the URL. This message is displayed in the host’s web browser (see Figure 20) and is captured with Wireshark on frame No. 14.

Peter Chow, chow_pete@yahoo.com
5.3. Packetzer Software

Using another type of network sniffing software to capture and/or analyze the traffic sessions can provide another point of view in identifying curious or suspicious types of traffic. Save the Wireshark captured session and reopen it with Network Chemistry’s Packetzer software, a network utility that captures, analyzes and provides useful packet information from different protocols (GoToAssist, 2012 and Informer Technologies, 2012).

Figure 21, illustrates the same data session captured by Wireshark reopened using the Packetzer software. Notice starting at frame Number 13, that the Source Address is the same Host IP address (10.210.205.92) to the destination IP address (209.143.153.58) when using the Wireshark application.
However, unlike Wireshark, after Right-Clicking on frame Number 13 and opening the “Follow TCP Stream”, Packetzer displays the information in the “Stream Content” (Decode in Packetyzer), and includes a tab for “Trace.” This is useful in providing a more granular and visual analysis of the capture data stream, see Figure 22.
Following the TCP 3 Way Hand Shake between the communication paths, each TCP flag indicates the corresponding sequences. Following are explanations for each TCP flag, see Figure 23 (Microsoft Support, 2012).

- **A, ACK-** (Acknowledge) The receiver will send an ACK that equals the senders sequence number plus the Len, or amount of data, at the TCP layer.
- **SYN, and FIN flags count as 1 byte. The ACK can also be thought of as the sequence number of the next octet the receiver expects to receive.**
- **S, SYN-** Synchronize is used during session setup to agree on initial sequence numbers. Sequence numbers are random.
- **F, FIN-** Finish is used during a graceful session close to show that the sender has no more data to send.
- **R, RST-** Reset is an instantaneous abort in both directions (abnormal session disconnection).
- **P, PSH-** Push forces data delivery without waiting for buffers to fill. This is used for interactive traffic. The data will also be delivered to the application on the receiving end without buffering.
- **U, URG-** Urgent- Data is sent out of band.

Figure 23: TCP Flags

Observing each flag of the TCP 3 Way Hand Shake, starting from frame 13 the trace identifies at timestamp 12:00:56:733.77 when the host source sends a SYN flag to initialize connection with the destination. Following the sequences as illustrated, even though the destination replies back with a SYN, ACK at frame Number 17, and is acknowledged with an ACK at frame Number 18, there is still no data being sent back from the destination to the host. It is only going thru the TCP 3 Way Hand Shake without data being transmitted. Therefore, the session has not been blocked and is allowed to continue with the hand shake sequences. Notice the starting timestamp was at 12:00:56:733.777 (converted timestamp 2012-07-30 12:00:56.733777) on frame 13 and ended on frame 179 at 12:01:00.034.710 (converted timestamp 2012-07-30 12:01:00.034710). A period of about 3 and a half seconds has lapsed; during this time another session was started by the host to access the same destination website. Frame 14 started at 12:00:56.733.966 with the same Source host IP address, however with another source port number of 40390, and was initiated with another TCP 3 Way Hand Shake, starting with a SYN but with the Source IP address on port 80.

Peter Chow, chow_pete@yahoo.com
Notice how starting at frame 14 “TCP Flow”, as shown on figure 24, after the TCP 3 Way Hand Shake SYN, ACK is sent from the destination, the source sends an ACK, PSH request at frame 19.

Figure 24: Packetyzer capture, Frame Number 14

The ACK, PSH allows for data to be sent to the host. However, it is intercepted by the Websense firewall and instead of the requested website, in this case www.anonymizer.com, it is blocked and a warning message is sent to the host’s web browser. Clicking on the “Decode” tab shows that it has been moved to Location: http://192.168.116.101:15871/cgi-bin/blockpage.cgi?ws-session=2483493383.

Even though frame 13 initiated a request first to gain access to www.anonymizer.com website, because a second request at frame 14 was initiated, it was blocked and moved at frame 19 (part of TCP 3 Way Hand Shake from frame 14). Therefore, subsequent frames (i.e. frame 178) belonging to frame 13 TCP 3 Way Hand Shake would be blocked. Moreover, all requests to www.anonymizer.com would be blocked by the firewall. See Figure 25.

Peter Chow, chow_pete@yahoo.com
5.4. Capturing Anonymizer Traffic

Now that we know how normal traffic looks when a host requests access to a blocked website, let’s turn our attention to how it looks when the JAP Anonymity application is turned on and the host’s web browser (10.210.205.91) is now using the anonymizer proxy services. Using the Network Chemistry’s Packetzer software again we capture the host opening a web connection to www.anonymizer.com website. Figure 26, verifies that the host can access the blocked website.

Figure 25: Packetyzer capture, Frame Number 14 – TCP Flow

Figure 26: Bypassing Firewall and accessing blocked website

Peter Chow, chow_pete@yahoo.com
Figure 27, shows that the Packetzer software successfully captured data at the time the host was accessing the blocked website. Reviewing and analyzing the captured data, notice that there are a lot of "Continuation or non-HTTP traffic" that was not present when the anonymizer proxy was not enabled. "Continuation or non-HTTP traffic" is common traffic with HTTP. These packets contain additional content that didn't fit into a single packet and is part of a larger payload. Therefore, it is not an indication that an anonymizer proxy is being used.

However, it should raise suspicion and warrant additional review as to why a large volume of “Continuation or non-HTTP traffic” was generated. Upon review, none of these frames points to the blocked website, instead they point to 128.30.52.37, 72.55.137.241, and 88.198.24.24.

Peter Chow, chow_pete@yahoo.com
Opening a web browser and resolving these IP addresses, IP address 128.30.52.37 points to www.w3.org (see Figure 28). IP Address 72.55.137.241 points to InfoService Name: Octavius (see Figure 29), and IP Address .198.24.24 points to InfoService Name: is.beneficum.de (see Figure 30).

Figure 28: 128.30.52.37 points to www.w3.org

Figure 29: 72.55.137.241 points to InfoService Name: Octavius

Figure 30: 88.198.24.24 points to InfoService Name: is.beneficum.de

Both IP addresses 72.55.137.241 and 88.198.24.24 point to InfoService for ANON/JonDonym anonymizer proxy services. Even though the sniffer software did not capture content that included anonymizer proxy strings, it was able to capture suspicious traffic that warranted further review.

Peter Chow, chow_pete@yahoo.com
While it is not conclusive that “Continuation or non-HTTP traffic” indicates an anonymizer proxy is being used, it does however point to anomaly traffic that can used to set firewall rules to trigger, and to pursue additional review. Understanding and establishing a baseline of what is considered normal traffic within a network infrastructure can aid in combating against anonymizers. In addition to setting Blacklist filters, creating ALCs to deny PHP and CGI proxy servers and scripts can help mitigate the use of anonymizer applications and add additional layers of security.

5.5. Blocking the detected anonymizer traffic

While the purpose of this paper is to address awareness regarding the usage of anonymizers (The Good, Bad, and Ugly,) it is also prudent to mention how to block anonymizer traffic once it has been detected. There are numerous ways to deploy countermeasures; therefore, the actual techniques and how-to-use of an application will not be addressed in this paper. However, a brief overview on detecting and blocking anonymizer traffic will be presented.

5.5.1. Detection

Both Wireshark and Packetyzer are excellent tools when installed on a standalone system to monitor packet traffic patterns. However, it is not the most efficient method to monitor an enterprise network. Deploying purpose-built and dedicated appliances with specialized applications that can monitor the infrastructure holistically is a more responsive way to analyze and detect packet traffics. Hardware platforms that can be used include Cisco’s IPS 4200 Series Sensors (Cisco, 2012) or a server-class computer that has been hardened (a system operating system that has been made secured with reduced vulnerability.) After the system has been hardened select and install an array of software applications and options, such as Snort, Bro, and Suricata. After selecting the platform and software package, the question then becomes how to deploy the solution. It is normally incorporated into the network infrastructure as a Network-Based Intrusion Detection System (NIDS) and can be deployed similarly to deploying a firewall, either In-band (see Figure 31) or Out-of-band (see Figure 32) depending on the network architecture and design, and which one is better suited over the other.

Peter Chow, chow_pete@yahoo.com
Some differences between In-band versus Out-of-band are compared in Nevis Network paper titled “An Architectural View of LAN Security: In-Band versus Out-of-Band Solutions” (Nevis Network, 2007), see Figure 33.

<table>
<thead>
<tr>
<th>Feature</th>
<th>In-band</th>
<th>Out-of-band</th>
<th>Benefit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoint Compliance and User Authentication</td>
<td>Performed in straightforward manner, with remediation options that avoid VLAN steering.</td>
<td>Must be done in a provisional VLAN, then client traffic steered to an assigned or quarantine VLAN. Threats can spread within VLAN.</td>
<td>Does not ever require client to re-acquire IP address, which adds delays in users logging in.</td>
</tr>
<tr>
<td>Identity-Based Access Controls</td>
<td>Internal stateful firewall policies based on source, destination, and traffic content.</td>
<td>VLAN steering would work if different zones are placed in different VLANs. Finer granularity requires upstream firewalls.</td>
<td>In-band provides fine-grained identity-based access controls as basic security feature.</td>
</tr>
<tr>
<td>Malware Detection</td>
<td>Continuous malware detection using various techniques, including behavior and signatures</td>
<td>No visibility into user traffic since out of flow of network traffic during session. Requires additional upstream IDS for comparable security.</td>
<td>In-band provides persistent malware detection and prevention as a basic feature.</td>
</tr>
<tr>
<td>Visibility and Monitoring</td>
<td>Continuous monitoring of and visibility into all user activities, with associated user-based reports</td>
<td>No visibility into user traffic since out of circuit. Requires additional sensors, displays and reporting infrastructure for comparable security.</td>
<td>In-band provides persistent role-based monitoring and visibility as a basic feature.</td>
</tr>
<tr>
<td>Quarantine Enforcement</td>
<td>Done using stateful firewall approach, shielding all users from each other</td>
<td>Places non-compliant users in a common quarantine VLAN</td>
<td>In-band protects vulnerable or infected clients from each other</td>
</tr>
<tr>
<td>Cost</td>
<td>No hidden deployment or reconfiguration costs, no upgrades to existing infrastructure required.</td>
<td>Initial capital expense for devices and controllers, but higher operational costs, and potential upgrades of enforcement points</td>
<td>In-band offers lower overall cost of deployment and management.</td>
</tr>
</tbody>
</table>
One of the major considerations when selecting NIDS software packages is the cost. Snort is an open source network intrusion prevention and detection system (IDS/IPS) developed by Sourcefire. Snort, combines the benefits of signature, protocol, and anomaly-based inspection, (Sourcefire, 2012) is free, and operates on both Linux distributions and Windows, which makes this one of the top picks by network security practitioners. To learn more about Snort installation, configuration, writing Snort Rules, and the user manual, see Sourcefire’s Snort Official Documentation at http://www.snort.org/docs. Figure 34 illustrates Snort alerts outputting to a Kiwi Syslog server (retrieved from the “Installing Snort 2.8.5.2 on Windows 7” by Kasey Efaw, http://www.snort.org/assets/135/Installing_Snort_2.8.5.2_on_Windows_7.pdf).

5.5.2. Blocking (prevention)

After configuring the NIDS rules (signature), when an event matches the rule(s), it will then forward the alert to an event logger, such as a Kiwi Syslog server. This will only alert administrators. Manual action must be taken by the administrator to prevent or deny access to stop anonymizer usage. A Snort rule to detect this proxy is shown below, see Figure 35 (Brozycki, 2008).

```
alert tcp SHOME_NET any -> SEXTERNAL_NET any (msg: "PHP Proxy detected"; pcre: "/(index\.php\?q=)\.(html)\?i/"; classtype:policy-violation; sid:50010;)
```

Figure 35: Snort rule

Peter Chow, chow_pete@yahoo.com
The other option to NIDS is NIPS (Network-Based Intrusion Prevention System). While NIDS will only alert (Passive, monitor and notify), NIPS (or IPS) can take immediate action(s) (Active, monitor and automatically defend) set by an administrator. Depending on the network infrastructure (In-band or Out-of-Band provisioning) and type of appliances (separate or built-in Firewall/IPS) being used, different configurations and parameters are required. See Nicholas Pappas paper on Network IDS & IPS Deployment Strategies for comparison and deployment options (Pappas, 2008).

### 5.5.3. Out-of-band (OOB) NIDS

Network-Based Intrusion Detection Systems (NIDS) are normally provisioned as Out-of-band and passively monitor signatures for exploits, in this case anonymizer traffic. In this configuration the NIDS appliance only used one network interface card (NIC) and is connected directly into the network, illustrated in Figure 36. The NIC is set to promiscuous mode, it only receives traffic. It monitors the network traffic and when interesting traffic is matched to the rule an alert is sent to the administrator who in turn takes appropriate action (such as manually configure the firewall) to block the traffic. Other considerations for OOB provisioning include lower load demand on the NIC, lower memory usage, and less CPU processing. In addition, it is not a single point of failure and will not bring down the network if the NIDS stops working.

![Figure 36 NIDS – Out-of-band](image-url)
5.5.4. **In-band (in-line) NIPS**

Network-Based Intrusion Prevention Systems (NIPS) are provisioned In-band and require two NICs to pass traffic thru the NIPS. Therefore, they require higher load demand on the NICs, higher memory usage, and more CPU processing is needed. In this configuration, it is a single point of failure for that segment if the NIPS stop working (see Figure 37). Because the NIPS is an in-line arrangement, when interesting traffic is matched to the rule, not only will it send an alert to the administrator, it can also be configured to automatically drop or block that traffic. Although this could result in a faster reaction, it could also have more false-positive consequences, whereby it may falsely drop legitimate traffic.

6. **Conclusion**

The point of this paper was to gain an understanding of what and how Anonymizers and Proxy servers are used. An introduction and example of an anonymizer application was illustrated and showed that it required very little technical skills to circumvent a corporate firewall’s rules and access a website that is normally blocked. However, for the security practitioner, this can pose a major challenge. Having the technical expertise and specialized skills to implement the most optimal and secured solution can be very costly in time and expenses. In contrast, those who use anonymizer applications require very little knowledge and a modest, to no cost, investment.

Peter Chow, chow_pete@yahoo.com
There are free of charge Proxy services which may be suitable for the common user to add a level of confidentiality, but for the professional road warrior who is off the corporate network, paying for the premium monthly subscription would be a prudent course of action.

The good, bad, and ugly of anonymizers is summarized by the same usage but results that are drastically different. This will keep network engineers, system administrators, and security practitioners on a diligent watch, being mindful that a simple rule set on a firewall may not be good enough to keep unwanted network traffic off the corporate network. Therefore, due diligence in a corporate environment must be exercised, whereby having well crafted security and acceptable usage policies created, established, and enforced with consequences if the policies are violated. Moreover, these policies need to be addressed and supported at the highest corporate executive levels to ensure validity and seriousness when these policies are breached. When anonymizers are used as they were intended, to add a level of security and confidentiality in protecting ones identity while surfing on the Internet, then anonymizers are a useful tool. Regardless of who, how or what anonymizers are used, they are not going away and more will be developed and made available for all who want to use them for purposes of good, bad, and ugly.

7. References


Peter Chow, chow_pete@yahoo.com


Peter Chow, chow_pete@yahoo.com
Appendix A

Downloading JAP

Step 1: Open a web browser and enter in the address bar [http://anon.inf.tu-dresden.de/index_en.html](http://anon.inf.tu-dresden.de/index_en.html) to open the JAP Anonymity & Privacy website. Locate “Download” on the left side of the homenage and click. See Figure 31 (JAP, 2012).

![Figure 31: JonDonym anonymous proxy (JAP)](image)

Step 2: Click on “Windows” to download the application for the Windows operating system, Figure 32 (JAP, 2012).

![Figure 32: Download JAP application](image)

Step 3: Select “Save as” to save the jasetup.exe program, Figure 33 (JAP, 2012).

![Figure 33: Saving JAP application](image)

Peter Chow, chow_pete@yahoo.com
Appendix B
Installing JAP

Step 1: After downloading the application, click on the application to start installation, Figure 34.

Figure 34: Launching the installation application

Step 2: Next, select components to install, click and check on “JAP”, then click on the “Next” button, see Figure 35.

Figure 35: Select and install application components

Step 3: Choose the location to install the program. Use the default “Destination Folder” setting and install it into “C:\Program Files\JAP” directory by clicking the “Next” button. See Figure 36.

Figure 36: Selecting an installation directory

Peter Chow, chow_pete@yahoo.com
Step 4: Choose a Start Menu Folder, use the default folder by clicking on the Install button to continue, Figure 37.

Figure 37: Create program shortcut

Step 5: Click “Close” after the installation has been completed, Figure 38.

Figure 38: Setup completed

Step 6: The application will automatically update help files; no action needs to be taken, just wait for it to be completed, Figure 39.

Figure 39: Updating help files

Peter Chow, chow_pete@yahoo.com
Step 7: After the update to the help files has been completed, the Installation assistant will start. Select Language type, in this example, “English”. Click on the Simplified view and then click on the “Next” button to continue, Figure 40.

![Figure 40: Language selection](Image)

Step 8: In Figure 41, the Installation assistant will prompt you to enter a premium code. Leave this blank and click the “Next” button to use the free service.

![Figure 41: Bypassing activation code](Image)

Step 9: Next, the Installation assistant will display a message to select Premium services. Click “Next” to continue, Figure 42.

![Figure 42: Skipping Premium services](Image)

Peter Chow, chow_pete@yahoo.com
Step 10: Select the “All data are either colored in green or orange” and then click “Next” to continue, Figure 43.

Figure 43: Testing installation

Step 11: Installation is now completed, click “Finish”, Figure 44.

Figure 44: Completed installation
# Upcoming SANS Training

Click here to view a list of all SANS Courses

<table>
<thead>
<tr>
<th>Course</th>
<th>Location</th>
<th>Dates</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS Amsterdam August 2020 Part 1</td>
<td>Amsterdam, NL</td>
<td>Aug 03, 2020 - Aug 08, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS FOR508 Canberra August 2020</td>
<td>Canberra, AU</td>
<td>Aug 17, 2020 - Aug 22, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Amsterdam August 2020 Part 2</td>
<td>Amsterdam, NL</td>
<td>Aug 17, 2020 - Aug 22, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Virginia Beach 2020</td>
<td>Virginia Beach, VAUS</td>
<td>Aug 31, 2020 - Sep 05, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Philippines 2020</td>
<td>Manila, PH</td>
<td>Sep 07, 2020 - Sep 19, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS London September 2020</td>
<td>London, GB</td>
<td>Sep 07, 2020 - Sep 12, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Baltimore Fall 2020</td>
<td>Baltimore, MDUS</td>
<td>Sep 08, 2020 - Sep 13, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>Threat Hunting &amp; Incident Response Summit &amp; Training 2020</td>
<td>New Orleans, LAUS</td>
<td>Sep 10, 2020 - Sep 17, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS OnDemand</td>
<td>OnlineUS</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
<tr>
<td>SANS SelfStudy</td>
<td>Books &amp; MP3s OnlyUS</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
</tbody>
</table>