Global Information Assurance Certification Paper

Guy_Wilcox_GSEC
VPN's & Protocols for Security GSEC option. 1 ver. 1.4
Guy C Wilcox 4/25/2002

Abstract
This document describes Virtual Private Networks (VPN's), with an emphasis on the protocols used to deploy secure VPN's across IP backbones and specifically the public Internet. Various types of VPN's are discussed, as well as their uses, requirements, and the protocols and technologies used in VPN implementation. Current trends in the VPN technologies are discussed also. It is assumed that the audience for this document has some general knowledge of Ethernet and Internet technologies, networking protocols, and network devices. The information contained herein is intended to assist network administrators in the deployment, use, and administration of VPN's, and to increase their awareness of the various security issues involved.

Introduction
In the past few years, Virtual Private Networking has become a very popular method of allowing remote users network connectivity. Leased lines that allow users in remote locations to connect to an organizations network can be expensive, and the costs are usually proportional to the distances involved. The further away the user is from the network he or she is connecting to, the greater the cost of leasing the line. Also the costs for a leased line incur regardless of the amount of the amount of actual usage the line has. The use of VPN's instead of leased lines will cut the costs due to inexpensive connections to the Internet. The cost savings can be realized by any sized organization, and can be a tremendous savings to large organizations. Also adding to the popularity of VPN's is the ability to securely connect remote Local Area Networks (LAN's) to corporate networks. In his book Demystifying VPN author Michael Busby states "VPN's exist and serve a useful purpose primarily because of the existence of the Internet and its enabling protocols, TPC/IP." (*Busby, xi*)

What is a Virtual Private Network?
A Virtual Private Network (VPN) is simply a private network connection within a public network, as shown in figure 1 below. A VPN is a combination of software and hardware that allows remote users such as telecommuters, or a remote LAN to use a public unsecured medium such as the Internet, to establish a secure private connection with a host network. See figure 1 below.

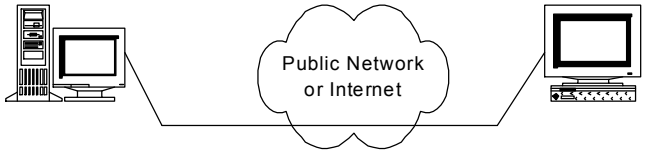

Fig. 1 VPN, a private connection over a public network.

VPN's are not limited to any one particular networking transport technology, and there are various methods of implementing VPN's. They have been built upon TCP/IP, frame relay, X.25 and ATM. Because of the significant cost savings that can currently be realized over the use of leased lines in the setup of VPN's, a large percentage of them are being built over the Internet using TCP/IP and IPsec protocols. (*Busby,2)* Deploying VPN over the Internet allows for virtual private connections to and from almost anywhere in the world. A VPN must provide a high degree security for all data transmitted over it and for any information regarding the users at both ends of the VPN, and the networks or computers at both ends.

The Internet Engineering task Force (IETF) has defined a large number of standards, recommendations, and statements of common practice that are used for communications over the Internet, including VPN standards. To do so the IETF requests input from various working groups and forums. The IETF codes decisions they have made regarding specific protocols and methods of performance into what are called Requests For Comment (RFC). The RFC's are numbered and appear in documents as (RFC 0001) and so on. Any RFC's that the IETF has on its standards track should be considered a standard. Therefore in this document any available IETF RFC's that are listed after a protocol or its acronym can be referred to as a standard and can be further researched through the IETF. The RFC 2764, for example is the "Framework for IP Based Virtual Private Networks". *(Gleeson, 1)*

Three main categories of VPN's

There are three main categories of VPN's. The specific category of VPN is implemented by an organization to address the needs of the organization and a specific group or type of users.

- The first category is Remote Access VPN's. As the name implies, Remote Access VPN's provide users with secure access to a corporate LAN or intranet when they are at remote locations. For example, instead of using an expensive leased line or long distance modem connection to the corporate LAN, the remote user connects to a local ISP and the VPN software on his or her computer sets up the VPN connection with the corporate VPN server across the Internet. Various technologies such as

Digital Subscriber Line (DSL), Integrated Services Digital Network (ISDN), and analog telephony can be used to facilitate a secure connection of remote users, telecommuters and/or branch offices and the corporate intranet.

- Intranet VPN's, the second category, differ from Remote Access VPN's in a couple of ways. Intranet VPN's are setup for offices in different locations to connect to one another using dedicated connections and a shared networking infrastructure. Corporate HQ, and branch offices would possibly use an Intranet VPN. Most Intranet VPN's allow access to authorized users only, and the corporation's security policies would be guiding document for its usage.

- Extranet VPN's, the third category, are used for connections between the corporate employees, their customers, suppliers, and other interested parties using dedicated connections and a shared networking infrastructure. The difference between Intranet VPN's and Extranet VPN's is that the Extranet VPN's allow access to users outside of the corporation. Some restrictions may apply to non-corporate users depending again upon corporate security policies. *(Templeton, 1)*

Three methods of VPN implementation

There are Hardware-based, Software-based, and Firewall-based VPN implementations. There are advantages and disadvantages with the use of any of these three technologies, and the requirements of the organization should be considered carefully while planning VPN.

- The first type of VPN is hardware-based. The hardware-based VPN's use routers to provide VPN functionality, or other devices that were specifically designed for VPN. Usually devices specifically deigned as VPN products are based upon and will only support IPSec. Routers used in hardware-based VPN's still perform the functions required of them as routers along with the extra duties required by the VPN protocols. The router based VPN's are also very secure, and are relatively easy to implement. They can also support various suites of protocols such as IPSec and PPTP, whereas dedicated VPN devices usually only support IPSec protocols. Several vendors including Cisco offer routers useable for the hardware-based implementation.

  Other types of VPN's may be more flexible in operations, but the hardware-based VPN's provide the highest network throughput of all VPN systems. Hardware-based VPN's are generally the more expensive.

- Software-based VPN's are set up in situations where both endpoints of the VPN are not controlled by the same organization or when firewalls between the endpoints are implemented differently. Where performance requirements are not too demanding, software-based VPN's may be the best choice. They are harder to setup and manage in multi-vendor or cross platform settings, because require more familiarity with the OS's and security measures involved. Some of the software VPN packages require routing tables and network addressing schemes that may be difficult to deal with, and very few VPN application vendors supply guidance regarding security.

- Firewall-based VPN's have the advantage of the firewalls security mechanisms, and can satisfy the requirements regarding strong authentication. They also can offer various alarms and extensive logging capabilities. They can be setup to help protect the operating system by removing or stopping un-secure services.

According to a recent article, The State of the VPN gear market, by Tim Greene Network World VPNs Newsletter, 02/25/02,: " Hardware-based VPN gear is starting to take the lead over VPN equipment that is based on software running on general-purpose servers. Greene's article also stated that the following are the findings of a recent study indicating a healthy future for VPN's.

- The total sale of VPN gear worldwide in 2001 was $1.3 billion.

- Projected sales of VPN gear worldwide in 2002 are $2.9 billion.

- Low-end VPN equipment will continue to be more popular than high-end gear for large sites.

(Green, 1)

Security aspects and requirements of VPN's

Corporate data is placed in a high-risk situation when the systems containing or transmitting the data are connected to the Internet, unless they have a strong formal plan in place for securing information and dealing with a variety of threats to it. Organizations with sensitive information to protect must have a well thought out security policy prior to having a presence on the Internet.

"A secure network starts with a strong security policy that defines the freedom of access to information and dictates the deployment of security in the network." *(Cisco ,1)*

Threats to the security of Internet communications include, but are not limited to: data theft, identity spoofing, virus', worms, Denial of Service attacks, buffer overflows, and man-in-the-middle attacks. VPN protocols such as IPSec and PPTP are intended to mitigate several threats to the security of transmitting data over the Internet. The following are requirements of the VPN protocols to secure data communications over the Internet from potential attackers.

- The first requirement of a "Virtual Private Network" and the security of a data transmission is the requirement of privacy or confidentiality. The data and the information regarding the entities at both ends of a network communication or transmission must be removed from the public view. VPN's address this requirement by encrypting transmitted data using state of the art cryptography technologies.

- The number two requirement placed upon VPN's is the requirement of "Authentication". Authentication as it is required of VPN is the act of positively identifying the other end of a communications channel. The use of an authentication header security protocol is just one of the steps taken during VPN communications to verify or authenticate, the origin of a transmission.

- Next is the requirement is to verify the "Integrity" of the data transfer. VPN's data integrity checking mechanisms include the use of key based algorithms to verify that the data has not been tampered with.

As stated earlier, a VPN must provide privacy of data. This is because the Internet and other public networks are not secure and do not have any features that would keep one person from looking at another's information as is travels the Internet. The information to be sent is placed on the Internet in what is called clear text. Data transmitted in clear text can be viewed, modified, and stolen by hackers, script kiddies, or identity thieves, just to name a few. There are several software programs and utilities available, with names like sniff, snoop, and snort that will allow individuals to capture and view data as it traverses the Internet. Tools such as a protocol analyzer can easily be used to view the clear text information as it is transmitted. Even the network diagnostic tools built into modern operating systems can be used collect data and information about systems on the Internet.

Information is sent and received over the Internet, using Ethernet technologies and the TCP/IP protocol stack. To cover the subject in full detail, is beyond the scope of this document, however background information regarding TCP/IP packets and how they are generated for transmitting over an IP backbone, is needed in order to have a point for starting a discussion about data encryption which is used by VPN's to achieve data privacy.

TCP/IP introduction (brief)
TCP/IP is a protocol suite consisting of several network communications protocols, which map to a network communications protocols in the TCP/IP architectural model or protocol stack. The TCP/IP architectural model is based on the OSI model, which divides networking tasks into 7 layers. The TCP/IP architectural model differs from the OSI model by dividing the chores of network communications into 4 layers with dedicated protocols to deal with communications at each layer.

There are six primary protocols associated with the TCP/IP protocol suite. The Transmission Control Protocol (TCP) (RFC 793), a connection-based, transport layer, protocol designed to verify that all packets that are sent from one machine are received by the other. The User Datagram Protocol (UDP), is a transport layer protocol and is similar in function to TCP, but is not connection-oriented and does not verify packet receipt. The Internet Protocol (IP) (RFC 791) performs a number of functions at the internet layer. The Internet Control Message Protocol (ICMP) (RFC 792), operates at the internet layer and is responsible for reporting errors and messages. The Address Resolution Protocol (ARP) is responsible for mapping IP addresses to physical addresses. The Internet Group Management Protocol (IGMP) (RFC 1112), is a protocol and a set of specifications to deal with adding and removing machines from address groups.

The TCP/IP protocol suite supports both connection-oriented and non-connection-oriented networking communications. The suite of protocols handles the details involved in getting reliable and non-reliable communications established between computers, getting the required frames of data transferred between them, and dropping the communications link after the data is transmitted.

Packets and Frames
IP packets are generated by adding header information to the data being sent from the application, as it passes through each layer of a protocol stack, on the way to the medium that physically connects the computer to the Internet. As shown in Figure 2 below

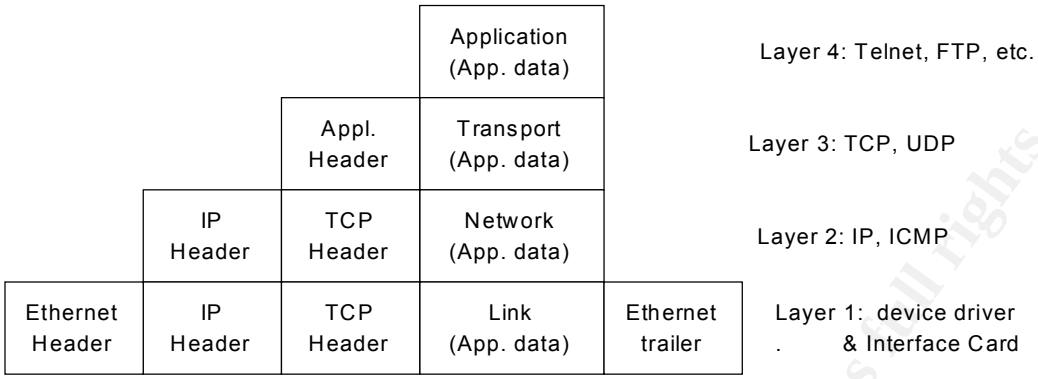

Figure 2. Addition of header information as data is pushed down the TCP/IP stack.

Frames are what packets are referred to during the actual transmission of data over the specific medium. At the destination computer the header information is removed from the packet a layer at a time, until it reaches the application it was sent to.

There is much more to TCP/IP that has not been mentioned here, but the previous information should help the reader understand the following concepts. To learn more about TCP/IP and other related protocols an excellent resource is TCP/IP illustrated, Volume 1: The Protocols. Other references are also listed at the end of this document.

Encryption

One of the key security features of VPN's is that they will provide data privacy over the Internet. This is accomplished by encrypting the data before it reaches the Internet. Encryption is the act of taking the clear text data and scrambling it into what is called cyphertext. The cyphertext is then transmitted over the public Internet and it is secure from man-in-the-middle attacks and form Internet spies. When the cyphertext reaches the recipient the message gets decrypted back into clear text. This processes of encryption and decryption combined form what is called a cryptosystem.

There are two types of cryptosystems; they are called public key and private key cryptosystems. The keys in these systems are encryption algorithms that are applied to the actual text to create cyphertext. Encryption algorithms differ in the number of binary digits that make up their length and the longer they are the harder it is to break their code. Common encryption algorithms are the Data Encryption Standard (DES), Triple-DES (3-DES), and RC4.

Private Key Cryptosystems are symmetric cryptosystems and use the same secret key for both encrypting the data at the originating site and for decrypting the data on the receiving end of the VPN. The use of the same key on both ends of a VPN has a few drawbacks. If the key is stolen anyone with the key can decrypt all of the future data that they can collect that was encrypted using that key or they could decrypt data collected prior to obtaining the key. Therefore keys must be delivered to users where their identity can be verified, and the keys should be replaced periodically to thwart hackers.

Public Key Cryptosystems are asymmetric cryptosystems and use a pair of mathematically related keys. They use a private key that is kept secret and a public key that can be publicly known. The use of two keys is more secure than using just one private key. Two of the public key systems in use today are Diffie-Hellman (DH) and Rivest Shamir Adleman (RSH).

Tunneling

The VPN incorporates a strategy called tunneling to help accomplish secure data transfer. Tunneling is the process of encapsulating an entire packet within another packet and sending it securely over a network. The network understands and knows how to deal with the protocol of the outer packet. The outer packet contains the information regarding the points where the packet enters and exits the network.

There are three basic protocols used to accomplish tunneling, they are the Carrier protocol, the Encapsulating protocol, and the Passenger protocol. The carrier protocol is used by the network, the encapsulating protocol is the protocol that is wrapped around the original data, and the passenger protocol involves the original data.

The use of tunneling has a couple of advantages. You can use encapsulate packets of information that the network or Internet does not support inside the IP packets created for tunneling and send them securely through a tunnel across the Internet. Another possibility is that packets containing non-routable IP addresses can be encapsulated in tunneling IP packets sent across the Internet to extend a private network.

Steps involved to establish a VPN connection are as follows:
First the remote location will request a VPN connection to the local end of the VPN. The authentication process will then be started which can involve strong user verification and authentication. Next the Keys for the session are negotiated as well as other characteristics of the session. The encrypted connection is then established and data can begin to flow between the entities involved.

The most popular VPN architectures are IPSec VPN's, which make up about 70% of the VPN's in use. The advantage IPSec has over other contenders is that it operates at the network layer and can be deployed independently regardless of the applications running on the network. The next in popularity of deployed VPN's which less than 20% of them use PPTP protocols. The remainder of VPN's deployed are similar to applications like Secure Shell, or are proprietary with an architecture based in the application layer.

The IPSec Protocols

Internet Protocol Security (IPSec) (RFC 2401) is a set of extensions to the IP protocol family that take care of encryption and authentication at the transport layer (layer 3). IPSec provides confidentiality, integrity, authenticity, and replay protection through protocols. These protocols are the **Authentication Header (AH)** (RFC 2402), and **Encapsulated Security Payload (ESP)** (RFC 2406). The Authentication Header (AH) is a security protocol that provides authentication and optional replay-detection services. AH is imbedded in the data to be protected. The Encapsulated Security Payload (ESP) is a security protocol that provides data confidentiality and protection with optional authentication and replay-detection services. ESP completely encapsulates user data. AH and ESP can be used together or alone in a VPN. *(Cisco, 7)*

IPSec also provides support for the **Internet Key Exchange (IKE)** (RFC 2409) protocol and for **digital certificates**. The IKE protocol is used to negotiate the services dealing with the exchange of keys and other services required to authenticate peers. Digital certificates contain several unique fields of information that are used to automatically authenticate users or devices without the need to perform a manual key exchange.

IPSec provides two encryption modes, transport and tunneling. In the **transport mode**, only the actual information that the IP packet contains gets encrypted, the original packet headers remain unchanged. This mode has its advantages and disadvantages. An advantage is that only a few bytes are added to each packet, so the bandwidth requirements to transfer files are not significantly increased. A disadvantage is that passing the IP header in the clear allows an attacker to see the source and final destination of the packet. *(Cisco, 8)*

In the **tunnel mode**, the IP packet is encrypted in its entirety, and is encapsulated into a new packet. An IPSec header is then pre-pended to packet then a new IP header is added that contains the address of the destination gateway or router. In this mode a router or a dedicated VPN device at the source performs the encryption and sends the encrypted packet through the IPSec tunnel to the destination's router. The destination's router strips off the headers and decrypts the packet. The router then forwards what has been reverted to the original IP packet, to the final destination. Two major advantages to the tunnel

mode are: The tunnel mode protects against network traffic analysis the an attacker could only determine the tunnels end points with captured transmission data, and not the true source and destination. The second advantage is that the end users' operating systems do not need to be modified for them to enjoy the benefits of VPN. *(Cisco, 8)*

PPTP VPN's

Point-to-Point Tunneling Protocol (PPTP) (RFC 2637) is another TCP/IP protocol that is used in the implementation of VPN's. Microsoft and U.S. Robotics initiated the work regarding the PPTP protocol and their intentions were to a need for dial-up VPN's, as opposed to IPSec which was intended for LAN-to-LAN tunneling. PPTP is an extension of the Point to Point Protocol (PPP) (RFC 2284), a layer 2 protocol that defines point-to-point connections over IP networks. PPTP like ESP encrypts packets and sends them over the Internet to maintain a secure tunnel and virtual WAN connection between computers in different locations.

PPTP encapsulates PPP packets at layer 2, which allows users to send packets that are not specifically IP packets. With PPTP the typical client will be running a Microsoft operating system where the encryption protocol used is Microsoft Point-to-Point Encryption (MPPE). The standard for MPPE is based on RSA RC4 a 40-bit or 128 bit encryption, and is regarded as acceptable but less secure than the 168-bit 3DES that can be used by IPSec *(Marcotte, 1)*

Conclusions:

The basic idea behind VPN's is to gain a secure connection to local computing resources from remote sights. And the implementation of VPN's can be accomplished in a variety of ways, due to the many protocols that VPN's use. I have discussed several of the dozens of protocols in use to accomplish IP networking in a secure manner. The important aspects of assuring a high amount of security with VPN's, including authenticating users, encrypting data, and verifying that the data has arrived at the destination unchanged have also been discussed. There are certainly many more details that are involved in implementing VPN's, in fact there are several books in print that cover the subject in great detail. As stated in this document the authority on this subject is the IETF and the details reside in the various RFC's. Another source with a library of information on the subject is Cisco Systems Inc. Cisco maintains an excellent web site at www.cisco.com, which is a wealth of information regarding networking and internetworking.

Cited References

Busby, Michael "Demystifying VPN" Wordware Publishing, Inc. 2001

Greene, Tim "The state of the VPN gear market" Network World VPN's Newsletter , 02/25/2002
http://www.nwfusion.com/newsletters/vpn/2002/01238883.html

Marcotte, Greg "Protocols serve up VPN security" Network World, 05/31/99
url: http://www.nwfusion.com/newes/tech/0531tech.html

Cisco Systems, Inc "IPSec" White Paper. 07/01/2000
url: http://www.cisco.com/warp/public/cc/techno/ipsecur/ipsec/tech/ipsec_wp.htm

Cisco Systems, Inc. "An Introduction to IP Security (IPSec) Encryption" 07/18/2001
warp/public/105/IPSECpart1.html

Gleeson, B. et. al., Request for Comments: 2764 A Framework for IP Based Virtual Private Networks
http://rfc.sunsite.dk/rfc/rfc2764.html

Templeton, David "Building Virtual Private Networks" Dec 20, 2001 GSEC

Additional References

Stevens, W. Richard "TCP/IP Illustrated Volume 1 The Protocols" 1994 Addison-Wesley Publishing Company

Kosiur, David "Building and Managing Virtual Private Networks" 1999 Wiley Publishers

Napier, Duncan "Administering Linux IPSec Virtual Private Networks" Sys Admin, March 2002
url: www.sysadminmag.com

Cope, James "IPSec: Making the VPN Secure" 02/11/2002
url:http://www.computerworld.com/ciw/Printer_Friendly_Version/0,1212,NAV47_STO68..

Using IPsec The OpenBSD organization
url: http://www.openbsd.org/fav/faq13.html

IP Security Protocol (ipsec) Charter 02/05/2002
url: http://www.ietf.org/html.charters/ipsec-charter.html

"IETF Request For Comments (RFCs)", Virtual Private Network Consortium
url: http://www.vpnc.org/rfcs.html

RFC Hypertext Archive @ sunSITE Denmark
url: http://rfc.sunsite.dk/

Last Updated: May 25th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
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