Global Information Assurance Certification Paper

Hardware Flow Classification's Potential Impact on Security-in-Depth Design
David Merrick
GSEC Practical Version 1.3
Submitted 04/15/02

Abstract

The main choke points of using packet classification in security-in-depth design are the speed, the depth of packet inspection and relating packet flows. Most security products (Firewalls, NIDS and Routers) currently lack either the ability to do high-speed Layer 7 packet inspection or the ability to do flow classification. With the use of hardware-based packet inspection for flow classification, the ability to do high-speed packet inspection without impeding network traffic and the distribution of inspection points and reaction capabilities would be possible. The ability to distribute inspection and reaction capabilities means more accuracy and security can be built into the network in a layered approach. Specific points in the flow can be used to inspect for different attacks and mitigate their impact. This will not necessarily eliminate all attacks but it will make it far more difficult as there are more hurdles to clear.

The goals of this paper are to briefly describe flow classification, detail a specific product which provides this hardware flow classification capability, discuss how flow classification in hardware will impact current network equipment, discuss the impact on Security-in-Depth designs and illustrate a potential new network design with hardware flow classification devices in place.

THE BASICS

Flow Classification
Most people are familiar with the process of packet classification. The next evolution is the process of flow classification.
Packet classification for security in general starts to lose efficiency under the following conditions: when the source/destination ports are dynamically chosen from ephemeral ports and when an application uses multiple protocols in separate packet streams.
The Hifn 3010 Secure Flow Processor Fact Sheet has a good example:
(http://www.hifn.com/products/3010.html)

> … applications (such as) NetMeeting, where the protocol Q.931 is a control setup protocol for H.323 that gets spawned on a well-known port. Q.931, in turn, spawns H.245 on a dynamically assigned ephemeral port. Further, RTCP (real-time control protocol) channels and its associated RTP (real-time protocol) streams are also spawned on dynamically assigned ephemeral ports.

Flow classification is a process that not only performs standard packet classification but also associates packet flows based on the application information contained within the packets and the known behavior of that application.

Currently flow classification is done in software. Application proxies are the best-known examples of this process. Application proxies work by processing flow coming in on one interface, disassembling it, examining the flow and then reassembling it on another interface. This allows granular control over what protocols and services are allowed in and out of networks, but at the price of speed.

With the introduction of the Hifn 3010 Secure Flow Processor (SFP), flow classification has moved into hardware. This not only helps with the processing speed issue but also assists in the ability to distribute the flow processing ability throughout the network. By referencing a database of application protocols and having an understanding of the characteristics of the traffic flow, systems using a hardware flow classification allow for more intelligent and targeted applications of security.

The Hifn 3010 SFP

Hifn introduced the 3010 Secure Flow Processor in February 2002. This chip is a hardware implementation of software flow classification specifically designed for use in firewalls, NIDS, virus detection and other network security processes. The documented throughput is 4Gbps (2Gbps in each direction). The chip can be installed in-line to the traffic flow or used as a co-processor.

Several features of the 3010 allow for multiple uses and implementations that can be used to strengthen network equipment and in turn change Security-in-Depth network design. The features (in addition to the overall flow classification) that should be most useful are:

1) The ability to design the chip directly in-line or as a co-processor. This allows for the chip to be used either as an initial sensor or to assist a dedicated security system in analyzing traffic flow in real-time or as part of a forensic analysis of an attack.
2) The ability to configure the reference database. This will allow the chip to be customized for specific uses. You can use virus signatures, known-attack signatures, permitted/denied applications (for tailoring) and custom rules (for example – define and deny IP spoofing).
3) The chip is independent of the application using it. Its purpose is to analyze the traffic per the database and then pass that information to the application to handle. This allows for flexibility in implementation.
4) The speed of processing. At 4Gbps, it can be used at the edge of most networks as well as at internal points within the network without dropping packets.
5) You can serially link multiple chips to analyze packet stream for different attack signatures in the same device. Alternatively, the chips can be designed in parallel if the network device implements load-balancing in front of the chips and can correlate the separate data output streams from the chips.

The Hifn 3010 SFP allows for more intelligence in edge devices and at more points in the network without adversely impacting network performance. One important item to remember is that the SFP performs the flow classification and analysis only, the OS of

the device itself must make decisions and implement any required actions. The SFP primarily offloads the workload of processing, tracking and associating the packets. In the following pages, we'll examine how the Hifn 3010 SFP can be integrated into network equipment and some of the potential security uses for which the equipment can be used.

EQUIPMENT

Routers

Currently routers have been limited in the level of packet analysis they do and in general perform no flow classification at all. One specific attack that routers have the capability of handling, if configured properly, is IP spoofing. Unfortunately, the use of ingress and egress filters on a heavily loaded router adversely impacts CPU performance. A potential solution to this problem consists of using a router with a hardware flow classification chip. By using the SFP in a parallel or serial in-line configuration, the packet inspection for the ingress and egress filters is offloaded from the CPU. An advantage of using flow classification is that you can now apply dynamic filters. In the example of IP spoofing, the steps would be as follows:

1) Set a rule in the SFP database that defines IP spoofing as the use of an incorrect or reserved IP source address on packets on any interface.
2) Maintain a table that is populated with associated IP addresses and interfaces. This table would be dynamically populated based on the packet inspection from the SFP.
3) As traffic flows through the router the SFP can detect spoofed IP source addresses and pass the information to the IOS.
4) At this point the interface can be blocked dynamically and an administrator notified.

This method would help alleviate attacks that use IP spoofing. This would be especially useful against DRDoS (Distributed Reflected Denial of Service) attacks. A detailed description of a DRDoS attack can be found at http://grc.com/files/drdos.pdf. By eliminating the problem at the edge of the Internet you have effectively nullified this potential attack.

Another use for the SFP would be to recognize DDOS attack patterns and initiate a response that consists of throttling the down channel bandwidth, reserving bandwidth for outbound traffic and implementing a dynamic filter to allow authorized traffic. Additionally, the attack filter could be propagated upstream to help limit the effect of the attack while allowing legitimate traffic to flow downstream. DDOS attacks are resource attacks. In the case of bandwidth attacks, limiting the attack at the ISP before it clogs your pipe is the most useful recourse.

Switches
Switches have had L7 flow processing for some time but it has been executed in software vs. hardware. Like in routers this has an impact on the CPU of the switch. Adding an SFP at this point allows for a couple of advantages.

In the case of a switch in front of a cluster of application servers, the SFP can be configured to flag any traffic flow that does not conform to the specific application residing on the cluster servers. This allows for illicit access to data files other than through the appropriate application can be restricted and logged. Also, you can potentially flag, log and if needed prevent application calls by user.
A specific example would be a disgruntled employee attempts to delete or modify a database from his desk using his supervisor's ID. The SFP could key on the ID being used at an unassociated IP or MAC address. Additionally, you would have the event logged. The employee could attempt to delete the files from the supervisor's system as well. This could not be prevented with this design, but it would be logged and you would have some data for auditing.

Another advantage in using the SFP would be in spotting anomalous behavior on the network and either passing it to an IDS or applying preventive measures directly. You could configure the SFP to only pass authorized application traffic and/or within certain baseline traffic parameters. This would be especially useful in a situation where a new email virus and it is attempting to spread. A burst of mail traffic to the email server or an unknown application sending out email could be flagged and acted upon. Trojans could also be spotted as an unauthorized application. And by implementing IP spoofing rules, you could stop malicious outbound traffic at the breached machine.

Firewalls
There are three main types of firewalls: packet filtering, circuit-level and application level (proxy server). These firewalls are implemented either in software or hardware. As firewalls have evolved the three types have become increasing similar.

The biggest potential of the SFP is to not only speed up packet inspection but also allows for dynamic application filtering, virus filtering and flagging/redirecting suspicious packet flows.

Dynamic application filtering allows for rules to be built based on the application behavior and flow classification. Reference the Hifn white paper "Improving Security Performance and Cost Using SFP" at http://www.hifn.com/docs/a/WP-0121-00-Improving-Security-Performance-and-Cost-Using-SFP.pdf for a detailed explanation.

The advantage of using flow classification is that you don't have to open holes for each of the protocols. You configure the system to use known application behavior and only open holes for traffic related to the allowed application even if the application depends on multiple protocols. By doing this in a dynamic manner (meaning creating then removing firewall holes as needed), security is increased further. The SFP analyzes the initial traffic flow, determines the application and if it is allowed.

Then the SFP can monitor that flow and have the Firewall open additional holes as needed. This adds to security, as holes are not opened until needed and only for specific applications. In the example from Hifn, if an intruder attempted to initiate an RTCP connection without it being tied to an authorized flow, it would not be allowed.

The SFP can also aid in detecting known virus signatures before they reach the email server and initiate a response. It can also be configure to detect questionable file attachments such as .VBS files.

Related to virus detection and dynamic filtering is the ability to detect known intrusion signatures or suspicious traffic and flag or redirect it to a honeypot or an IDS for analysis and response.

An example would be a probe for a known OS or application vulnerability. This traffic could be redirected to a honeypot and with the use of an SFP augmented IDS could be analyzed further. In the case of suspicious traffic it could redirect the traffic directly to an IDS for analysis and further processing. This design helps keep potentially dangerous traffic isolated from critical portions of your network.

One of the recent design changes to proxy servers that have been made to make them faster was to be able to modify the filtering table to pass packets once the initial application level processing was processed. This speeds the process up but also leaves the system more vulnerable. By integrating an SFP into a proxy server you would be able to track the flow of the packets without sacrificing the application level processing. It could potentially allow the proxy server to be a dedicated hardware device vs. being built on top of a general use system.

IDSes

Intrusion Detection Systems could also benefit by the use of an SFP. In fact, there are some systems that have recently been released into the market that leverage hardware packet analysis for the speed advantage it gives.

The SFP could be used in an IDS sensor in the in-line mode to flag both know traffic and suspicious traffic and alert an IDS server or forward filtered traffic for additional analysis. By putting multiple SFPs in a serial in-line design within a sensor, each SFP could be used to detect different types of attacks. Some could look for L2-L4 attacks, others for specific application or OS attacks and still others for non-baseline traffic. By setting the first SFP to pass authorized traffic and redirect unknown/unauthorized traffic to the other SFPs for analysis makes the sensors more effective.

Using the SFP in a serial or parallel configuration as a co-processor in an IDS central server would aid in analysis. Again, the idea is to filter out authorized traffic based on the rules for the network. By using co-processors the primary CPU can continue to communicate with sensors and crunch the data for analysis. Also by flagging known authorized traffic a more accurate baseline can be built for the network.

One specific use for an SFP modified IDS sensor would be for use with a honeypot or honeynet. By using the sensor to track and log all traffic based on its flow classification, we get a needed insight into analyzing potentially new attacks from the network view. The goal would be to aid in the development of network level attack signatures vs. host level attack signatures. These signatures could then be added to IDS sensor or even firewall databases to aid in the overall prevention.

The end goal for increasing the processing capabilities of both the IDS sensors and the IDS servers is to make them more efficient and decrease the reaction time. By adding flow classification and the ability to filter at the application layer, the closer we get to eliminating false positives and negatives. The addition of filtering and recognition of suspicious traffic also helps in getting closer to real-time alerts. Both of these items increase the effectiveness of IDSes.

Desktops
The use of the SFP at the desktop is somewhat limited but has some potential. An SFP integrated into a NIC could be used to help baseline application traffic for that system. It could also be used to add time or application restriction to that system remotely.

Equipment Summary
In this section we looked at the potential uses of the SFP in different types of equipment and at the different applications of the technology. The Hifn SFP may be the first, but it will probably not be the last chip in the flow classification arena. As mentioned previously, there are manufacturers releasing equipment that have some of the capabilities listed and are designed for a particular purpose. In the next section, we will look at putting all the pieces together into an overall network design.

NETWORK DESIGN

ISP
Starting at the edge of the ISP's network we would place an IP Spoofing aware router. This router would help eliminate DRDoS attacks by using dynamic filtering. By logging incidents it could also aid the ISP in removing potential miscreants from its systems. Additionally this router could be designed to recognize a DDoS attack pattern and implement a response.

For smaller customers, ISPs could add more rules to the SFP database or utilize some of the other discussed equipment and offer some of the services that a small business or home user might not be able to afford otherwise. Examples would be the IDS capabilities and the Virus prevention. Other examples would be firewall services and DDoS prevention.

Corporation
At the edge of the network implementing an SFP router would be useful for preventing breached systems from initiating outbound IP spoofing and early detection of intrusion reconnaissance probes.

The next piece of equipment would be the addition of a multi-port firewall (primary firewall). The firewall would be configured to use application rules and create dynamic holes as needed. Additionally, initial virus scanning and known IDS signature rules could be applied at this point. By utilizing four interfaces instead of standard three, a firewall could be configured to route suspect traffic to an isolated honeynet or IDS.

Between the Firewall and the servers in the DMZ, an IDS sensor should be inserted to assist in detection/response of application and OS specific attacks.

On the Honeynet segment, a modified IDS sensor should be added to help with network attack signature development.

Data from all IDS sensors would be routed to a firewall isolated IDS Control Server. Using SFP(s) as co-processors or serially, the Server could speed analysis and response to network attacks.

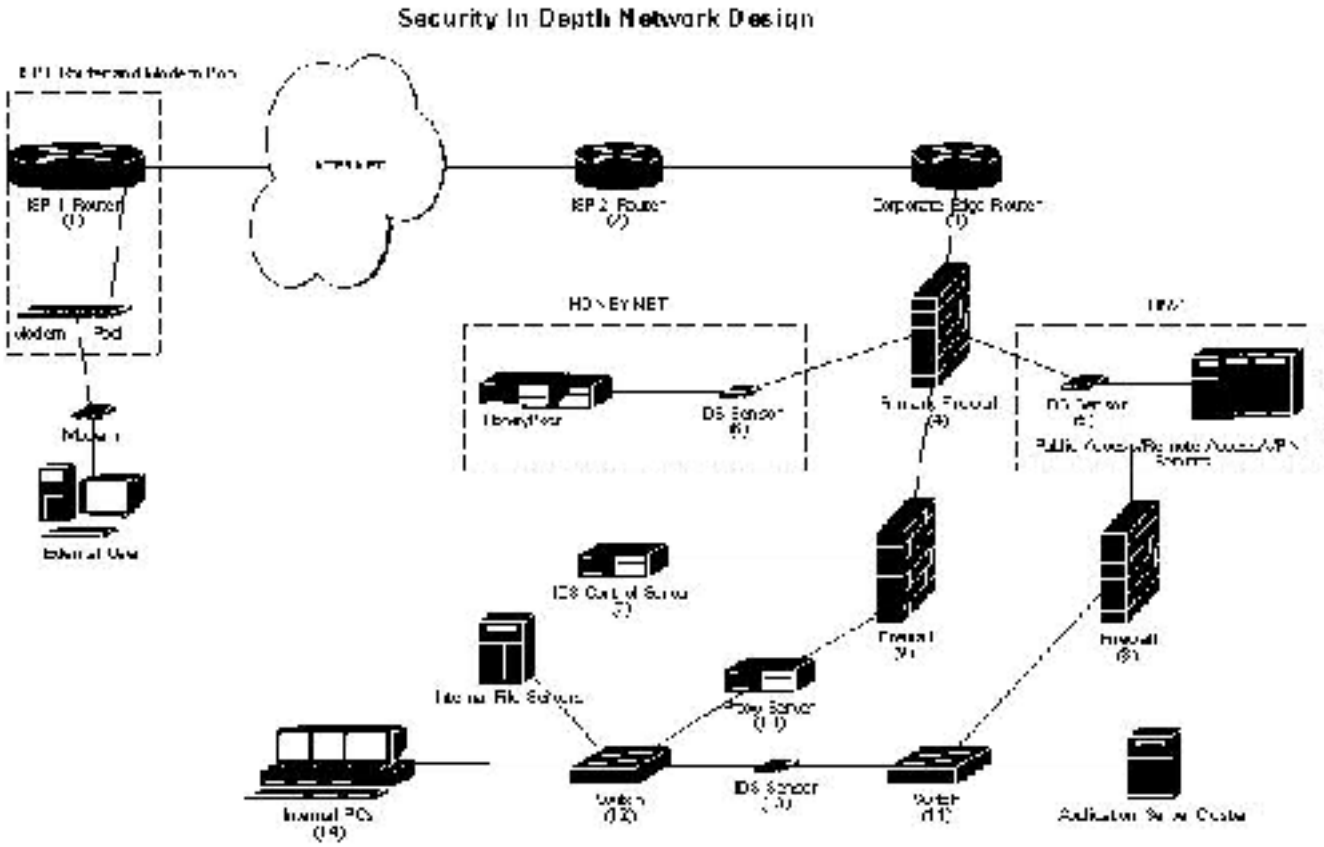
Between the DMZ segment and the trusted network another SFP firewall or an SFP switch should be installed. This could be restricted to allow specific applications, specific application calls and specific IP addresses access to the backend servers.
By locating your VPN gateway and/or other Remote Access Servers in the DMZ and then routing the decrypted traffic through an internal SFP firewall or SFP switch, you can address the issue of dealing with encrypted traffic as well.

A secondary firewall system should be between the primary firewall and the trusted network. This could be a combination of both a firewall and an application proxy server.

Internally, SFP switches should be placed in front of critical systems and application server clusters to help protect against illicit internal access and application calls.
SFP switches can also be used to help baseline network traffic and flag suspicious traffic. By implementing IP spoofing rules as well as authorized application rules you can control the traffic on your network and intercept malicious outbound traffic.

Additionally, adding IDS sensors at key points to augment your SFP switches or to alleviate the switches from having to perform any analysis is also recommended. The advantage of using sensors is that they can be controlled through the primary IDS console and can add multiple layers of intrusion detection.

Lastly, utilizing an SFP augmented NIC in the desktop, you can remotely baseline your systems and have an early warning system of a breached system.



1) ISP edge router - prevents IP Spoofing (outbound) and provides smaller customers known DDoS attacks and known Virus protection.
2) ISP edge router - prevents IP Spoofing (inbound) and mitigates DDoS attacks.
3) Corporate router - prevents IP Spoofing (outbound), coordinates DDoS response with ISP edge router and provides early warning of recon probes.
4) Primary firewall – utilizes application-level rule base in hardware, creates dynamic holes as needed, scans for known viruses and IDS attack signatures and routes suspect traffic to honeynet for analysis.
5) IDS Sensor – detects application and OS specific IDS attacks/probes.
6) IDS Sensor – designed to capture inbound and outbound traffic and aid in designing network signature for new attacks.
7) IDS Control Server – utilizes parallel or serial co-processors to perform analysis.
8) DMZ–to-Trusted Network Firewall – Restricts traffic by IP address Source/Destination, Source/Destination Ports and specific application requests.
9) Secondary Firewall – Uses application-based rule set to dynamically open/close holes, restricts access to IDS Control Server, restricts Internet bound access to proxy server.
10) Proxy Server – Restricts outbound Internet access of users and applications. Utilizes an SFP for high-speed processing.
11) Application Server Cluster switch – Restricts access to authorized applications and application calls. Assists in baselining the network.
12) General Internal Switch – Used to baseline network, early detection of breached systems, controls network traffic based on authorized application list and flag suspect traffic.
13) IDS Sensor - Augments overall intrusion detection, could supplement or replace some of the listed uses of the General Switch.
14) SFP NICs – Used to baseline system traffic and provides early warning system of breached systems.

CONCLUSION

The goal of this paper was to show the potential changes to Security-in-Depth design by adding hardware flow classification into the mix of network equipment. As discussed above adding more intelligence to the packet analysis process, enabling dynamic filtering on application behavior and packaging it all into a chip that operates at Gigabit speeds will change the landscape. No longer will you have a router that just routes or a firewall that just forwards packets. You now have the ability to implement layers of Intrusion Detection and attack prevention without adversely impacting the primary purpose of the devices. This ability can augment existing devices to make them more effective and efficient.

One other issue that is appearing more often is the use of encrypted communications in networks. Encrypted communication insures secure communication but also makes packet analysis useless. Using SFP augmented equipment will help here as well by dropping or routing to the honeynet all encrypted traffic destined for unauthorized hosts and/or ports (i.e. Any encrypted traffic destined for port 80 on your web server). There are three additional methods of dealing with encrypted traffic:

1) Isolate all encrypted inbound traffic in your DMZ. Any traffic from your DMZ into your internal network should be unencrypted and passed through a firewall. Alternatively, use a gateway to terminate one end of the encrypted traffic flow and analyze the traffic before or after encryption.
2) Run Host-based IDSes and Intrusion Prevention software on systems terminating encrypted communications.
3) Utilize proxy servers as endpoints for outbound encrypted communications.

The Hifn 3010 SFP is a step in the right direction but like all technology it is not a solution in and of itself. Vendors will still need to implement and tie the interfaces into their products. The issue of interoperability at the Vendor level is still an issue. Also in adding the additional abilities to the network equipment, you add a layer of complexity to the network.

Two of the nicer things about integrating this processing at the chip level is that first, in the case of routers and switches the configuration could be setup once and modified only occasionally and secondly in the case of all the devices, the configuration could be setup through the existing user interfaces to the systems.

Flow classification in hardware is not a silver bullet but it is a step in the right direction. Overall security is still dependent on a multi-layered approach. Careful network design to eliminate points of failure, educating users and having good policies and procedures that assist you in keeping your network secure are essential.

REFERENCES

1) Hifn**;** "**Why You Need Flow Classification**", Sep. 2001

URL: http://www.hifn.com/docs/a/WP-0001-00-Why-You-Need-Flow-Classification.pdf (First access: 03/13/02 - Verified 04/15/02)

2) Hifn; "**Hifn 3010 Secure Flow Processor Fact Sheet**", Feb. 2002

URL: http://www.hifn.com/docs/3010.pdf (First access: 03/13/02 - Verified 04/15/02)

3) Gibson, Steve; "**Distributed Reflective Denial of Service (DRDoS)**", Feb. 22, 2002
URL: http://grc.com/files/drdos.pdf (First access: 03/18/02 - Verified 04/15/02)

4) Hifn; "**Improving Security Performance and Cost Using SFP**", Mar. 2002

URL: http://www.hifn.com/docs/a/WP-0121-00-Improving-Security-Performance-and-Cost-Using-SFP.pdf (First access: 04/05/02 - Verified 04/15/02)

5) Interview notes and follow-up emails with Rahul Patel, Business Line Manager, Hifn.

6) Smith, Gary; "**A Brief Taxonomy of Firewalls – Great Walls of Fire**", May 18, 2001
URL: http://rr.sans.org/firewall/taxonomy.php (First access: 04/05/02 -Verified 04/15/02)

7) Kessler, Gary C.; "**IDS-in-Depth**". Information Security August 2001

URL: http://www.infosecuritymag.com/articles/august01/cover.shtml#ids

(First access: 03/18/02 – Verified 04/15/02)

8) Top Layer; "**AppSafe 3500 Data Sheet**", 2001

URL: http://www.toplayer.com/pdf/Datasheet_TLN_APSafe3500.pdf

(First access: 03/18/02 – Verified 04/15/02)

9) TopLayer Networks and ISS; "**Gigabit Ethernet Intrusion Detection Solutions**", Jul. 25, 2000 URL: http://www.toplayer.com/pdf/iss_tln_GigResults.pdf

(First access: 03/18/02 – Verified 04/15/02)

10) Gong, Dr. Fengmin; "**Next Generation Intrusion Detection Systems (IDS)**", Mar. 2002

URL: http://www.intruvert.com/technology/IntruVertNextGenerationIDSWhitePaper.pdf

(First access: 03/18/02 – Verified 04/15/02)

Last Updated: July 28th, 2017

Upcoming Training

SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
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 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
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
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 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 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
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
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
Community SANS Indianapolis SEC401	Indianapolis, IN	Oct 09, 2017 - Oct 14, 2017	Community SANS
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event