Global Information Assurance Certification Paper

Leo Erkkila January 9, 2002

CORPORATE PERSONAL FIREWALLS AND OUTBOUND PROTECTION

INTRODUCTION

The popularity of laptop computers, broadband Internet access and VPN connections has set new requirements for network security solutions. To provide new tools to enhance security with corporate and home users, many vendors have introduced new personal firewall products. Sometimes also referred as desktop firewalls, these products include technology commonly found in traditional firewalls and anti-virus software. Personal firewalls are not used to replace traditional firewalls or anti-virus agents; instead they are used as an add-on solution to enhance overall security.

Most commonly, a personal firewall protects the host machine by filtering malicious network traffic and denying some dangerous applications to operate.

This work focuses on outbound traffic and how to properly filter it in personal firewalls. If too much is filtered out, problems usually occur. If nothing is filtered, the security level is not optimal.
There are some tests, like the LeakTest (1), which can be used to test this feature. One must first understand the concept of LeakTest, before the results can be fully comprehended. Failing LeakTest proves that the personal firewall is not full proof, but the test does not give any results of the overall security level of the product.

Outbound protection is important if some type of malicious code has already infected your machine. It can be also used to prevent end users from running unauthorized applications, like the famous Gnutella suite of file sharing applications. These popular peer to peer networking applications can be considered as a serious threat to corporate information security (2).

PERSONAL FIREWALLS AND TRAFFIC FILTERING

If we take a look at the personal firewall products on the market today, we notice that there are many competing vendors and solutions available. They all seem to have good protection features. In fact, a network security professional can immediately notice many flaws in the products. Some products do not support all the network interfaces a host machine may have. Some do not support outbound traffic filtering. Some only have basic packet filter type firewall engine. Some products do not block non-IP protocols (NetBEUI, IPX, etc.). Logging features and information content of the collected logs can vary. It is very important to take these small details into account, when selecting a personal firewall product. In corporate solutions, there is usually some kind of management system included. The functionality and security of the management system should also be considered. Weak security in the management system lowers the overall security level of the solution.

The most fundamental task of personal firewalls is to filter network traffic. We can divide traffic filtering into three categories:

1. Filtering based on fixed rule base
2. Filtering based on intrusion detection system dynamic blocking feature
3. Filtering based on application recognition

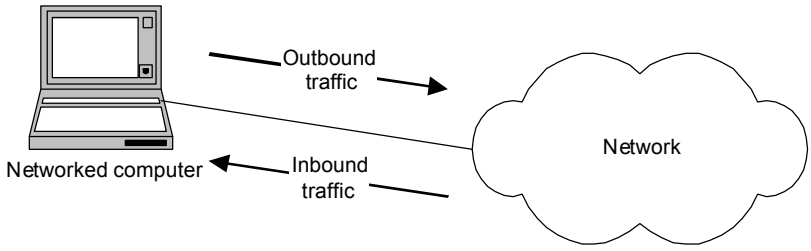
The best overall security is of course obtained when all these are combined. Some performance drop may occur, but modern PC based desktops and laptops can provide more than enough performance to compensate. And some companies prefer security over performance, so this drop in performance may be considered harmless.

A very common configuration seen is to block all inbound traffic and to allow all outbound traffic if IDS (Intrusion Detection System) or application rules do not block it. Application rules are efficient, but they are very problematic in corporate use. How to efficiently maintain the application rules of 1000 computers? We can allow the user to maintain the rules, by accepting or denying traffic for each used application. In this case the personal firewall asks the user, whether or not to allow this application to send data to network. We can assume that the user will eventually answer yes when it is not appropriate. Most users do not have enough knowledge or patience to make correct decisions to even partially administer a personal firewall. Sometimes it is very challenging even for trained network security professionals. If network administrators maintain the application rules,

the workload is enormous. The application rules should contain cryptographic hash values (most commonly MD5 hash values) of all the executables and system files used in all the desktops and laptops. What a daunting task! Collecting the information for used applications is one thing, but collecting the information for Windows system files is even more challenging. System files are also bound to change when new patches and service packs are applied. In practice this is not possible, because if we only allow the applications listed in personal firewall configuration, patches and service packs cannot be applied to the machines until they are first tested, correct hash values calculated and applied to client computers. The same problem is faced when setup programs are launched for installing new applications to client computers. There are very few organizations where these kind of restrictions would work, in other companies they would cause too much delays and thus lower the efficiency of the IT systems. And if applying new security fixes is delayed because of personal firewall, we can question whether this approach increases or decreases the overall security level in the organization.

IDS dynamic blocking is a very good feature. If the IDS module detects a traffic pattern for a Trojan horse, scanning attempt or network level attack attempt, it can dynamically block all traffic necessary to neutralize the threat. The efficiency of the IDS is of course dependent of up to date information of the threats. IDS dynamic blocking can never be full proof, because it does not detect new or modified Trojans, scanning techniques or network level attacks.

THE NEED FOR OUTBOUND FILTERING



Why do we need outbound traffic filtering? Let us take an example. You are using your laptop in your office, and you are browsing the web. Somehow a new Trojan infects your machine by exploiting a security weakness in your web browser. The anti-virus software does not notice the Trojan, because it is of a new type. The Trojan starts to collect your company's sensitive data and tries to send it to some

Internet server using HTTP upload. Luckily your company's gateway firewall blocks HTTP upload. You are however unaware of the situation and take your laptop home with you at the end of the day. Later at home you connect the laptop to your ADSL Internet connection and believe that the personal firewall is efficiently protecting your computer. Think again. Even if your personal firewall would have outbound filtering, the HTTP port is usually left open because it is required for web access. And very few personal firewalls contain content inspection features similar to your company's gateway firewall. In this case the Trojan can communicate with outside world and that is a bad situation.

We certainly need to have outbound filtering, but we can never make it full proof. The reason is simply that if your machine is networked, you always have to allow some traffic. Trojans can be modified to use almost any kind of traffic, which is why all outbound traffic should be considered as a risk (3).

PROTOCOL INSPECTION AS A SOLUTION

The previous chapter mentioned that a gateway firewall was able to block HTTP upload. To accomplish this, a firewall must understand the syntax of the particular protocol. In this example the protocol was HTTP, in practice the firewall should understand the syntax of at least a few dozen most commonly used protocols. This would add the security level of the firewall significantly. For best security, there should be protocol level inspections for all the traffic types you are allowing outbound. Protocol level inspection alone cannot provide full proof security. First of all, it cannot inspect the contents of the traffic in all cases. For example SSH and HTTPS protocols carry the data in encrypted form. It is very difficult for the protocol inspection module to check the traffic efficiently because of the encryption.

Another thing is the content inspection effectiveness. Even if the protocol inspection ensures that all the traffic passing through ports 20 and 21 is real FTP traffic, it cannot ensure that the files being transferred are not sent by a Trojan horse. Protocol inspection may also bring problems, because you need to upgrade your personal firewall when new protocol versions are taken into use; otherwise the personal firewall does not understand the new syntax. In practice this is not a big issue, because new widely used protocols are not introduced very often.

In Check Point Firewall-1 this kind of protocol inspection is provided by "security servers" modules (4). This product is not a personal firewall, but it can be used as a reference when discussing protocol inspection. Most personal firewall products lack protocol inspection, because it is very demanding technology to implement.

COMMON PROBLEMS WITH OUTBOUND FILTERING

Internet and other TCP/IP networks were designed so that traffic can efficiently travel from one place to another inside packets. Every time we want to limit this freedom, we have to plan the changes well; otherwise we will have problems later on. The situation is no different with outbound traffic filtering. As mentioned before, a Trojan might use HTTP protocol to communicate because it is commonly allowed in various different firewall configurations. To efficiently protect against this, we would block the HTTP ports in personal firewall. Sounds to be a good idea, if we don't need to browse the web. Most people however do, and users are furious if such a luxury is taken away from them. The use of HTTP proxy servers does not change the situation. Also other problems arise, some hotels and ISP's (Internet Service Providers) require that you first open the Internet connection using some access control web page. The page usually contains pricing information and legal terms. You would then activate the Internet connection by using your web browser to agree on the terms. We can see from this example, that you might need HTTP even if you only want to use FTP.

Another issue is with ICMP. ICMP echo_request and echo_reply (ping traffic) is allowed by most personal firewalls, because it is considered harmless. Normally it is harmless, but for example Trojans can exploit it. Trojans can use it in order to communicate through the personal firewall. In theory the Trojan can encode 8 bits of data into every ICMP echo_request packet by changing the packet size from 201 bytes to 456 bytes (256 different values equals 8-bit of information).

Some applications and services select port numbers quite randomly. Usually the source port changes constantly. Some protocols like IKE (Internet Key Exchange) usually uses UDP port 500 for both source and destination. Firewall rule base for IKE is easy to define, because the ports are always the same. Most of the traffic is not this simple, and makes building the rule base more difficult.

Generally it is not a good idea to permit outbound traffic based on RFC1918 IP addresses (also known as private addresses). An intranet server with IP address 10.10.10.10 is surely a trusted source when a laptop is in office network. If you take your laptop and connect it to your home ADSL Internet connection, the machine with IP address 10.10.10.10 may belong to your neighborhood 14-years old evil script kiddy (5).

OUTBOUND PROTECTION AND NETWORK PROTOCOLS

So far, we have only discussed personal firewalls and TCP/IP protocol. However TCP/IP is not the only network protocol used. Before the huge expansion of the Internet, other protocols were also used. For example NetBEUI and IPX/SPX are protocols that were commonly used just five years ago. Some companies are still using them, and many are using them is some parts of the network. Some Windows versions include these protocols by default, when you install a new network adapter. If you don't manually remove them, they are active and can be used to access your machine via network.

When you buy a personal firewall, you expect that it can protect your machine against threats from network. Your machine most probably uses Ethernet network interface card. This means that your machine communicates with the network using Ethernet frames (layer 2). TCP/IP is just one possible protocol, which travels inside Ethernet frames. The same Ethernet connection could also be used by many other network protocols. In fact your machine can communicate with the network using TCP/IP, NetBEUI and IPX/SPX protocols (layer 3) all at the same time.

Some personal firewalls cannot provide protection for non-IP protocols (like NetBEUI and IPX/SPX). This should be considered as a weakness. When these kind of products are used, it is up to the administrators to make sure that non-IP protocols are not used or even installed on the machines.

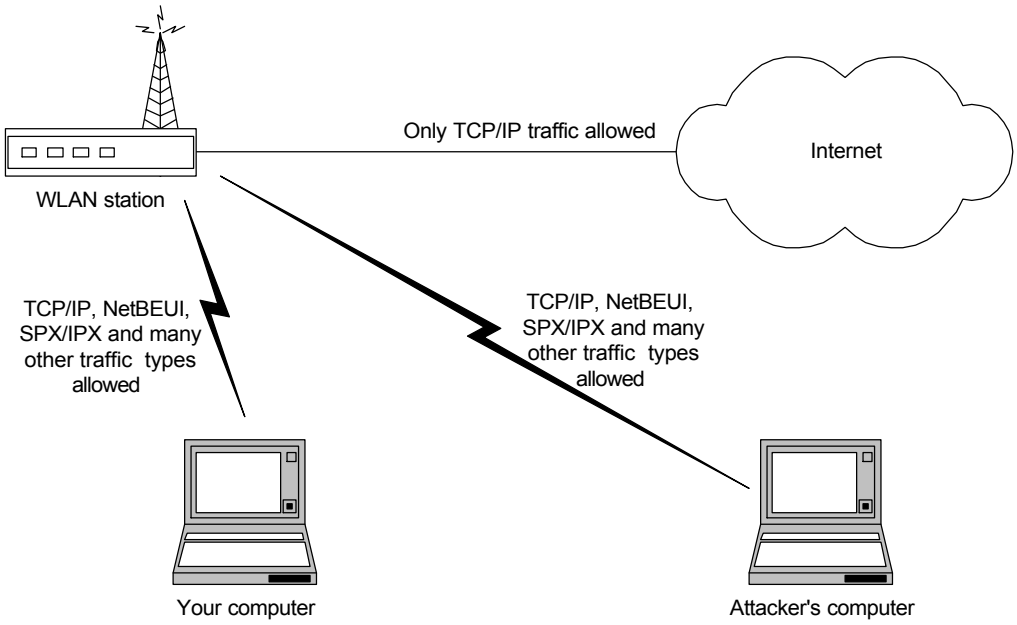
Normally non-IP protocols cannot be used over TCP/IP networks. There are however many different scenarios where non-IP protocols can compromise the security of remote users.

Whenever you connect your laptop (or other networked computer) to

Ethernet network, the machine can send and receive Ethernet frames to/from all the other machines located in the same Ethernet segment. In practice this means that if you connect a laptop to a network provided by some fair show organizer, the laptop could be contacted using NetBEUI and IPX/SPX by other computers in the same building. This was just an example that can easily happen in real life.

The introduction and popularity of WLAN (Wireless Local Area Network) has increased the need to have also non-IP protection in personal firewalls. WLAN operates like a wired Ethernet network, in a way that it allows Ethernet frames to be sent and received by all the machines in the same segment. Early WLAN solutions included WEP (Wireless Encryption Protocol) to provide security. However the WEP protocol has been proven to be insecure, so we should not rely on it. Whenever you are using WLAN, the same security risk is present as with any other Ethernet segment. Other machines might be able to contact your machine using NetBEUI or IPX/SPX protocol.

Let's take an example; take a look at the picture below.



The picture shows that although it is not possible to use NetBEUI or IPX/SPX to contact your machine directly from the Internet, it is possible to do it from a machine connected to the same WLAN network. This kind of situation is very common for example in airport WLAN networks, where even WEP is not used.

The best solution is to remove IPX, NetBEUI and other unused protocols from all corporate machines (6). Still a good personal firewall includes features, which can be used to control the use of these protocols.

CONCLUSION

It seems that more awareness is needed about personal firewalls and outbound protection, both among home users and network administrators. Personal firewalls seem to be similar to anti-virus products. You buy a box, install the software and your machine is protected. In practice there is much more to configure than in normal anti-virus applications. The network traffic filtering rule base is perhaps the most time consuming. It should be configured with great care, because many problems can be avoided and security can be vastly improved if the rule base is in order. Many products are installed with default settings, which allow outbound traffic quite loosely. This is expected because every corporate personal firewall solution needs to be tailored to fit the needs and requirements of the company's core network. By developing a good and flexible outbound protection for personal firewall clients, the network administrators can obtain the best possible security from the personal firewall without causing problems to end users.

REFERENCES

1. Gibson, Steve, "LeakTest", Gibson Research Corporation, November 23, 2001, http://grc.com/lt/leaktest.htm

2. Grimes, Brad, "Web Savvy", PC World, November, 2001

3. Markus, Henry, "Home PC Firewall Guide", November 25, 2001, http://www.firewallguide.com/

4. Nikitas, Michael, "Check Point Firewall-1's Stateful Inspection", SANS Institute, April 14, 2001, http://www.sans.org/infosecFAQ/firewall/inspection.htm

5. Farley, Marc and Stearns, Tom and Hsu, Jeffrey, "Guide to Security and Data Integrity" 1996, published by Osborne

6. DePaul University Network Security, "Securing Windows

95/98/2000", October 20, 1999,
http://networks.depaul.edu/security/win9x.htm

Last Updated: July 20th, 2017

Upcoming Training

SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event