Global Information Assurance Certification Paper

SSL Remote Access VPNs
Is this the end of IPSec?

Steven Ferrigni

GIAC Security Essentials Certification (GSEC)

Version 1.4b
Option 1

October 22, 2003

Table of Contents

Abstract

Remote Access VPNs, like every other modern technology are continually evolving and improving. Initially nothing more than a server connected to a modem into which remote users dialed, to gain access to a limited number of company resources, they now use broadband connections to allow customers, suppliers, vendors and mobile users access to a vast array of resources from Extranets to Intranets and even classified information.

Until recently IPSec based VPNs were the industry standard on which most companies relied as they provided the reliability and security required to protect sensitive company information. While IPSec continues to be the generally regarded standard for site to site VPNs, SSL remote access VPNs have recently been introduced and are quickly gaining in popularity prompting many to believe that IPSec remote access VPNs are on their way out. This paper looks at the two VPN technologies with respect to remote access, discusses the advantages and disadvantages of each and whether they can co-exist.

Introduction

Many recent technological advances have not only meant a shift toward industrial and retail globalization but also an increase in customer expectation and knowledge. The increase in Internet availability worldwide has enabled consumers to not only become more informed but also bolder in what they expect and what they seek.

All of this has led many companies to look to technology to provide an edge with which and on which to survive and excel. With facilities around the world and vendors, partners and staff spread even wider, the need for reliable and secure communications continues to increase.

This need ultimately led to the advent of remote access Virtual Private Networks (VPNs). That is, networks that provide access to corporate resources safely and securely. According to Cole, Fossen, Northcutt and Pomeranz the definition of a VPN is " a restricted use, logical computer network that is constructed from the system resources of a relatively public, physical network (such as the Internet), often by using encryption and often by tunneling links of the virtual network across the real network." [4] These virtual networks can be anything from a small remote office to a vendor or even a mobile user.

Initially these VPNs relied on expensive dial-up connections however, the increasing availability and decreasing cost of broadband Internet connectivity has led companies to develop Internet VPNs in an effort to provide a more flexible and cost effective solution. Until recently IPSec VPNs provided the best, most robust solution for Internet based connectivity but SSL VPNs are now rapidly gaining in market share, mainly due to the fact that they provide a higher level of flexibility. As a result, many believe that SSL will win out over IPSec and become the industry standard. This paper will review the benefits and issues of each and argue that each technology has its own merits and a combination of both will provide a truly secure and flexible solution.

A Look Back

Before looking at today's two predominant remote access technologies a brief history of remote access VPNs is necessary. When remote access VPNs were first introduced they were originally intended to allow a select few individuals access to a limited number of corporate resources remotely. This was originally done via a dial-up connection whereby the user dialed in to a modem, which was connected to a Remote Access Server (RAS). The user was usually prompted for a User ID and password and if valid, was allowed access to the network. The connection was rarely encrypted since it was believed that this method was inherently secure. Most argued that the only way for a person with malicious intent to intercept the information was to physically tap into the phone line. As technology evolved simple encryption was added so that the information flowing between the remote user and the server was encrypted using a simple algorithm.

This solution worked relatively well as long as the number of users with the ability to dial in remained relatively low. As the number of users increased, the corresponding hardware infrastructure needed to increase in the form of modem pools and multiple servers enabling multiple users to dial in at once. It also meant a considerable increase in operational costs as the number of support calls grew with users who were having modem problems or address resolution problems.

Another issue of these early VPNs was the relatively slow connection speed. For the most part users used regular home phone lines and regular modems, which generally meant average connection speeds of approximately 48 Kbps at best. Some, more serious users had expensive ISDN lines installed at home but this limited the user to one location. For those companies that had users who traveled it also meant very large long distance costs, since users would have to dial the modem pools directly or over a toll free number.

Soon however companies began to see the benefit of allowing broader remote access. Having staff on the road or working from home meant greater productivity and efficiency. Allowing partners and suppliers access to certain corporate resources or an extranet meant a greater working relationship leading to now common industry practices such as Just in Time manufacturing where companies closely monitor the production of their partners and provide necessary parts as required thus reducing the stock that both need to carry. For all of these reasons remote access VPNs grew in popularity. However when considering the cost of communication and support it often outweighed the savings that a VPN provided and so companies looked for other methods to provide VPNs.

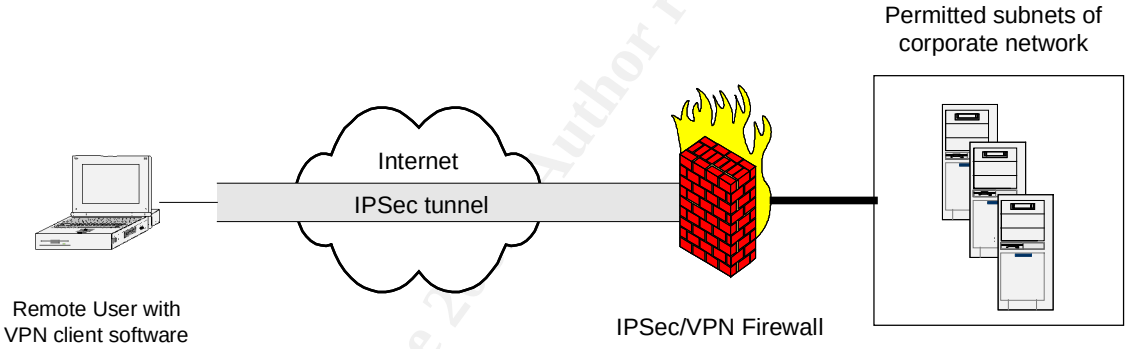
The Internet, with its increasing popularity and availability, provided the ideal solution. With Internet remote access VPNs users simply needed to get a connection to the Internet and they would be able to gain access to the corporate resources they required. Local numbers could be used which reduced communication charges significantly and for those that had broadband connections communication speeds increased significantly. This method of remote access VPN over the Internet raised another more serious issue however – security. Allowing access to confidential and private corporate resources over a publicly accessible medium such as the Internet made a lot of people nervous. As with any network, but especially with a VPN, in order for the environment to be effective it must have robust authentication, strict and controllable access controls and maintain confidentiality. Security of VPNs would need to be increased significantly to give people the level of comfort required to introduce such an environment. According to the IEC, “The TCP/IP protocols and the Internet were not originally designed with security in mind.”[1] As a result many different types of protocols such as PPTP, L2TP and IPSec, were introduced in an effort to ensure security for VPNs. Eventually IPSec became the more widely used because according to the How Stuff Works article, “IPSec provides

enhanced security features such as better encryption algorithms and more comprehensive authentication." [3]

As reliance on VPNs increases people's expectations also increase. With the Internet being available most anywhere today from hotel rooms to cafés, the demand is shifting to allow VPN access from anywhere. Currently IPSec VPNs has some limitations that have made some companies search for alternative solutions. It is primarily for this reason that the SSL VPN was developed and introduced and is gaining popularity. However, the many benefits of IPSec continue to make it a strong and highly popular solution.

IPSec VPNs

As shown by the figure below from the article by Lisa Phifer IPSec VPNs provide access to entire subnets of the corporate network. [5] A user who has the remote VPN client software installed comes through the Internet to the firewall or VPN gateway and initiates a key exchange (IKE). Once the user is properly authenticated a VPN pipe/tunnel is created and the VPN then has the option to run in two modes; tunnel and transport.



In transport mode the transport layer segment of the packet is encrypted while in tunnel mode the entire packet is encrypted, making tunnel the preferred method. The strength of IPSec VPNs lies in the fact that it encrypts packets of information, significantly increasing its ability to provide data confidentiality and integrity. It uses universally accepted cryptography standards such as 3DES, MD5 SHA for encrypting data and authenticating packets. It can use IKE with digital certificates or pre-shared secrets for two-way authentication to ensure that the user is who they say they are. It is for these reasons that IPSec is still the primary choice for site-to-site VPNs but the benefits listed below also make them reliable for remote access VPNs.

Benefits

The biggest benefit of IPSec is that because it operates at the IP layer it provides a lot of flexibility with respect to network configurations and applications. It means that traditional legacy applications can be accessed easily and simply without the need for major development and reconfiguration, using the respective

clients. Applications such as IBM green screen and other mainframe applications can all be run remotely using IPSec VPNs.

This IP layer functionality also means that it provides access to entire subnets of a corporate network, a benefit that network administrators and developers can truly appreciate (although many may consider it a weakness). This is a large benefit for administrators that need to run network administrative tasks such as SSH or Telnet.

When operating in tunnel mode "IPSec encapsulates the original IP data packet with its own packet, thus hiding all application protocol information."[6] This makes it possible to now route usually non-routable protocols such as VoIP, NetBeui and SNA, making it extremely flexible and configurable.

Another benefit is that it provides a work environment that users are familiar with. Since an IPSec VPN is virtually like putting the remote PC on the LAN as if the user were working from the office it provides an identical operating environment. This can cut down on support costs and user frustration. It also means that all work is done locally, making use of the local computing resources and not relying on server resources. As the power of home computers and notebooks increase, an IPSec VPN takes advantage of this power by allowing all applications to run locally thus putting less strain on corporate servers.

An IPSec VPN environment also allows a user to work locally in the event of the unavailability of the Internet. Internet access is not always possible and the fact that the user has all required applications installed locally means they can function until Internet access is possible. Office documents, PowerPoint presentations and email can all be work on locally and then synchronized back to the corporate network when the connection is available.

Once an IPSec tunnel is created through key exchange, multiple connections can utilize it at the same time without requiring additional key exchanges. This results in a performance advantage over its SSL counter part.

One final benefit is that VPN client software now has the ability to enforce certain requirements that protect the overall network from malicious intent. The client software can detect and require the presence of antivirus and personal firewall software. It can check the operating system version and which patches have been installed or are required. This protects the network from potential worms, viruses, Trojans and hackers. If any or all of the requirements are not met then access is denied.

Issues

The biggest drawback of the IPSec VPN is that it requires client VPN software to be installed on the remote PC or notebook. This practically eliminates the holy grail of "anywhere access" that many companies and users are seeking. It

means that Internet Kiosks and cafés cannot be used for VPN access and that anyone who is permitted to access the VPN must have either a corporate owned notebook or must be using a home computer. The client software is also the cause of the majority of support calls as users frequently have problems configuring the client. While this feature ensures a secure connection it limits the access significantly and is the main reason that SSL VPNs were developed.

The second major drawback of IPSec, according to many, is the fact that it provides access to an entire subnet within the corporate network. This means that the client PC can potentially be used as a vehicle into the network by a hacker. If the client PC becomes infected with a Trojan or virus or is being operated via some remote control software it could potentially spread to the entire internal network or give unauthorized access to malicious users. To combat this IPSec vendors have begun implementing clients that look for the presence of current antivirus software and updated operating systems. Many have also integrated personal firewalls with centrally managed rules. All these features significantly mitigate the risk of intrusion however the possibility still exists.

Another issue of IPSec VPNs is that since the connection comes through the firewall, it requires reconfiguration of firewall policies and may require the opening of ports on the firewall. While this reconfiguration is usually not complicated it can be depending on the number of users and the type of access required. The opening of ports on the firewall also presents an increased security risk as it opens up another door through which malicious users enter. Network address translations (NAT) are often required so that users can access internal resources since these resources often have non-routable, proprietary IPs. These NAT tables can become complex as the number of different VPNs increase.

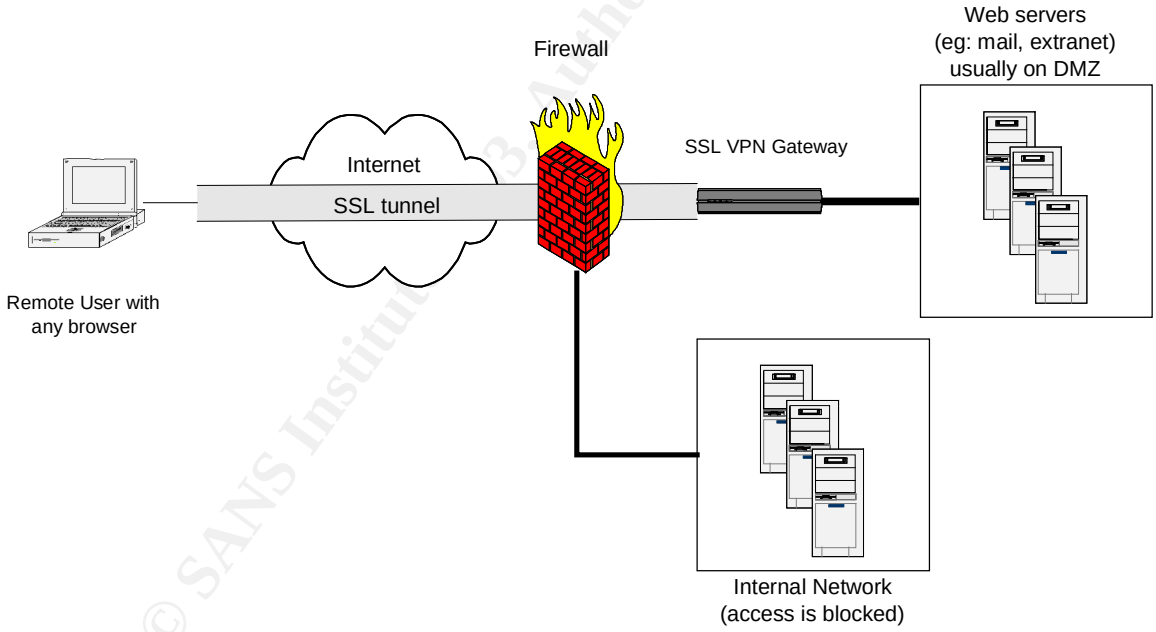
Also, the interoperability between vendors is virtually non-existent, meaning VPN clients from one vendor are not compatible with other VPN appliances. This could be problematic for users who need to connect to different VPN sites that use different VPN gateways. Business partners and consultants may need to access a multiple number of VPNs making configuration a nightmare or even impossible. Also many clients do not have versions that run in multiple operating systems such as Unix, Mac and Linux.

Access control can also be an issue with IPSec VPNs since they rely primarily on network access controls. A VPN gateway is solely responsible for creating the VPN tunnel with the client. Once the tunnel is created the information that passes through is not reviewed for any type of user rights or permissions, it is only encrypted. The permissions and user rights are governed by whatever controls the network. In a Windows environment group policies are applied as if the user was working at the office.

Despite the above stated issues, IPSec is currently the most secure VPN solution available especially when deployed on PCs/notebooks for which the company can be responsible. The ability to dictate the requirement of current antivirus and personal firewall software and to ensure that operating systems are patched virtually eliminates the risk of malicious intent. The requirement of the VPN client software further lowers the risk of breach. When pre-shared secret keys are used in conjunction with two-factor authentication security and data integrity is second to none. Having said that however, the client requirement severely limits accessibility to a limited number of computers and does not provide truly anywhere access, a feature which SSL VPNs can boast about.

SSL VPNs

As already stated above, SSL VPNs were born from the user community's want for VPN access from anywhere at any time. Because of the client requirement IPSec VPN are not able to provide that flexibility and so along come SSL VPNs. Like IPSec VPNs, SSL VPNs use the latest industry accepted standards of encryption and key exchange such as 3DES, MD5 and SHA. As the figure below, based on that by Phifer shows, SSL VPNs provide access to web based applications and not the internal network. [6] The web servers are usually sitting in the DMZ zone of the firewall thus protecting the internal networks.



All browsers have SSL inherently built into them making this type of VPN operating system or browser type irrelevant. It is primarily for this reason that SSL VPNs are gaining in popularity but for all the foreseeable benefits it also has some issues that need to be considered.

Benefits

As already stated the primary benefit of an SSL based remote access VPN solution is that there is no client required necessarily[1]. For web-enabled applications such as mail or intranet a simple HTTPS connection to the web server is all that is required to access those services. This significantly increases the flexibility of the VPN solution as now these types of services can be accessed from anywhere in the world at anytime. Users can be at kiosks in the airport or at Internet cafés around the world and have access to the resources to which they are authorized through the VPN. Since most web-enabled applications such as Outlook, Exchange and Lotus Notes already support SSL there is very little configuration required. This also potentially reduces the cost of implementing and supporting a VPN. There is no client software to purchase and the support time is reduced from 2 hours per year per user to less than .5 hours per year per user as reported by Netilla Networks. [2]

Another benefit is that because SSL is built into all of the leading browsers, the SSL VPN is OS and browser independent. That is, users can access the VPN regardless if they are using a Unix or a Mac machine and regardless of if they use Internet Explorer or Mozilla. All of this versatility means that end users are comfortable with the software and nothing new is forced on them. In addition, the fact that an SSL connection is all that is required also means that the VPN is device independent as well. Web-enabled phones and PDA's can now also access the VPN provided they have and Internet connection.

SSL uses port TCP/443, which is normally already opened on the firewall to the DMZ. This means that SSL has the benefit of not requiring any configuration changes to firewalls. NAT tables are also not required as all information is passed via the browser and in not IP specific.

Since SSL does not allow access to subnets the danger of Trojans, viruses and malware being able to access internal resources is significantly reduced. It does not completely eliminate the risk of malicious intent but does goes a long way to reducing it. As such, the importance of ensuring that the remote PC is "clean" is also reduced.

Most SSL VPN vendors have incorporated features that ensure the PC is cleaned upon logout. Once the session is closed, cookies are deleted, any caches are removed and all traces of the VPN connection are deleted. This ensures that someone cannot sit at the PC once the authorized user has left and re-initiate a session. This is an important feature because presumably the PCs that are located at kiosks or cafés cannot be trusted and may contain key loggers or other malware.

[1] A client may need to be downloaded, usually through Java or ActiveX. See issues section.

Issues

The primary issue with SSL VPNs is that it only really provides VPN access to web-enabled applications. For legacy systems such as IBM green screens or mainframe, enabling access across an SSL VPN would require many hours of development if it were even feasible. It is also difficult for administrators to gain low-level access to run commands such as SSH or Telnet. While some vendors are working on providing such access it still requires the download of a thin client of some form. This download usually consists of a Java applet or ActiveX component that is loaded within the browser. Many Internet terminals at kiosks or cafés block the downloading and running of these types of applets as they are the primary vehicle for the spreading of malware. As such the running of these applications is not possible.

Another issue is that multiple key exchanges may be required during one session. This slows performance of the web server due to the load of performing constant SSL. One solution has been to introduce an SSL gateway or accelerator but his increases the costs of implementation.

Because there is no control over the remote computer, true security can always be questioned. As Checkpoint states, while many SSL servers can send NO CACHE Meta Tags to the client there is no guarantee that it will be honored by the client. [6] This may potentially leave traces of session information on the remote computer that may possibly be used to exploit the VPN. Some SSL vendors have developed technology similar to IPSec clients whereby they are able to check for and require personal firewall or antivirus software, however these are difficult to enforce on publicly accessed terminals.

The fact that SSL VPN provides browser-based access to applications means that Internet access is always required. If a mobile user does not have access to the Internet then he cannot work offline. Unlike IPSec where the applications were loaded locally SSL VPN applications are not local. This may mean a lack of productivity in the event of no access.

Despite all of the issues, SSL remote access VPNs ultimately provide what the end users crave and that it access from anywhere. It is for this benefit alone that many believe that it will become the dominant technology.

Which is Better?

With each having its benefits and issues, knowing which to choose for a VPN solution really depends on the requirements of a company. Both utilize robust security protocols and methods and the issues can be mitigated somewhat depending on the environment. If the company has a vast number of mobile users that require access to portal based web applications or email access then perhaps an SSL solution would be the better fit. If a small company needs to provide its AS/400 developers access from home for after hours support then IPSec would be the way to go. For most companies the overriding factor in

choosing one over the other is cost. As many of the SSL vendors are quick to point out, an SSL solution provides the most cost effective method for the implementation of a VPN especially in large organizations and when support costs are factored in. With the amount of support time estimated to be over four times greater per person per year for IPSec VPNs, a large user group would mean enormous support costs. Support gets even more difficult if a company tries to have control of the computers that access the VPN, as it would like to have for IPSec. However, for small companies that have a limited number of users that access the VPN over company owned notebooks an IPSec solution would be the more cost effective even when looking at the Total Cost of Ownership (TCO).

Conclusion

The inherent security of IPSec VPNs has been tried and tested and has withstood the test of time, which is the main reason that it will continue to be the primary solution for site-to-site VPNs. However the functionality that SSL remote access VPNs cannot be outweighed and vendors are confident that they too will stand the test of time. As the number of legacy applications continues to decline and the number of web-based applications continues to increase SSL will slowly become the primary solution for VPN access. However, the layer 3 encryption methodology of IPSec will always be considered the more secure and versatile. As such I believe that the two solutions will continue to co-exist for a long time to come. Many vendors such as Cisco, Checkpoint and Nortel are beginning to realize that it is unwise to throw all of their eggs in one basket and, thus, are beginning to offer a solution that utilizes a combination of the two. They are suggesting that the best solution offers an IPSec VPN to those users that require low-level access and from those computers over which the company has control. They are then using an SSL VPN solution to provide simple email and extranet access to staff, customers and vendors that require only web-based access. In this way costs are kept low as support calls remain low and access is granted to all users how and when they want.

List of References

1. "Virtual Private Networks (VPNs)." 2003. URL: http://www.iec.org/online/tutorials/vpn (Sept 2003)

2. Netilla Networks Inc. "A Functional and Cost Comparison of VPN Solutions: SSL vs. IPSec." 2002. (Aug 2003)

3. Tyson, Jeff. "How Virtual Private Networks Work." 2001. URL: http://www.howstuffworks.com/vpn.htm (Sept 2003)

4. Cole, E. AND Fossen, J.AND Northcutt, S. AND Pomeranz, H. SANS Security Essentials with CISSP CBK, Volume 2, Version 2.1: The SANS Institute, 2003. A126 – A148.

5. Phifer, Lisa. "Tunnel Visions: How do SSL VPNs match up with their older cousins?" Information Security Magazine. August 2003 (2003): 31 - 43

6. Checkpoint Software Technologies Ltd. "IPSec Versus "Clientless" VPNs for Remote Access." 2002. (Sept 2003)

7. Dell, Joseph. "A Primer on SSL-based VPNs." 2003. (Sept 2003)

8. Laubhan, Jeff. "SSL-VPN: Improving ROI and Security of Remote Access. Secure Authentication and Access to your Critical Resources." (Aug 2003)

9. Greene, Tim. "SSL Catching up to VPNs in Popularity." 18 Feb 2002. URL: http://www.nwfusion.com/news/2002/130001_02-18-2002.html (Oct 2003).

10. Smith, Tom. "VPN Case Study: Companies Tap Secure As-Needed Connections." 30 May 2002. URL: http://www.internetweek.com/story/showArticle.jhtml?articleID=6406308 (Sept 2003)

11. Janowski, D. AND Sarrel, M. "Improving Performance and Availability of SSL VPN Solutions." 19 Aug 2003. URL: http://www.pcmag.com/print_article/0,3048,a=45228,00.asp (Oct 2003)

12. Ribeiro, John. "Aventail Secures Edge of SSL VPN Network." 11 Sept 2003. URL: http://www.nwfusion.com/news/2003/0911aventsecur.html (Oct 2003)

Last Updated: September 24th, 2017

Upcoming Training

SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
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
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague Summit & Training 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VA	Oct 14, 2017 - Oct 21, 2017	Live Event
SANS Tokyo Autumn 2017	Tokyo, Japan	Oct 16, 2017 - Oct 28, 2017	Live Event
CCB Private SEC401 Oct 17	Brussels, Belgium	Oct 16, 2017 - Oct 21, 2017	
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201710,	Oct 23, 2017 - Nov 29, 2017	vLive
San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
Community SANS Vancouver SEC401^	Vancouver, BC	Nov 06, 2017 - Nov 11, 2017	Community SANS
Community SANS Colorado Springs SEC401~	Colorado Springs, CO	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS St. Louis SEC401	St Louis, MO	Nov 27, 2017 - Dec 02, 2017	Community SANS
Community SANS Portland SEC401	Portland, OR	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Dec 04, 2017 - Dec 09, 2017	Community SANS
SANS Austin Winter 2017	Austin, TX	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Bangalore 2017	Bangalore, India	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201712,	Dec 11, 2017 - Jan 24, 2018	vLive