Global Information Assurance Certification Paper

Securing the SOHO: A Discussion with a Tutorial of Tiny Personal Firewall 2.0

Dave Shackleford
GSEC Practical Assignment version 1.4b

Abstract

Conducting business activity from remote locations generates a new set of problems related to information security. This paper will discuss the management and security of the SOHO (small office or home office) from the perspective of the company as well as that of the remote worker. From the company's perspective, there are a number of technical concerns and implementation issues that must be addressed. The company is also responsible for providing the employees with a definitive policy that outlines how electronic business should be conducted, and the steps the employee must take in order to comply with information security guidelines within the company.

It is important for company employees to be aware of the many different types of risks that pose a threat to the company information on remote systems. With a well-written remote access security policy, there are a number of steps the employee can take to minimize risk and protect remote systems from compromise. Finally, this paper will provide a step-by-step tutorial of one particular host-based firewall product called Tiny Personal Firewall version 2.0. Free for personal use and relatively inexpensive for business use, this product can be used effectively to significantly minimize risk for telecommuters with broadband Internet access.

Main

As the business world becomes progressively more and more networked, the traditional environment in which people work is changing. Many companies are discovering that allowing staff to work from distant locations, commonly referred to as telecommuting, provides certain benefits to the company. Even though remote sales professionals have been using remote connectivity for some time, the advent of more efficient networking technology has enabled larger numbers of employees to take advantage of remote work opportunities. For the company, this can save money in overhead and keep employees motivated. For the employee, avoiding traffic and general quality-of-life improvement are the primary benefits.

As companies and organizations have increasingly relied on networks to run their businesses over the past 20 years, the inclusion of information security as a standard business practice has increased as well. Systems administrators, network engineers and administrators, and help desk personnel are all well aware in modern business society of the plethora of threats that attack their borders and internal systems daily. Although most malicious attempts to compromise business systems go unnoticed by the end users, it is generally agreed upon by information security experts and practitioners that the overall number of attacks is increasing steadily (Hassell, "Security Isn't Just for the Corporate World").

According to Jonathan Hassell, the typical SOHO user is concerned with

protecting the network from external attackers. He says that the typical SOHO user's internal security concerns include "…protecting children from adult Web sites, limiting access to newsgroups, and generally filtering Internet content." He also notes an interesting theory on why intruders might target SOHO users: to gain experience for larger conquests in the future (Hassell, "Security Isn't Just for the Corporate World"). Along with viruses, these "script-kiddies", or inexperienced hackers, comprise the vast majority of threats to systems on broadband networks.

For companies implementing a remote access work plan, which could involve sales personnel connecting to the corporate network or telecommuters that perform all work remotely, there are two primary areas of concern. The first is the technical implementation, and the details therein. To properly implement a remote work program, the organization's network must have certain key factors in place and configured. The second primary area of concern is the corporate remote access policy. Many companies underestimate the importance of properly planning and implementing a remote access policy. In today's environment, having all guidelines and requirements for remote access to the organization's network spelled out explicitly is paramount.

Companies are aware that remote access by employees now poses significant security risks. One concern is that intruders can access company information remotely just as employees would. This is typically accomplished by compromising either the remote employee's access information or penetrating the company network's resources in place for enabling remote access. The next area of concern is that attackers will either read or modify company data while it is in transit between the organization's network and the remote access employee (NIST, "Security Issues for Telecommuting", pg. 1). From the company perspective, there are areas of technical implementation to consider.

The first technical area to consider and implement is the firewall. A firewall is a piece of hardware or software that is used to protect internal resources from external influences, and is often used in conjunction with a router (Hassell, "How Firewalls Work"). There are a number of different types of firewalls available that can be used to help protect an organization's internal network. A few of the different types are:

- Packet-filtering firewalls: This type of firewall can be either static or dynamic. A static packet filter only looks at packets for pre-defined characteristics, and then screens them based on matches. A dynamic packet filter can monitor actual sessions, and decide whether a certain packet is appropriate in an actual context (Brown and Brown, pg.1). In general, packet-filtering firewalls are the most simplistic type of firewall, and are less common now than many more sophisticated filtering mechanisms.
- Proxy Services: Proxy services are slightly more "intelligent" than packet filters. Proxy servers act as a sort of "middleman" between

the internal network users and the external networks such as the Internet. When an internal network client accesses the Internet, he/she will actually pass through the proxy server. At this point, the internal user's IP address is replaced with the proxy server's IP address, shielding the internal address from any Web sites or external resources. This is also referred to as Network Address Translation, or NAT. Proxy servers can also store a cache of frequently accessed content, and provide this to internal requests much more quickly and safely than processing an internal-to-external transaction (Hassell, "How Firewalls Work"). Proxy servers can easily be used in conjunction with other types of firewalls and network gateways.

- Stateful Inspection firewalls: This is a somewhat newer technology that does not inspect the entire packet. Certain parts of each packet, such as certain headers, are compared to a database of information that is known to be good. If the format of the data is found to be acceptable, then the packet is let through. If the information raises a flag, then the packet is dropped. This type of firewall is powerful, yet can be defeated by certain types of malformed packets (Hassell, "How Firewalls Work").

Firewalls are an essential technology for business networks, and are highly recommended (in a smaller context, of course) for remote access users. Even though firewalls are powerful pieces of technology, they are limited in what they can protect the network from. Viruses, for example, are often transmitted by e-mail. There are a number of other measures a company can implement to successfully set up and maintain a secure remote access environment. Some of these include:

- Network-wide anti-virus software: The newest versions of network-based anti-virus software are very robust and scalable. Typically, an administrator can manage them from a single console, with virus definitions "pushed" out to the client desktops. For remote users, this may not be an effective option, however; in this case, the remote version of the software can be placed on a daily update schedule that checks for definitions at a predefined time. Leading vendors in this space include Symantec, Network Associates (McAfee), Trend Micro (aimed more at the gateway level), and Sophos.
- Virtual Private Networks: This is becoming one of the most common implementations of a remote work force. VPNs work by creating an encrypted "tunnel" between the company and the remote user that can safely pass encrypted data through the public Internet space. This technology requires two basic elements: software running on the client machine, and a hardware appliance on the company side that allows VPN tunnel connections (Brown and Brown, page 2).

- Data Encryption: This concept is often implemented for remote users via a VPN. There are varying types of cryptographic methods that an organization can employ to protect its data, and one of the most common is 3DES (Brown and Brown, page 2).
- Authentication: This concept relies on remote users to provide some alternate means of identifying themselves to the network. This could be a fingerprint (biometrics), a password, digital certificates, or a security token such as RSA's SecurID.
- Intrusion Detection: Having an intrusion detection system may not facilitate prevention unless it is a very sophisticated model that works in conjunction with firewalls; however, intrusion detection systems can alert administrators to the presence of suspicious activity on the network, which can greatly decrease response times to incidents and minimize the damage done (Brown and Brown, pg.3).

Aside from technical implementation, the other key aspect to a successful and secure remote access program is the organization's information security policy. Depending on the organization, this could be included within the overall security policy, or be a stand-alone policy dedicated to remote access only. This policy can be as simple as a few suggested guidelines for remote users to follow, or a strict step-by-step mandate that must be followed to the letter. According to the National Institute of Standards and Technology, the first step in planning for secure telecommuting is to determine the necessary type and level of access (NIST, "Security Issues for Telecommuting", pg. 1). The two determinations that management must make are:

- What would transpire if an intruder gained an employee's level of access?
- What are the chances that an intruder could capitalize on an employee's account to gain additional privileges within the network?
  (NIST, "Security Issues for Telecommuting", pg. 2).

There are generally two approaches to information security: disallow everything, and then allow only what is necessary, or allow everything and then remove what isn't necessary. For the most part, the former way of thinking is the more secure of the two, and this definitely applies to an organization's remote access policy. Some companies will take the hard-line approach, and restrict remote access employees to using PCs that are owned and configured by the company; this is similar to any PC that is in use within the organization's network. Other organizations may adopt a more laissez-faire attitude, letting employees configure their own hardware and software (Connolly, pg.1). Typically, a middle-of-the-road approach for a company's remote access policy is to specify certain system requirements for the remote PC (regardless of who owns it), designate certain software that will run on the machine such as anti-virus software and/or a host-based firewall program, and lay down guidelines for how the system should be configured and used for business purposes. Some

companies will require the remote user to bring the PC in to be configured, if they are allowing the use of an employee-owned PC for business use.

The remote users should be aware of the types of threats that can plague broadband connections, and depending on the requirements of the company security policy, what steps should be taken to prevent and eliminate them. According to Jonathan Hassell's article "Three Big Security Problems", there are three major areas of vulnerability that users should be aware of:

- Insecure operating systems: Most PC users in the world are using a version of Microsoft Windows. Knowing this, hackers find it very easy to target the Microsoft operating systems and wreak havoc on the most people. When an operating system is installed initially, it is NOT secure in the least (unless you are using an OS like OpenBSD). "Hardening" a system, or taking steps to make it more secure, will greatly reduce the risk of an attacker gaining access to a remote access machine.
- Unused Open Ports: Many services and applications, both inherent in the operating system and added separately, make use of ports. A port is a logical object that is created by the operating system for connections to be made to and from the system. The chances are good that a typical system has a number of ports open that don't need to be. A good way for users to discover which ports are open on their systems is by visiting a Web site that will scan their remote system, such as Steve Gibson's *Shields Up!* Utility, available at https://grc.com/x/ne.dll?bh0bkyd2 (Hassell, "Three Big Security Problems"). For Microsoft operating systems, certain open ports used for network inter-communication are instant "red flags" for hackers; these include 135, 139, and 445, depending on the particular operating system.
- Backdoors: Backdoor programs, or Trojan horse programs, are often installed by attackers or viruses as a means of accessing the system at a later time (after the initial exploit or penetration). These are often disguised as innocent programs that a user would not recognize as something other than a part of the normal operating system.

According to CERT's document entitled "Home Network Security", there are a number of other threats that SOHO users should be aware of. Denial-of-service, or DoS, attacks are always a threat, and they are very difficult to prevent. In a DoS attack, an attacker sends useless traffic to a particular target at a very fast rate. This has the effect of preventing legitimate traffic from reaching the intended destination. A machine that has been compromised by a backdoor program could be enlisted in another type of attack called a Distributed Denial-of-Service (DDoS) attack, where a user's system is used as a "middleman" to attack a different target. Windows shares, or shared drives, are also targets for attacker when they are not protected with passwords. If an intruder gains access to a shared drive, he or she could upload other hacking tools or backdoor programs to further compromise the machine or network.

Many IT professionals believe that none of the aforementioned threats are

actually the largest security problem facing SOHO users. Viruses and worms "…can have devastating effects if they get through your SOHO machines" (Siepmann, pg.1). As email has become the most critical business application, the number of security vulnerabilities affecting users via email clients such as Microsoft Outlook has risen dramatically. There are a number of different types of viruses and worms in existence today, including macro viruses, boot sector viruses, and polymorphic viruses. Most halfway decent virus-scanning software should detect the majority of these, but new viruses and worms are appearing daily. Another, somewhat related, type of threat is active/mobile code such as JavaScript and/or ActiveX objects. Embedding small pieces of this code in Web sites can allow intruders to gather information about remote users or execute commands on remote machines via the Web browser (CERT, "Home Network Security", pg.19).

There are quite a few steps that an individual or organization can take to make the remote computing environment much safer. CERT lists some of these in their "Home Network Security" paper:

- Use anti-virus software: This will more than likely be a primary component of the organization's remote access security policy. It is the user's responsibility, however, to make sure that the software is running and up-to-date.
- Use a firewall: There are both hardware and software versions of SOHO firewalls that can be easily configured to screen out unnecessary or unwanted traffic for broadband users. This may be specified in the remote access policy, as well.
- Back up critical data: A schedule for backing up critical data will probably be specified in the company security policy, but it is up to the remote user to maintain this.
- Patch the OS: This applies to applications, as well. According to the CERT Coordination Center, over 95% of network intrusions could be averted by updating the operating system and applications with vendor patches (Rogers, pg.2)
- Email attachments: Do not open email attachments from unknown sources, or peculiar sounding emails from known sources without verifying them first.

Another technology that is gaining popularity for use on client computers within the organization, as well as remote users' computers, is "sandbox" software. This type of software creates a virtual memory space, referred to as a sandbox, that can "…intercept all the active content…e-mail attachments, Java applets, scripts, ActiveX files, and executable files" (Bass, pg.1). This content can then be run within the isolated space, run normally, or blocked entirely. A leading vendor of this software is Finjan software, with a freeware product called SurfinGuard available for non-commercial use. Disabling active code in the browser and email applications can also minimize this kind of threat.

Tiny Personal Firewall version 2.0.15

A personal firewall can substantially reduce the risks associated with an "always-on" broadband connection to the Internet. Many organizations are making this a mandatory part of the remote access security policy for employees. Some of the features that NIST recommends these products contain are:

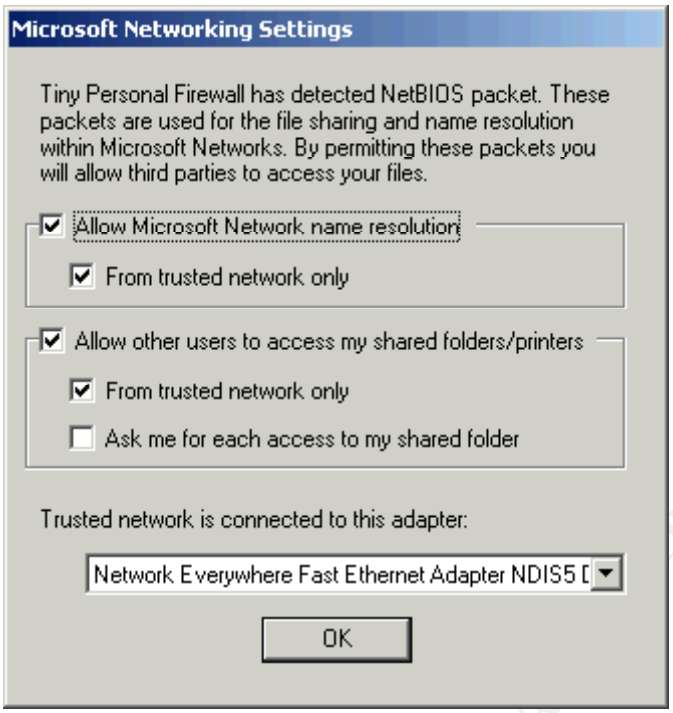
- Logging: This is essential for any personal firewall product (Kuhn et al., pgs. 10-11).
- Connection notification: The firewall should notify the user when an incoming or outgoing connection is attempted (Kuhn et al., pgs. 10-11).
- "Paranoia level" tuning: The firewall should be configurable for a high level of security (Kuhn et al., pgs. 10-11).
- Configurable rule set: The firewall should allow rules to be customized for users' needs (Kuhn et al., pgs. 10-11).
- Password protected configuration: The firewall settings should be able to be protected with a password (Kuhn et al., pgs. 10-11).

Some other recommendations for securely configuring a personal firewall include logging the IP address, date, and time of possible infractions, dropping all incoming packets to services that are inherently insecure such as NetBIOS 135 and 139, and dropping all outgoing packets except those recognized as being needed to conduct business (Kuhn et al., pgs. 11-12). The following numbered steps and screenshots are intended to provide a basic guide for installing, configuring, and maintaining the freeware version of Tiny Personal Firewall from Tiny Software.

1. Download the binary executable for TPF from Donwload.com at this URL: http://download.com.com/3000-2092-6313778.html?tag=list (Note: this may change. Do a search on Google). Save the file, named pf2.exe (1.35 MB) to your local machine.

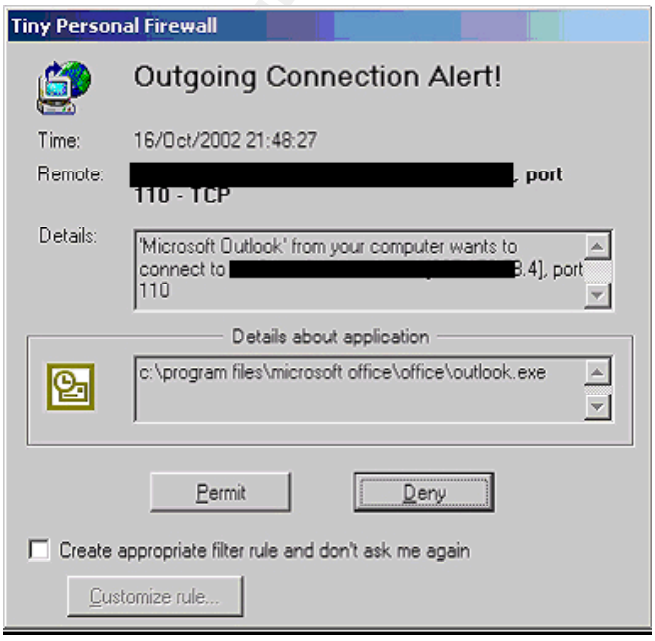
2. Double-click on the file to open the setup program. Click 'Next'. Select the directory where you would like to install the program (the default is C:\Program Files\Tiny Personal Firewall) and click 'Next'. Click 'Next' at the next two prompts, and the program will install. You will then have to reboot your machine.

3. If your computer is on a network with other Microsoft Windows machines, the firewall will detect the presence of NetBIOS traffic when the computer reboots for the first time. The screen that you will be presented with looks like this:



It is recommended that you leave the default settings in place, as the firewall is “intelligent” enough to determine which traffic is coming from the trusted network. Click “OK”.

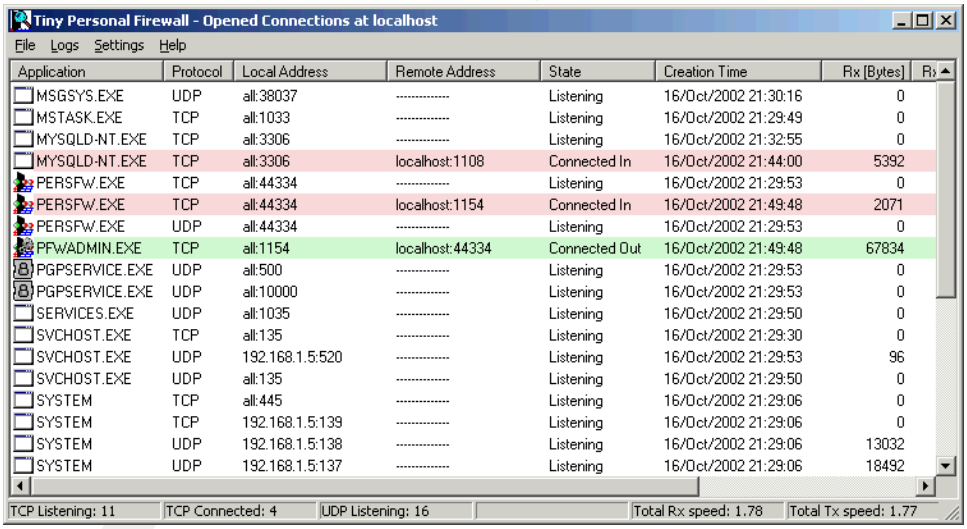
4. As an example of what will be presented to you whenever the firewall detects an outgoing or incoming connection, open your email application and check for new mail. You should see a screen pop up that is similar to the following:



As this is an application that you trust, check the box labeled 'Create appropriate filter rule and don't ask me again', and then click 'Permit'. Similar windows will appear for Web browsers such as Internet Explorer and Netscape Navigator, VPN clients, etc.

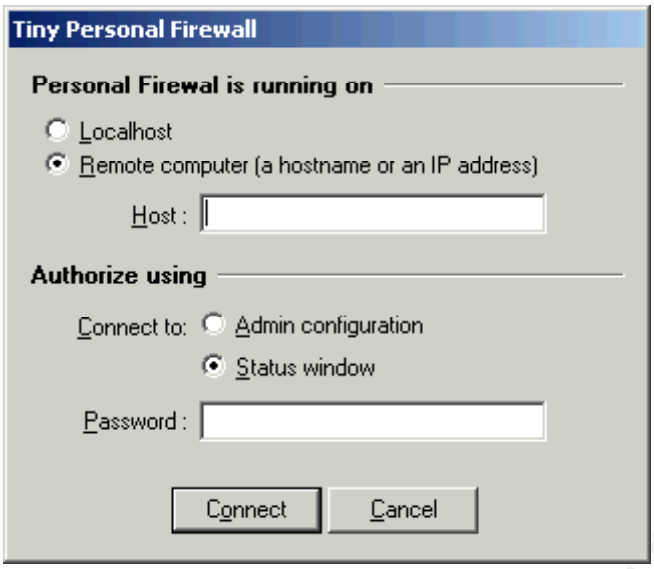
5. There should be an icon for the firewall in your system tray in the lower right-hand corner of the computer's screen. This icon looks like this:

By right-clicking on the icon, you will be presented with several options. The third option, 'About', will display some basic information about TPF such as the version number. The last option, 'Exit', will close the firewall. The first two options are of more import. The first, 'Firewall Status Window', will display the following screen when clicked:



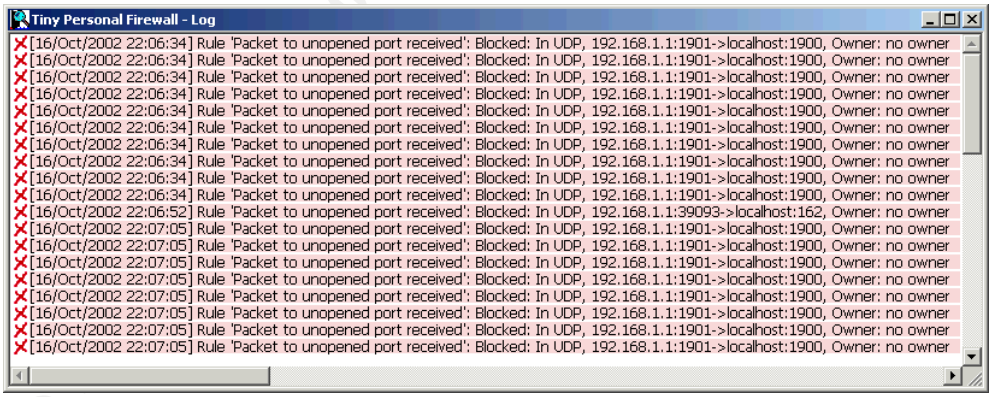
From this main console, which displays applications and information about them (including protocols, local and remote ports and addresses used, state, etc.) the vast majority of the firewall's functions and features can be accessed. We will discuss each of these in turn.

6. In a network with multiple firewalls installed, one firewall can actually be used to manage or monitor another. By clicking File → Connect, the following screen will be displayed:

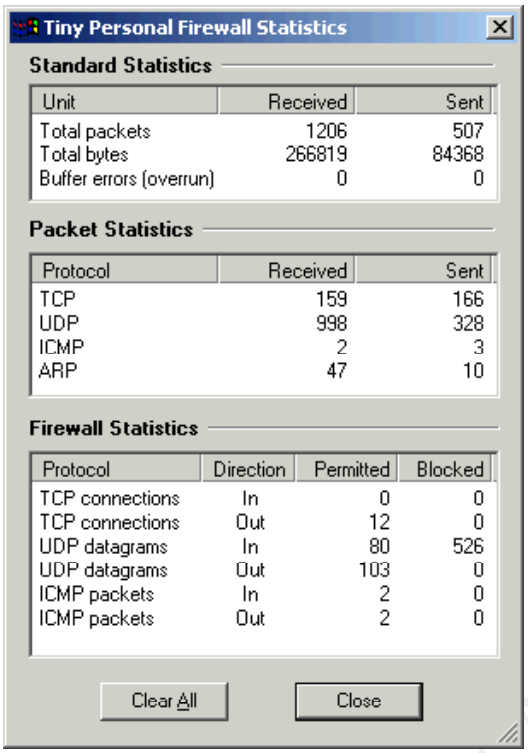


An administrator could connect to, and change the settings of, another machine's firewall by entering its NetBIOS name or IP address in the 'Host' text box under 'Remote computer'. Setting a password for remote administration is simple and then any changes to the firewall could be made from any other system with the firewall installed and the correct authentication.

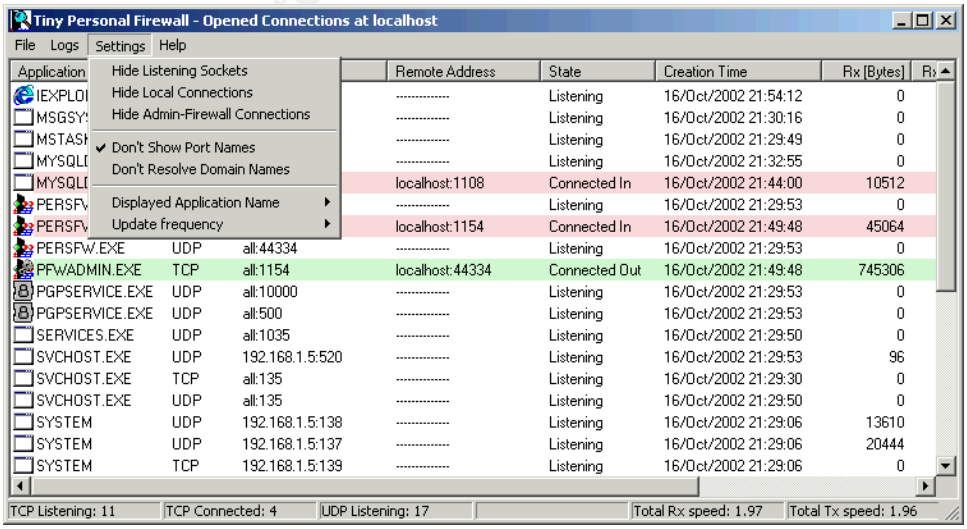
7. By selecting Logs → Firewall Log, the following will be displayed in a separate window:



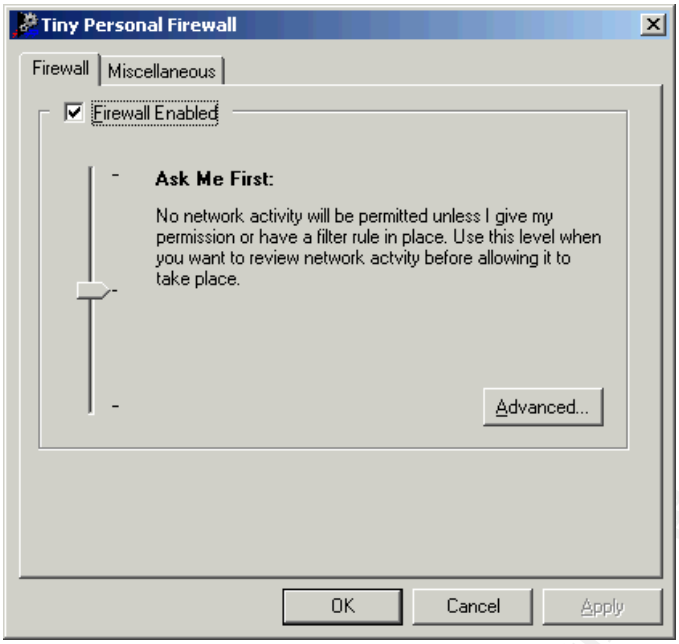
In the above example, only blocked attempts are shown. A green check mark will appear next to any entry that represents a successful connection through the firewall. Another log-related option is Logs → Statistics. This will open the following screen, which displays summary statistics such as the number and type of packets, and whether they were allowed or blocked:



8. The 'Settings' menu item within the Status Window contains a number of options related to the Status Window itself. You can choose to hide or display the listening sockets, or ports that are waiting for connections to be made, local connections, or admin-firewall connections. You can also choose to show the port names or resolve domain names to remote sites you are connected to:

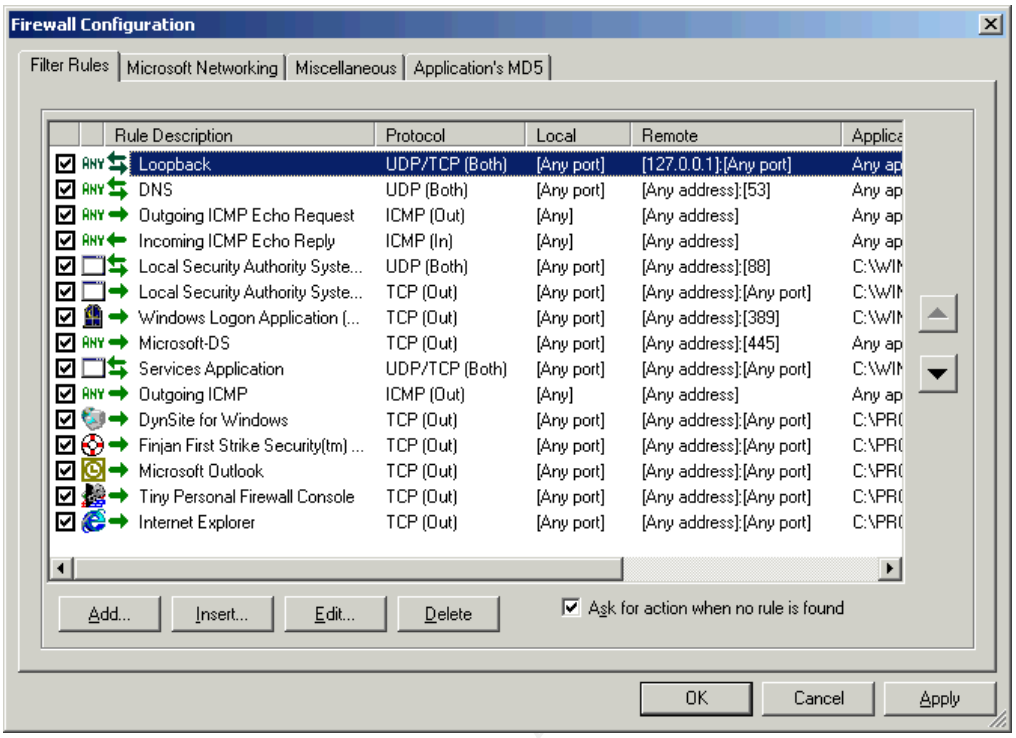


9. By right-clicking on the firewall icon in the system tray and selecting 'Firewall Administration', you should see the following screen:

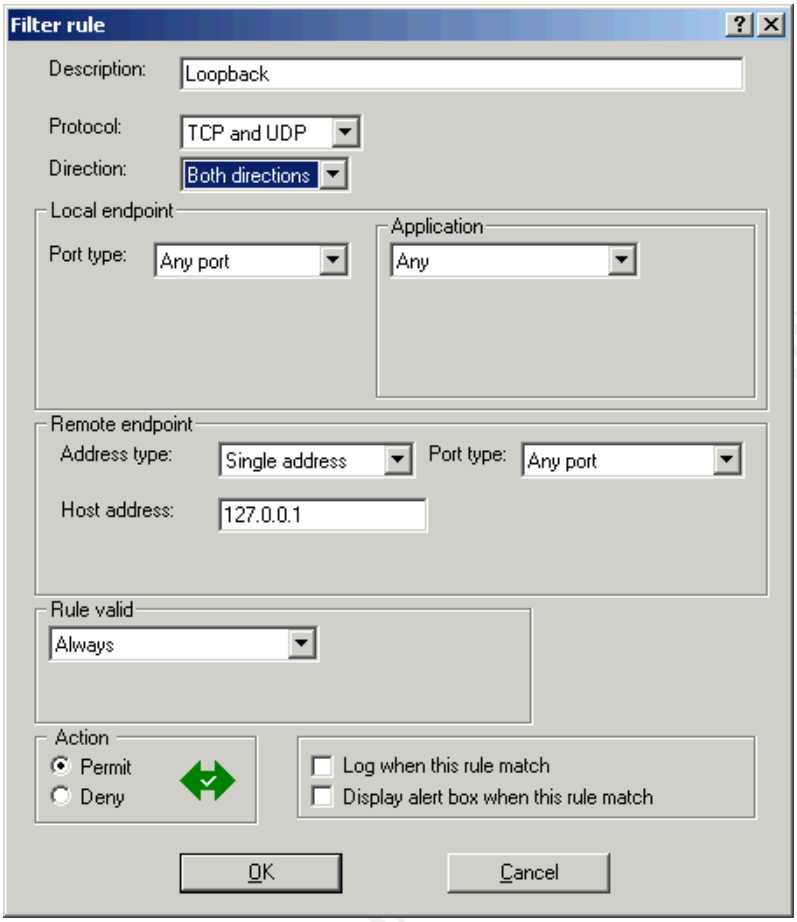


There are three basic settings that can be established, and each of these can then be modified as needed. The three settings are 'Don't Bother Me', 'Ask Me First', and 'Cut Me Off'. 'Cut Me Off' actually shuts down network access to the machine, which is an ideal option for evening hours or times when the machine is not in use. 'Ask Me First' gives users the ability to approve or disapprove of firewall activity in real-time, as events occur. No applications will be allowed to access external resources without the user's approval. Likewise, no incoming connections will be accepted either, unless the user says it's OK. Finally, 'Don't Bother Me' is the least secure setting available; at this level, all connections are permitted. This should sound familiar: Deny All, Allow All, or somewhere in-between.

10. The 'Advanced' button for each setting presents a different screen, as seen in the next screen:

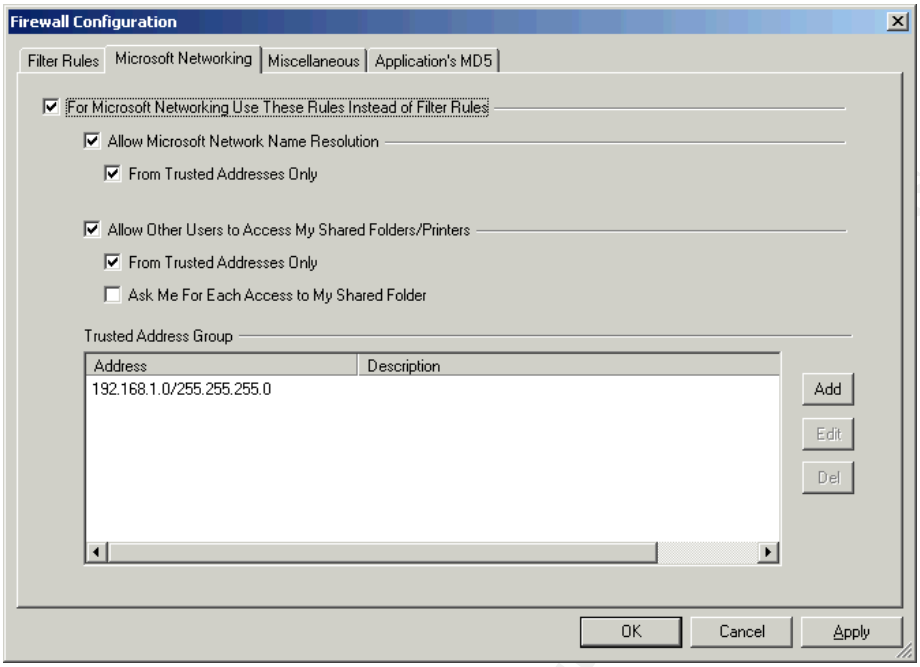


The first tab, 'Filter Rules', lists all of the individual firewall rules, and this allows for fairly granular changes to the firewall's overall configuration. For example, setting the Firewall settings to 'Cut Me Off', but then only allowing several business-specific applications and addresses through would be one ideal way to greatly improve the machine's security. Bu clicking on a rule to highlight it, and pressing the 'Edit' button, you will see the following screen:



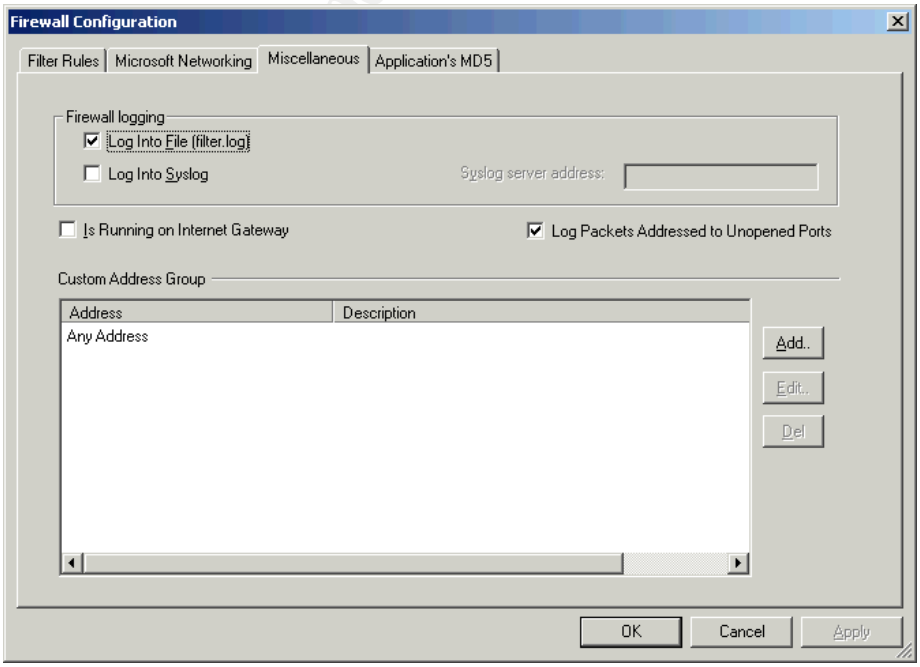
The fields that can be selected and changed here are fairly straightforward. The **Rule Description** is simply the rule's name. The **Protocol** can be one of a number of settings including TCP, UDP, TCP and UDP, or ICMP. The **Direction** setting can be Incoming, Outgoing, or Both. The Local and Remote ports, addresses, and applications can be set. Finally, you can set the rule to be valid only at certain times, permitted or denied, logged when it's activated, or displayed to the user in a popup window when it's activated.

11. The 'Microsoft Networking' tab in the Advanced features will display the following screen:



You may recognize these settings as the same ones you set upon the machine re-booting. In this console, however, it is possible to add trusted network IP ranges. For VPN applications that may rely on Microsoft SMB and NetBIOS traffic, this is an important feature.

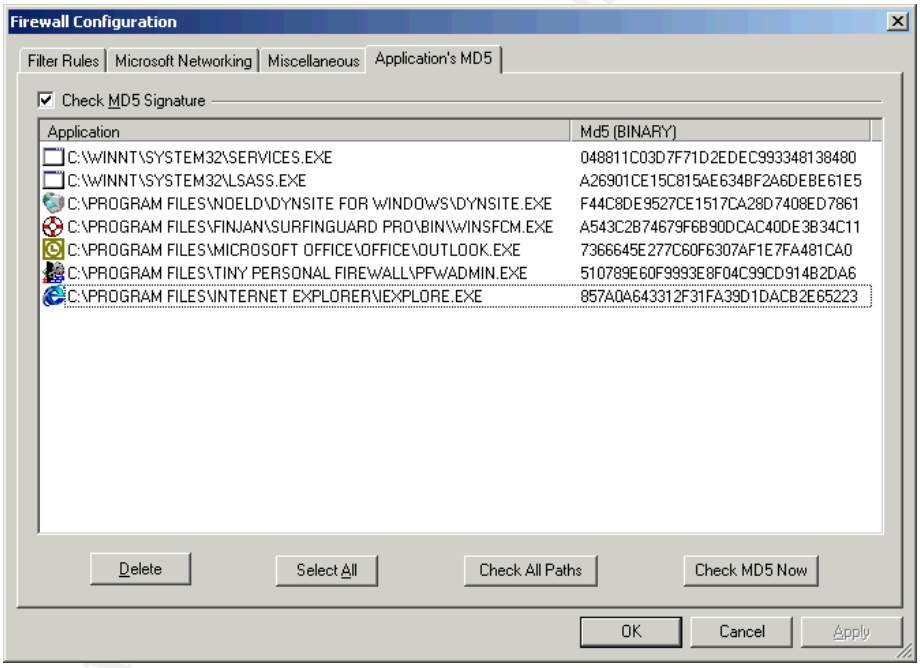
The next tab is the 'Miscellaneous' tab, shown here:



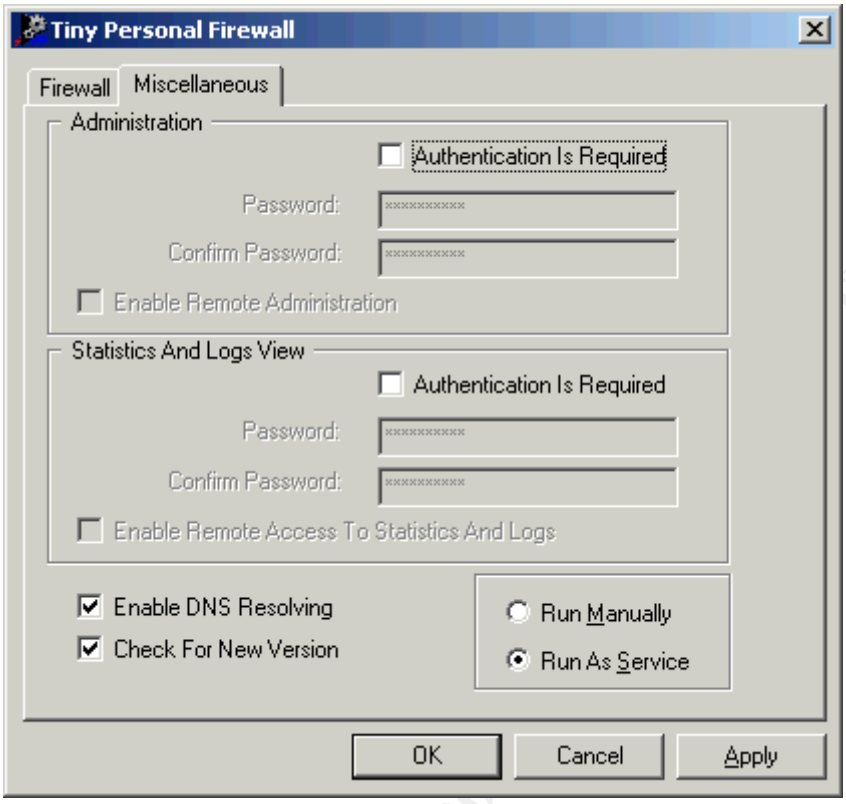
In this settings area, you can choose to log to a file (the default) and/or to Syslog. You can let the firewall know that it is running on a gateway

machine, if your network is configured to process all network requests through this machine. You can also log any packets that are addressed to ports that are currently closed. The 'Custom Address Groups' area is solely for defining IP addresses or IP address ranges that you want to "lump together' for logging purposes.

The 'Application's MD5' tab is used for cryptographic comparison of MD5 Checksums in particular applications. Not all applications will have MD5 checksums associated with them, but for those that do, this is an easy way to make sure that the file has not been tampered with. For those of you unfamiliar with this concept, a one-way **hash** is created for an application by running the MD5 cryptographic algorithm on it once it is created. The value that is generated will always be the same; thus, running the same algorithm on the file at a later time and comparing the two will tell you if the file has changed in the interim. This can alert you to the possible presence of a backdoor or root kit.



12. Finally, the original 'Firewall Administration' screen that you saw after right-clicking the icon in the system tray had one other tab on it: the 'Miscellaneous' tab. On this tab, shown here, you can elect to require password authentication for TPF administration and/or log/statistics viewing, as well as remote administration capabilities on either option. You can also enable DNS lookups for site names, enable/disable TPF checking for updated versions of itself, and choose to run the firewall as a service (i.e. starts up automatically with the computer) or manually (you start it yourself).



List of References

Bass, Steve. “Home Office: Your Second Line of PC Defense.” PCWorld.com. November 2001. URL: http://www.pcworld.com/resource/printable/article/0,aid,62223,00.asp (10 Oct. 2002).

Brown, Bruce and Brown, Marge. “SOHO Security.” Extremetech.com. 27 February 2002. URL: http://www.extremetech.com/print_article/0,3998,a=23325,00.asp (10 Oct. 2002).

CERT Coordination Center. “Home Network Security.” CERT.org. 5 December 2001. URL: http://www.cert.org/tech_tips/home_networks.html (8 Oct. 2002).

Connolly, P.J. “Secure the home office sensibly and easily.” Infoworld.com. 8 March 2001. URL: http://staging.infoworld.com/articles/tc/xml/01/03/12/010312tcsoho.xml?Template=/storypages/printfriendly.html (9 Oct. 2002).

Hassell, Jonathan. “How Firewalls Work.” Security Administrator. 4 May 2001. URL: http://www.secadministrator.com/Articles/Print.cfm?ArticleID=20882 (8 Oct. 2002).

Hassell, Jonathan. “Security Isn’t Just for the Corporate World.” 23 February 2001. URL: http://www.secadministrator.com/Articles/Print.cfm?ArticleID=20026 (8 Oct. 2002).

Hassell, Jonathan. “Three Big Security Problems.” 9 March 2001. URL: http://www.secadministrator.com/Articles/Print.cfm?ArticleID=20225 (8 Oct. 2002).

Kuhn, D. Richard, Frankel, Sheila E., & Tracy, Miles. “Security for Telecommuting and Broadband Communications.” NIST.gov. 14 December 2001. URL: http://csrc.nist.gov/publications/drafts/security_for_telecommuting_and_broadband_communications.pdf (10 Oct. 2002).

NIST. “Security Issues for Telecommuting.” NIST.gov. 15 August 2001. URL: http://csrc.nist.gov/SBC/PDF/NIST_ITL_Bulletin_01-97_Telecommuting.pdf (11 Oct. 2002).

Rogers, Larry. “Yesterday I couldn’t Spell Systems Administrator; Now I Am One!” CERT.org. 17 September 2001. URL: http://www.cert.org/homeusers/ira_sysadmin.html (11 Oct. 2002).

Siepmann, Frank. “SOHO Security Solutions.” NetworkComputing.com. 3 April

2000. URL: http://www.networkcomputing.com/1106/1106ws2.html (11 Oct. 2002).

Last Updated: July 24th, 2017

Upcoming Training

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
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
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
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 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 San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	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
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
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
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
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 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
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor