Global Information Assurance Certification Paper

Traversing Firewalls with H.323

By Stephen Cypher
Version 1.4B

Abstract

The International Telecommunications Union (ITU) has developed a set of standards that specifies how computer equipment and services format and transmit multimedia data over networks that do not guarantee quality of service. An example of this type of network would be the Internet. It is an umbrella standard that is comprised of several sub-standards and is termed Recommendation H.323. The standard allows for terminals to connect with other terminals that may use dissimilar client software but support the H.323 standard. H.323 defines how audio and video information is formatted and packaged for transmission over a network such as the Internet.

The main purpose of a firewall is to prevent intruders from accessing a private network. It does this by guarding all untrusted entry points and preventing external entities from directly accessing network elements. The benefits of a properly configured firewall are that a private network will remain protected against all external threats.

The potential for successful communication between two H.323 clients over the Internet is greatly increased with the absence of network firewalls. In most cases it is not possible to simply bypass a firewall, thus crossing over or passing through it, is the only option. Traversing firewalls securely is one of the more difficult obstacles faced when building an infrastructure for supporting H.323 traffic. Networking vendors have recognized the need for products to overcome the firewall traversal problem and have developed both hardware and software based solutions

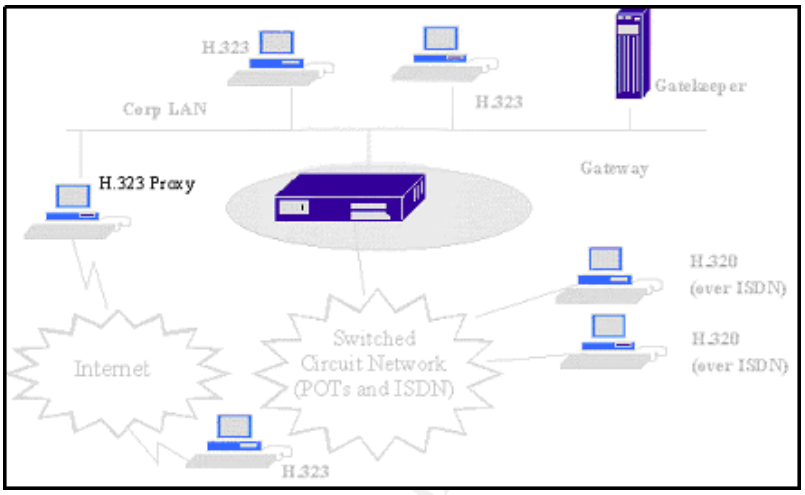
The purpose of this paper is to discuss secure methods for traversing network firewalls with H.323 traffic. Towards this goal, we will briefly describe the components and protocols that make up an H.323 network, the initial call setup process that takes place when two clients establish communication, security concerns with certain H.323 protocols and finally discuss some of the vendor solutions for traversing H.323 traffic over network firewalls.

One topic that this paper will not discuss is firewalls that are configured to use Network Address Translation. (NAT) NAT presents many additional obstacles when dealing with H.323 traffic and firewalls and will not be covered in this paper.

Generic H.323 Overview

H.323 Components

An overview of how H.323 works is helpful to understand issues addressed in later sections of this paper. A generic H.323 architecture is shown below. This graphic does not illustrate a network firewall and but will covered in greater detail in later images.



Generic H.323 architecture

H.323 Terminals – Endpoints that can interact with each other directly in point-to-point or multipoint conferences and provide real-time, two-way communications. H.323 Terminals must support voice, with video and data being optional. Terminals can either be hardware or software based, e.g. PictureTel conferencing unit, MS NetMeeting, CUseeMe client, etc.

MCU – The H.323 MCU main functions is to maintain all the audio, video, data and control streams between all participants in the conference. The MCU allows three or more terminals to participants in a conference.

Gateway – Provides translation between circuit-switched networks (ISDN) and packet-based networks. (LAN) These devices enable endpoints on different types of networks to communicate with each other.

Gatekeeper – A device that services include address translation, admission control, bandwidth control and zone management. It also provides for call authorization and accounting information.

Zone – All H.323 devices that are registered to a single gatekeeper.

These are the components that are required to field and enterprise level H.323 based teleconferencing service. These components can be implemented in both hardware and or software.

Associated Standards, Protocols and Ports

The H.323 standard provides for audio, video and data sharing and collaboration. It is an umbrella standard that is comprised of several sub-standards to address each of the three main services it provides. The table below summarizes the relationships between the various services, protocols and ports of the standard.

Function	Supported H.323 Standard	Protocol	Port(s)
Control	H.245 call control	UDP	Dynamic > 1024
Audio (codec)	G.711, G.722, G.723.1, G.728, G.729	UDP	Dynamic >1024
Video (codec)	H.261, H.263	UDP	Dynamic >1024
Data	T.120 (a family of protocols)	TCP	1503
Multiplexing	H.225 umbrella includes: Q931 for call signaling	TCP	1720

T.120 Standard

T.120 is one of the many standards that fall under the H.323 umbrella of standard. T.120 is a list of recommendations for providing the transmission of information in multi-point multimedia communications. It is composed from several protocols to ensure that file transfer, whiteboard and chat usage, and application sharing, can be used when two or more terminals are communicating.

One of the more popular applications in use is File Transfer Protocol. (FTP). The protocol used to upload and download content between machines. Most often port 21 (the port that FTP uses) is closed when configuring a firewall due to the vast amount of well know hacks associated with it.

Application sharing is inherently dangerous as it gives remote users and anyone who can hack them mouse and keyboard access to a machine that may be protected by a firewall. Hackers can insert a DOS command shell into a shared document and basically do what they want (put in viruses, install sniffers, delete files, etc.).

The Chat application is also a potential security risk due to the fact that it transmits information in clear text and can be easily read by someone sniffing a network. Several products are available for monitoring this type of communication.

T.120 Standard (continued)

One of the things to consider when tunneling H.323/T.120 traffic though a firewall is that the tunnel itself in most cases is not secure. This means that a potential hacker has the ability to see and manipulate any data passing though the tunnel. Even though one site is well protected by a firewall, the other is not, allowing anyone who gains access to the unprotected site the ability to pass through the tunnel to the protected site and access resources associated with it.

Client Registration

A gatekeeper is an optional component in a H.323 network that provides call control services to the H.323 endpoints that are registered with it. These services include address translation, admission control, bandwidth control and zone management. It also provides a mechanism for call authorization and accounting information. In order for a H.323 client to place a call with a gatekeeper it must first register with it. The client configuration process involves entering the IP address of the gatekeeper itself, an alphanumeric alias name and a numeric name. The numeric name is also referred to as the E.164 address. Upon successfully registration with a gatekeeper the client has the ability to call other H.323 client on the network that have registered with a gatekeeper. It can contact them by their IP address, their alphanumeric alias (Name) or numeric address. (E.164)

With the addition of gatekeepers in a H.323 network an administrator has the ability to adding extra levels of security. One addition would be to have user authenticate to a Radius server before registering with a gatekeeper. This would require that a user enter a name and password before the gatekeeper would add it to its table. Another option would be to statically enter the H.323 endpoints in the gatekeeper so that only know client would be able to register. These additions to securing the gatekeeper help to prevent unauthorized entities from using its services.

Call Setup Process

To better understand why traversing network firewalls securely with H.323 traffic is difficult, it is helpful to understand the communication that takes place between two terminals during the establishment of a call. The two protocols that are used during this opening phase are the H.245 and H.225 protocols. Q.931, which falls under H.225, is used for call signaling. The process can be broken down into three phases:

Call Setup Process (continued)

Phase I
H.323 terminal (A) starts by sending a "*Setup message"* to another H.323 terminal (B) containing its destination address. Terminal (B) responds by sending a Q.931 "*Alerting message"* followed by a "*Connect message"* if the call is accepted. During this first phase of call signaling, the only port used for communication is TCP port 1720. If the destination terminal accepts the call, the second phase of negotiations using the H.245 protocol begin.

Phase II
During the H.245 negotiations, both terminals will exchange their terminal capabilities. The terminal capabilities include media type, codec choices, and multiplex information. Each terminal will respond with a "*terminal Capability Set Ack message"*. The terminals' capabilities may be resent at any time during the call.

Phase III
The final phase of the call setup deals with the master/slave relating between the two terminals. The master/slave relationship is used to resolve any conflict that may arise between the two terminals during the duration of the call. Once the call setup process is complete, the audio and video channels are opened and the video conference call begins.

It is in phases two and three where crossing a firewall becomes a problem. The ports used during these negotiations are dynamically assigned, meaning that any UDP port between 1024 and 65,535 can be used. Since the standard calls for them to be dynamically assigned there is no way to predict which ports will be used, thus making it impossible to configure any kind of rule on the firewall. Opening up a hole with this range of UDP ports would defeat the purpose of the firewall itself.

Vendor Solutions

Cisco MCM Routers

The Cisco Multimedia Conference Manager (MCM) is a Cisco IOS software feature set that enables IP networks to support secure H.323 videoconferencing, with (QoS) service capabilities. The Cisco Multimedia Conference Manager (MCM) is a H.323 Gatekeeper and Proxy, implemented as a subset of Cisco IOS. The Cisco MCM is installed on Cisco routers dedicated for that purpose. These capabilities ensure appropriate allocation of network resources for videoconferencing on the network.

Concept:
A possible network configuration, which traverses a firewall, would be to setup a configuration with two zones. Zone 1 would be considered all videoconferencing equipment attached to the network on the inside of your firewall. Zone 2 would be considered any videoconferencing equipment on the outside of your firewall (the Internet). A Cisco MCM router would be placed in each zone and would be configured to be the gatekeeper and the proxy for that zone. Only H.323 traffic is permitted over a single fixed port via Generic Routing Encapsulation (GRE) through the firewall. Clients external to the firewall would register with the Router/gatekeeper on the outside of the firewall and internal client would register with the router/gatekeeper on the inside of the firewall. Clients would need to register with their appropriate gatekeeper in order to initiate a call.

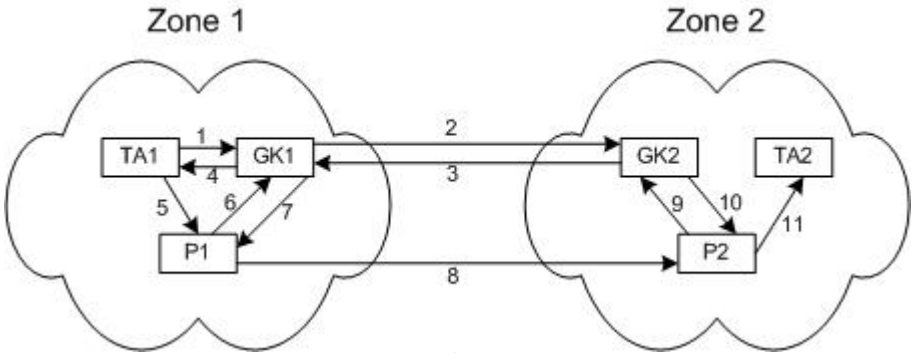
Operation:
The call process for an external client initiating a secure call to an internal client would work as follows:

1. Terminal in Zone-1 (TA1) contacts the gatekeeper in its zone with the alias or E164 address of a terminal in Zone-2 (TA2) that it wishes to communicate with.
2. The gatekeeper in Zone-1 (GK1) contacts the gatekeeper in Zone-2 (GK2) to see if the requested client is registered and then retrieves the IP address of that client.
3. GK2 responds with the IP address of the proxy for that zone (P2) instead of the IP address of TA2 in order to hide its identity.
4. The GK1 knows that in order to make a call to the P2 it need to place the call through its own proxy (P1). The GK1 returns the IP address P1 to TA1.
5. TA1 now contacts P1.
6. P1 consults GK1 to discover the true callers destination (Which is TA2s address).
7. GK1 instructs P1 to call P3.

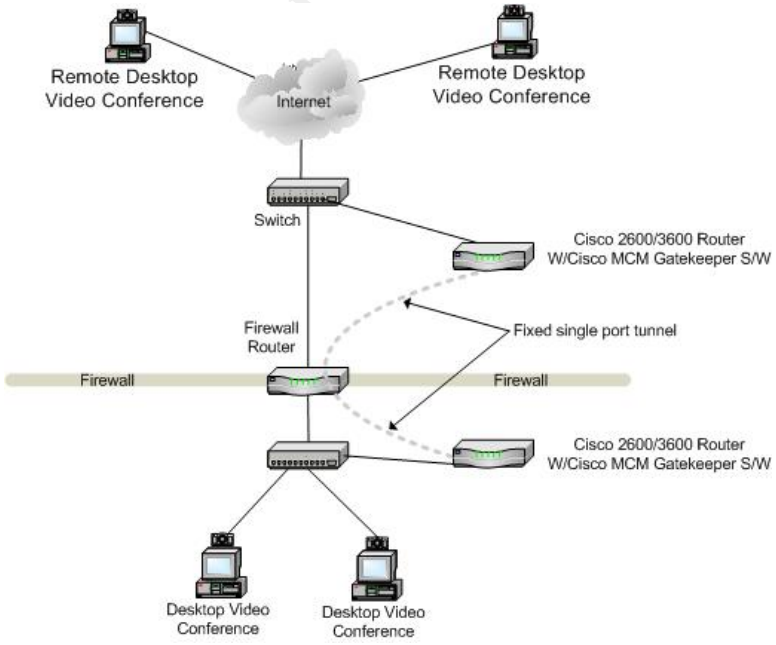
Operation: (continued)

8. P3 consults GK3 for the true IP address of TA2.
9. GK2 gives TA3's address to P2.
10. P2 now completes the call to TA2.

The diagram below illustrates the communication that takes place between two H.323 terminals when attempting to place a call across two zones. This same handshake signaling would take place if there were a network firewall between the two zones. The numbers represent each leg of the communication path between two clients (TA1 & TA2) during the call initiation process. This process is not part of the H.323 call setup process, but it is used for locating clients in different zones.



The diagram below illustrates where the Cisco MCM routers would be placed in the Cisco firewall traversal solution.



CUseeMe Conference Servers

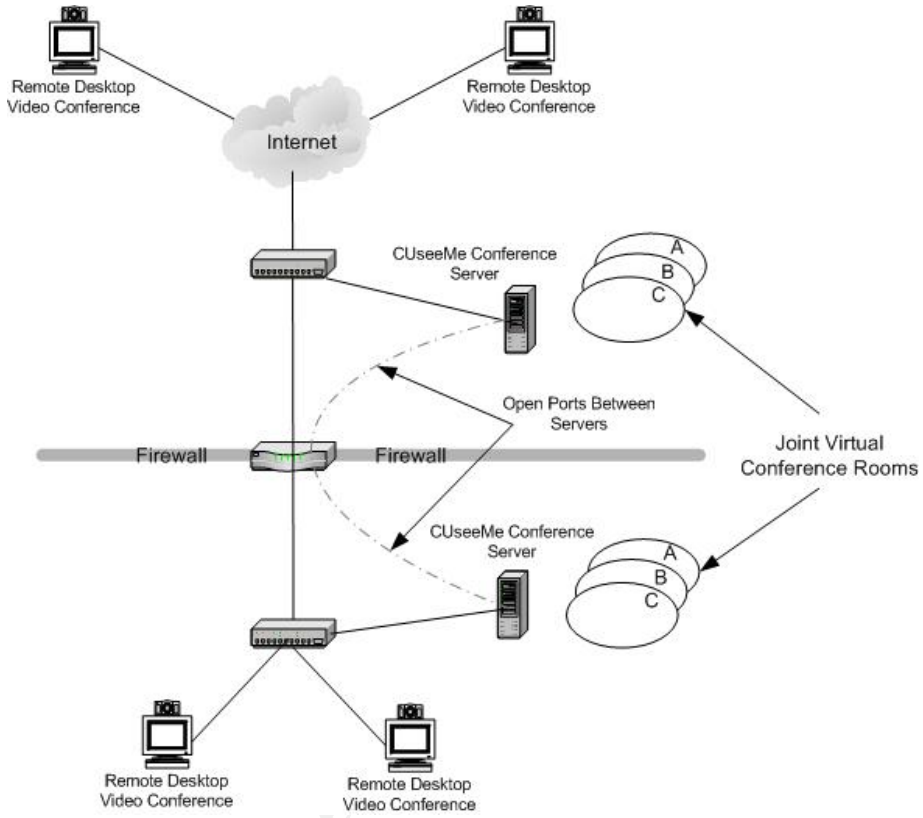
The CUseeMe conference server is a software-based conferencing solution, which is implemented by creating virtual conference rooms on an existing IP network using the H.323 standard. The conference server has built in features such as a full H.323 MCU, a Gatekeeper, T.120 data collaboration capabilities and H.320 to H.323 gateway services for ISDN connectivity. The software is available on several operating system platforms including Microsoft, Solaris, and Red Hat

Concept:
CUseeMe approaches the firewalls traversal issue by placing servers on both sides of the firewall. The server on the outside the firewall handles incoming conference calls from the internet, while the server inside the firewall handles outgoing conference calls from internal clients. Ports are opened on the firewall to allow the two servers to communicate. The servers are hardened, enabling only those services, which are required for the proper function of the CUseeMe Server. The firewall is reconfigured to open three fixed ports TCP 7640, UDP 7648 and TCP 1503 so that communication between the two servers is permitted. CUseeMe uses proprietary software to tunnel the various H.323 protocols across the firewall. Access Control Lists within the firewall are modified to ensure that traffic originating from source addresses other than the servers is denied.

Operation:
Once the servers are configured and communication between them has been established, the virtual conference rooms can be configured. Identical rooms are configured on the inside and outside servers and are logically joined. One of the security features of the virtual conference room is that they can be password protected.

Like in the Cisco configuration, clients on the outside of the firewall register with the gatekeeper services on the external server and the internal clients register with the gatekeeper services on the internal server. Clients can then meet in a predetermined conference room to conduct conferences. One draw back is that external clients do not have the ability to directly contact internal clients as in the Cisco configuration.

The diagram below illustrates how the CUseeMe conference servers would be configured for traversing H.323 traffic through a firewall.



Aravox H.323 Filter

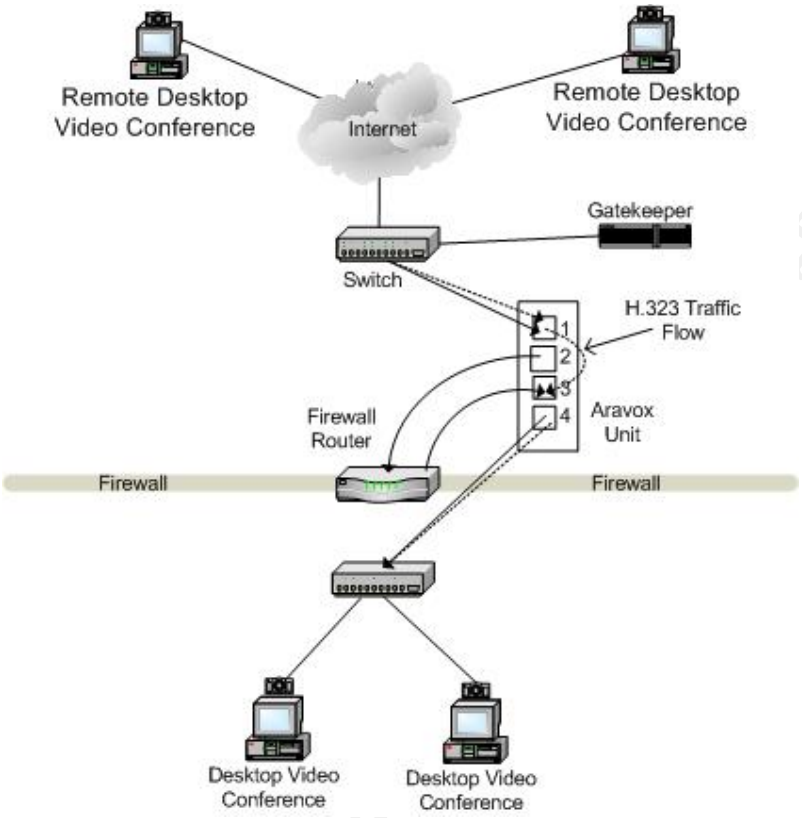
Aravox uses their Voice over IP technology to restrict access to specific devices and applications on a network while allowing the flow for real-time streaming application such as H.323. The Aravox device can filter out H.323 traffic from a data stream to an alternate path, and reinsert in into the original data stream after it passes though a firewall.

Concept:
The Aravox solution for traversing network firewalls is to place their H.323 filter directly between a company's firewall and their ISP provider. All network traffic would be funneled through their device and the H.323 traffic would be filtered out and would bypass the firewall. The device itself is basically a four-port unit that would be configured as follows

Operation:
Network traffic coming from the ISP provider would travel through port 1. All non-H.323 traffic would exit through port 2 and go directly to the firewall. The firewall rules would be enforced and any remaining traffic would return to port 3. The H.323 traffic that was filtered out for port 1 would bypass this phase and would enter back into the data stream in port 3. The Aravox claim is that it can securely send the H.323 traffic from port 1 to port 3 by opening "secure pinholes" between the two ports. By just filtering the secure H.323 traffic, the dynamic UDP port issue is not a problem. The process works the same for the traffic that is generated on the inside of the firewall.

One of the biggest drawbacks of the Aravox solution is that it places an additional device in the main flow of Internet traffic to and from a private network. The fact that it's an unfamiliar device could make network administrators feel uneasy about installing unproven technology and creating an additional single point of failure to a network.

The diagram below illustrates how the Aravox solution would be implemented on a network for traversing H.323 traffic through a firewall.



Conclusion

The purpose of this paper was to show the problems that are faced when trying to traverse network firewalls with H.323 traffic. We began with a brief overview of the components that make up an H.323 network and how they might be implemented. H.323 is a fairly new standard and not that well known yet. The next part of this paper discussed the T.120 standard and some of the applications associated with it. The functionality of these applications can be quite handy but can also leave a network vulnerable to attacks. It is in my opinion that if these applications are not needed that they should be blocked at the firewall. Call setup and signaling was also discussed in the H.323 overview. It is in this process that we discussed why traversing a firewall could cause problems. Dynamically assigned UDP ports are used in this process and make configuring a firewall for passing H.323 traffic extremely difficult. The last part of this paper showed three different vendor approaches to the firewall traversal problem.

A few things to keep in mind are that if H.323 endpoints on both ends of the communication path sit behind a firewall, both firewalls need to be configured to pass H.323 traffic. An organization can spend a lot of time and money to configure their firewall to traverse H.323 traffic, but if the terminal at the other end of the communication path is blocked by a non-H.323 friendly firewall, the call will not go through.

Often communication between terminals that use different H.323 client vendors may also experience problems trying to communicate. Even though each vendor's client complies with the H.323 standard it does not necessarily mean that communication will always go smoothly. The standard itself is fairly young and still has a ways to go.

References:

Internet

Cisco Systems (Vendor solution and H.323 research)
http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_configuration_guide_chapter09186a00800ca6a4.html

Cisco Systems (Vendor solution and H.323 research)
http://www.cisco.com/en/US/products/sw/iosswrel/ps1830/products_feature_guide_chapter09186a0080080675.html

White Pine Software (Vendor solution)
http://www.fvc.com/eng/webconferencing/conference_server.htm

Aravox Corporation (Vendor solution)
http://www.aravox.com/products.asp

Microsoft Corp. (NetMeeting)
http://www.microsoft.com/windows/netmeeting/corp/reskit/default.asp

H.323 Research Information
http://www.teamsolutions.co.uk/tsh323.html

H.323 Research Information
http://www.winnetmag.com/Articles/Index.cfm?ArticleID=8052

H.323 Research Information (H.323 graphic)
http://www.chebucto.ns.ca/~rakerman/articles/ig-h323_firewalls.html

H.323 Research Information
http://www.networkmagazine.com/article/NMG20000727S0027

H.323 Research Information
http://www.ktln.com/Technical/t120.htm

Last Updated: May 28th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 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
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
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