Global Information Assurance Certification Paper

"Securing the Internal Network from the Internet Perimeter with a PIX Firewall: Another Layer of Protection"

Naeem Qasim
March 10, 2001

Introduction:

Clients often desire to secure their internal network from the Internet perimeter. This will initially lead to a discussion about firewalls one of the defense in depth methods to secure internal information. " The Cisco PIX (Private Internet Exchange) Firewall provides this type of layer of protection from the Internet Perimeter. The PIX Firewall is a stateful firewall that delivers high security and fast performance to corporate networks. A stateful packet filtering firewall controls the flow of Internet Protocol traffic by matching information contained in the headers of connection-oriented or connectionless IP packets against a set of rules specified by the firewall's administrator". ("Cisco Secure PIX Firewall Series – Product Overview"). The stateful approach to security is regarded by the industry as being far more secure then the stateless packet screening approach. The PIX Firewall provides full protection that completely conceals the architecture of an internal network from the outside world.

This paper will illustrate how to implement a PIX Firewall in order to secure the internal network from the Internet. This will focus on the security features of the PIX Firewall and how to design and configure the PIX into an environment.

Skill Requirements:

In order to implement a PIX Firewall, an individual should have hands on experience configuring, downloading and upgrading Cisco IOS software. A status of junior level System Administrator is recommended. It is also important for the individual to have a moderate level of understanding regarding security features.

System Overview:

The PIX forms a boundary between an internal protected network and an external unprotected network. All traffic between the internal and external networks must flow through the PIX to maintain security. The external network may be accessible to the Internet and may contain systems that provide services such as HTTP, FTP, SMTP (electronic mail), and Telnet. The PIX selectively routes information between internal and external networks according to rules established by an authorized administrator. Administration can take place by authorized administrators on NT workstation or on other operating systems such as Unix. After the authorized administrator has configured information flow rules, the PIX limits connections between the networks to only those which are authorized. According to Cisco IOS Network Security written by Cisco Systems Inc., the security features provided by the PIX include the following:

- Adaptive Security Algorithm – implements stateful connection control through the firewall.

- Global and Nat statements – Global and Nat commands are used to control the internal systems can establish connections to the external network. By default, whichever hosts can initiate outbound connections can use all services during the outbound connection. The authorized administrator is able to restrict outbound connections in the following ways:
  (1) Deny or permit access to certain services
  (2) Restrict or permit access from an inside address or access to an outside address

- Access-List and Static commands- allow connections from the outside network to the inside network. The authorized administrator uses the static command to specify the IP addresses that are visible on outside interface for users to obtain access to. The access-list command specifies which services users can access on the Internal hosts.

- System Log Messages – error and informational audit records are captured and stored for review by the authorized administrator. Audit records are stored on the NT Workstation in two separate types of files: event log and syslog files.

- Security Administration – a console interface is provided to allow restricted security administration functions. The authorized administrator manages the PIX from a workstation on from the console port. Security administrative functions are implemented on the PIX Firewall and on the workstation.

- Identification and Authentication – all administrators must identify and authenticate themselves before performing any security relevant action. These individuals must log into the workstation or the PIX Firewall console before making any security changes. (Cisco Systems, Inc.)

Before configuration takes place, it is important to have a moderate level of understanding regarding the security features discussed above. It should also be kept in mind that all traffic between the internal and external networks must flow through the PIX to maintain security.

PIX Firewall Security Policy:

The PIX firewall which enforces filtering rules established by an authorized administrator for control access to the networks. The security policy enforced by the PIX addresses four areas: information flow control, identification and authentication, audit, and security administration. The basic objective of the information flow control policy is to limit services originating from either the internal or the external networks through the firewall based on the firewall configuration. The PIX Firewall's Adaptive Security

Algorithm (ASA) mechanism is used to implement the information flow control security policy. This mechanism allows a stateful packet filtering approach. Every inbound packet is checked against the ASA and against connection state information in memory. Relationships and rules are based on interface pairs. Each interface is assigned a security level in the range 0-100 where 100 is the most secure and 0 is the least secure. Interfaces with the same security level cannot communicate. The interface of the protected network (internal) is assigned a security level of 100; the interface of the unprotected network (external) is assigned a security level less than 100. "The ASA mechanism controls the establishment of connections from one network to another as identified by the security levels between interfaces. The ASA mechanism follows these ASA security interface standards.

- No packets can traverse the PIX Firewall without a connection/state.
- Outbound connections/states are allowed, except those specifically denied. An outbound connection/state is one where the Originator client is on a higher security interface/network than the receiver/server.
- Inbound connections/states are denied, except those specifically allowed by access-list. An inbound connection/state is one where the originator/client is on a lower or equal security interface/network than the receiver/server.
- All attempts to circumvent the previous rules are dropped and a message is sent to the Syslog server. (Cisco Systems, Inc.)

The inherent ASA basic rules for information flow are as follows:

- Allow any TCP connection that originates from the inside network.
- Permit TCP packets from the outside network that are return packets for an existing outgoing connection.
- Drop and log attempts to initiate TCP or UDP connections from the outside network to any IP address for an existing connection.
- Drop and log source routed IP packets from the outside network that are sent to any IP address for an existing connection.
- Drop ping requests silently to IP addresses for an existing dynamic connection.
- Answer, via the PIX Firewall, ping requests directed to static connections.
- Allow any UDP connection that originates from the inside network.
- Drop and log all other packets received on the outside interface.
- UDP connection objects are timed out based on a configurable scheduling frequency timer, started when the connection object is created.
- TCP connection objects are timed out based on a configurable millisecond clock timer, started when the connection object is created.
- Drop packets that arrive on the outside interface with a source IP address on the inside network". (Cisco Systems, Inc.)

After the authorized administrator creates the default PIX configuration as specified in the design stages, the PIX Firewall rejects all connections from the internal network to the unprotected, external network and any connections inbound from the external network. The authorized administrator using the access-list and static commands can

modify this default information flow policy. All decisions on requests for information flow are audited. The PIX supports one type of user, the authorized administrator. The authorized administrator is restricted to an administrator role to perform security administration of the PIX. The authorized administrator must identify and authenticate himself or herself to the PIX before performing any security relevant action. The security administration capabilities provided by the PIX include setting information flow security policies. Assigning users to the authorized administrator role; modifying the time and date. Managing the audit trail. As well as backup and recovery. Management of the audit trail and user accounts is audited.

Designing the PIX Firewall:

The design phase involves gathering information based on the current and future network infrastructure. The first phase is to come up with a conceptual design of the network (see appendix A). The diagram is based on an actual environment and all IP have been changed to protect the client. In the design, the PIX Firewall is placed between the perimeter router and the internal network. The PIX traditionally contains three interfaces, but it may include as many as six interfaces. The diagram (see appendix A) reflects two PIX Firewalls. The primary PIX has three interfaces, and the secondary PIX acts as a fail over to the primary. The outside interface of the primary PIX Firewall (starting from the left most interface - ethernet0/0) is connected to the Internet perimeter router. The second interface on the primary PIX Firewall is connected to the internal network. The third is linked to the demilitarized zone (DMZ). Finally, for the primary and secondary firewall to work in conjunction with one another, they are connected at the serial interface for fail over to take place in the unlikely event the primary firewall goes down. The secondary PIX Firewall holds the copy of the configuration of the primary PIX and is never in control until it detects that the primary PIX Firewall is not responding to its ping test.

The next phase is the most important in bringing any firewall to an environment. A site survey should be performed to evaluate what services already exists, what services are prohibited and what new services are needed. After deciding what services are allowed, the access-list is used to control the services to the external network, the internal network and the DMZ. This is imperative in defining a secure network. The services that need to be provided and the level of risk tolerable determine the level of security of the network. There is a DMZ in the design, which contains an external DNS, e-mail relay, web server and logging server. Some of the most predominant protocols and services that travel the Internet must be allowed to the DMZ, such as TCP, DNS, FTP, HTTP, HTTPS, SMTP, and SSH. The complete list of services that the Firewall must provide or deny will contribute to a superior configuration of the PIX Firewall. (Chapman and Zwicky)

The last phase is to obtain approval of the design and move forward with plans to implement the firewall. Before bringing in and configuring the PIX Firewall a checklist of items should be approved. The list should include checking for the proper IP addresses for each of the interfaces on the PIX, verifying the services deemed appropriate for the

security policy, defining what the firewall will allow or disallow, and resolving any other issues that might prevent a successful deployment.

Configuration of the PIX:

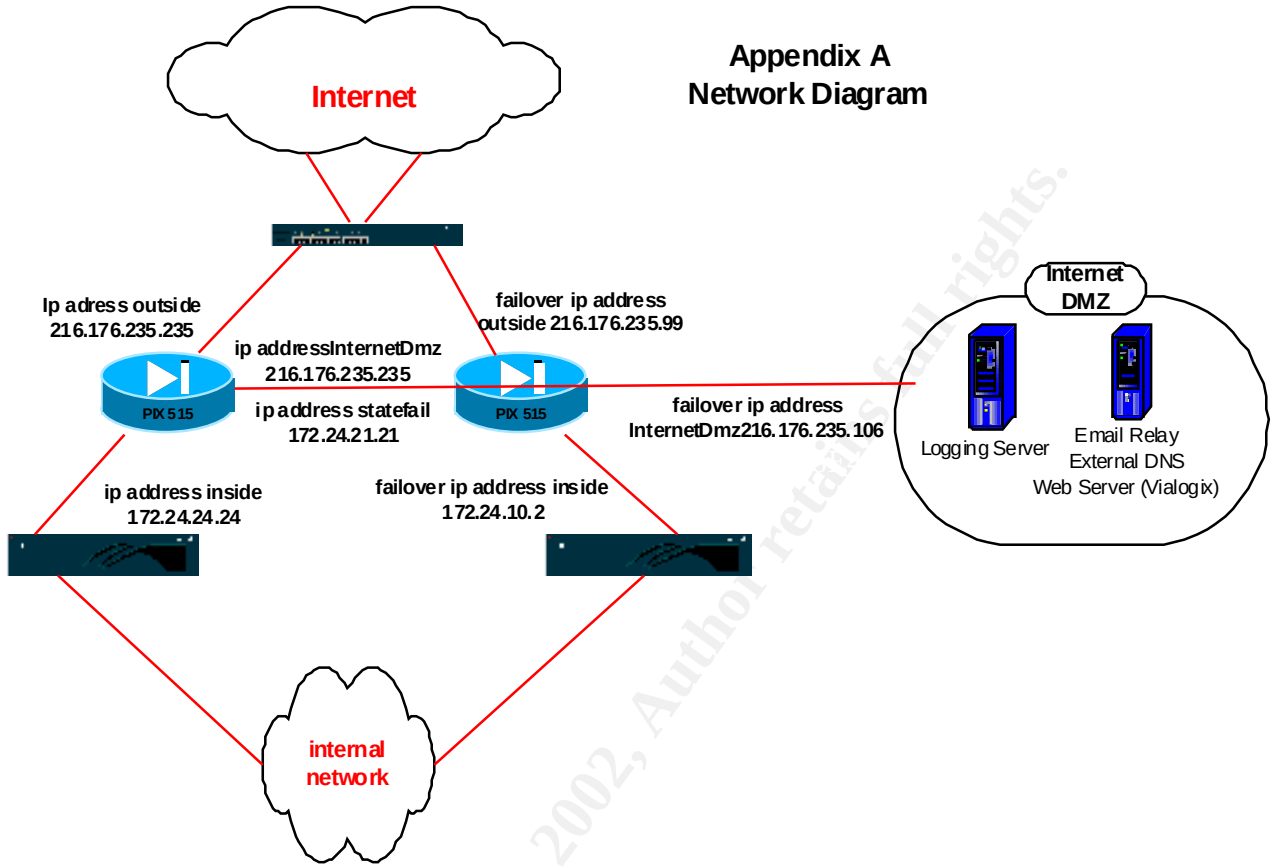
The configuration of the firewall begins by connecting to the console port of the PIX and using HyperTerminal to view the PIX Command Line Interface. As the PIX is booting up, the latest IOS version of the PIX can be viewed on the screen. The most current IOS version should read 5.3(1) ("Installing a PIX Firewall- Upgrading from a Previous Version, Step 1- Get a Console Terminal"). The initial command, the nameif command, assigns a name to an interface and sets the security level of each interface, which is portrayed by Appendix B, the PIX configuration page based on the design requirements. By default, the ethernet0 interface is called outside and has a security level of zero. The ethernet1 interface is called inside and has a security level of 100. Recall that the inside interface will have a security level of 100 and that the outside interface will always have security level of 0. The third interface must also be given a name such DMZ and a security level of 50. Next each interface must be provided with a proper IP address, including the serial interface of the primary and secondary PIX Firewall. An access-list and static statements for communication need to be created between a lower-level security interface and a higher-level security interface. This is when the planning of what services allowed and disallowed will guarantee a successful configuration. The importance of doing a preliminary site survey cannot be stressed enough. The next step is to create global and NAT statements for gaining access between a higher security interface (inside) and a lower security interface (outside). After the addition of the access-list, static, global and NAT commands, use the logging command to begin using the syslog server. ("Firewalls Networking for E-Commerce") This will assist in the detection of any firewall policy violations, which in turn will help to detect any holes in the firewall configuration. Firewall logs can be an additional measure for intrusion detection purposes. These logs will be of importance when tracking a security incident. Finally, add a route statement for preparing the router to work with the PIX Firewall.

Configuration of the PIX Firewall is essential. It is important to verify that the configuration is working properly and also beneficial to perform proactive testing in the attempt to gain access to network. Third party tools such as Nmap can be used to probe the defense of the network. These tools can also provide insight into the configuration and may be able to find vulnerabilities that were previously unknown.

Summary:

A properly configured PIX Firewall can safely insulate a company's trusted internal networks from an unprotected external network. The PIX Firewall can minimize security risk, though it is not the single solution for security. I have implemented PIX Firewalls in many environments and have found this form of security to be very stable and easily manageable for System Administrators. Through continuous testing and monitoring of the PIX Firewall for vulnerabilities and threats, a secure environment can be maintained.

Appendix A
Network Diagram



Appendix B
Pix Config

```
write mem

Building configuration...

Cryptochecksum: bd7483f9 8cecd700 0db28d29 572f9f1a

[OK]


SANS-PIX-1(config)# write t

Building configuration...

: Saved

:

PIX Version 5.3(1)
(To set the interface with a name and security level)
nameif ethernet0 outside security0

(To set the interface with a name and security level)
nameif ethernet1 inside security100

(To set the interface with a name and security level)
nameif ethernet2 InternetDmz security50

(To set the interface with a future name and security level)
nameif ethernet3 pix/intf3 security15

(To set the interface with a future name and security level)
nameif ethernet4 pix/intf4 security20

(To set the interface with a name and security level; this is interface with
fail-over permission)
nameif ethernet5 statefail security25

enable password Q.yYzhiOnjGemcpD encrypted

passwd 2KFQnbNIdI.2KYOU encrypted

(Creating the name of the host)
hostname SANS-PIX-1

(To enable ftp feature)
fixup protocol ftp 21

(To enable http feature)
fixup protocol http 80

(To enable h323 feature)
fixup protocol h323 1720
```

(To enable rsh feature)
fixup protocol rsh 514

(To enable smtp feature)
fixup protocol smtp 25

(To enable sqlnet feature)
fixup protocol sqlnet 1521

(To enable sip 5060 feature)
fixup protocol sip 5060

names

(Permits inside clients to communicate with the following protocol on the outside and certain host inside can only communicate with restricted protocol)
access-list inside permit tcp 172.24.10.0 255.255.255.0 any eq www

access-list inside permit tcp 172.24.10.0 255.255.255.0 any eq telnet

access-list inside permit tcp 172.24.10.0 255.255.255.0 any eq 443

<--- More --->

access-list inside permit tcp host 172.24.24.241 any eq smtp

access-list inside permit tcp host 172.24.24.242 any eq smtp

access-list inside permit udp 172.24.10.0 255.255.255.0 any eq domain

access-list inside permit tcp host 172.24.10.20 any eq ftp

access-list inside permit udp host 172.24.10.20 any eq 23

access-list inside permit udp host 172.24.10.21 any eq 21

access-list inside permit udp host 172.24.10.21 any eq 23

access-list inside permit udp host 172.24.10.22 any eq 21

access-list inside permit udp host 172.24.10.22 any eq 23

access-list inside permit udp host 172.24.10.22 any eq 1221

access-list inside permit udp host 172.24.10.22 any eq 1421

access-list inside permit udp host 172.24.10.23 any eq 21

access-list inside permit udp host 172.24.10.23 any eq 23

access-list inside permit udp host 172.24.10.23 any eq 1221

access-list inside permit udp host 172.24.10.23 any eq 1421

access-list inside permit udp host 172.24.10.24 any eq 21

```
access-list inside permit udp host 172.24.10.24 any eq 23

access-list inside permit udp host 172.24.10.25 any eq 21

access-list inside permit udp host 172.24.10.25 any eq 23

access-list inside permit udp host 172.24.10.26 any eq 23

access-list inside permit udp host 172.24.10.27 any eq 23

access-list inside permit icmp any any

access-list inside permit ip host 172.24.10.201 any

access-list inside permit tcp any any eq ftp

<--- More --->
```

(Permits outside clients to communicate with the following restricted protocol in the dmz host)

```
access-list outside permit tcp any host 216.176.235.107 eq smtp

access-list outside permit udp any host 216.176.235.107 eq domain

access-list outside permit tcp any host 216.176.235.10 eq ftp

access-list outside permit tcp any host 216.176.235.10 eq www

access-list outside permit icmp any any
```

(Permits client to communicate to dmz and data is forwarded from the PIX to the syslog)

```
access-list InternetDmz permit tcp host 216.176.235.107 host 172.24.24.241 eq
smtp

access-list InternetDmz permit tcp host 216.176.235.107 host 172.24.10.12 eq
smtp

access-list InternetDmz permit udp host 172.24.1.1

access-list InternetDmz permit udp host 216.176.235.107 any eq domain

access-list InternetDmz permit icmp any any

pager lines 24
```

(logging to syslog server)

```
logging host 172.24.1.1

interface ethernet0 auto

interface ethernet1 auto

interface ethernet2 auto
```

```
interface ethernet3 auto

interface ethernet4 auto

interface ethernet5 auto

mtu outside 1500

mtu inside 1500

mtu InternetDmz 1500

mtu pix/intf3 1500

mtu pix/intf4 1500

mtu statefail 1500

<--- More --->
(To set the outside address of the PIX Firewall)
ip address outside 216.176.235.235 255.255.255.248

(To set the inside address of the PIX Firewall)
ip address inside 172.24.24.24 255.255.255.0

(To set the InternetDmz address of the PIX Firewall)
ip address InternetDmz 216.176.235.235 255.255.255.248

ip address pix/intf3 127.0.0.1 255.255.255.255

ip address pix/intf4 127.0.0.1 255.255.255.255

(To set the statefail address of the PIX Firewall)
ip address statefail 172.24.21.21 255.255.0.0

ip audit info action alarm

ip audit attack action alarm

failover

failover timeout 0:00:00

failover poll 15

(To set the fail-over ip address of each interface)
failover ip address outside 216.176.235.99

failover ip address inside 172.24.10.2

failover ip address InternetDmz 216.176.235.106

failover ip address pix/intf3 0.0.0.0

failover ip address pix/intf4 0.0.0.0
```

```
failover ip address statefail 172.24.2.2

failover link statefail

arp timeout 14400

(Give global address for the internal clients on the internet)
global (outside) 1 216.176.235.100 netmask 255.255.255.255

(To perform NAT to inside)

nat (inside) 1 0.0.0.0 0.0.0.0 0 0

nat (InternetDmz) 0 216.176.235.104 255.255.255.248 0 0

(To let communication from a high security to low security interface)
static (InternetDmz,outside) 216.176.235.107 216.176.235.107 netmask
255.255.255.255 0 0

<--- More --->

(To let communication from a high security to low security interface)
static (inside,InternetDmz) 172.24.10.0 172.24.10.0 netmask 255.255.255.0 0 0

(The command binds access-list to the access-group)
access-group outside in interface outside

access-group inside in interface inside

access-group InternetDmz in interface InternetDmz

(Route traffic from the PIX through router)
route outside 0.0.0.0 0.0.0.0 216.176.235.97 1

timeout xlate 3:00:00

timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323 0:05:00
sip 0:30:00 sip_media 0:02:00

timeout uauth 0:05:00 absolute

aaa-server TACACS+ protocol tacacs+

aaa-server RADIUS protocol radius

no snmp-server location

no snmp-server contact

snmp-server community public

no snmp-server enable traps

no floodguard enable

no sysopt route dnat
```

```
isakmp identity hostname

telnet timeout 5

ssh timeout 5

terminal width 80

Cryptochecksum:bd7483f98cecd7000db28d29572f9f1a

: end

[OK]

SANS-PIX-1(config)#
```

Bibliography

Cisco Systems, Inc. Cisco IOS Network Security**.** Indianapolis, IN: Macmillan Technical Publishing1998. Volume1 and Volume 2.

"Installing a PIX Firewall- Upgrading from a Previous Version; Step 1- Get a Console Terminal." http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v50/config/config.htm (1 Mar. 2001).

"Firewalls Networking for E-Commerce." January 1997. URL: http://www.cs.dal.ca/~eem/6016/talks/firewalls/sld030.htm (20 Mar. 2001).

"Cisco Secure PIX Firewall Series- Product Overview." March 27, 2001. URL: http://www.cisco.com/univercd/cc/td/doc/pcat/fw.htm - ov (20 Mar. 2001).

Chapman and Zwicky. Building Internet Firewalls. First Edition. Sebastopol, CA: O'Reilly and Associates, 1995. pp. 342-346

Stevens, Richard. TCP/IP Illustrated, Volume 1 The Protocols. Reading, MA: Addison-Wesley, 1994.

Last Updated: July 26th, 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 Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 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
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
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
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event