Interested in learning more about security?

SANS Institute InfoSec Reading Room

Implementing a Secure Internal Network

This paper presents how-to options and suggestions for designing and securing an internal network. Scenarios are provided concerning designs that may currently be in place and discussions and analysis on the risks involved and the vulnerabilities presented are included. Figures 1 through 5 illustrate a phased approach that can be used to migrate to a more secure environment through the use of a combination of router and switch configurations. The final internal network design in figure 5 demonstrates a marked improveme...

Implementing a Secure Internal Network

GIAC GSEC Certification Option 1

Assignment version 1.4b

Ken Creekmore

April 4, 2003

TABLE OF CONTENTS

SUMMARY

This paper presents how-to options and suggestions for designing and securing an internal network. Scenarios are provided concerning designs that may currently be in place and discussions and analysis on the risks involved and the vulnerabilities presented are included. Figures 1 through 5 illustrate a phased approach that can be used to migrate to a more secure environment through the use of a combination of router and switch configurations.

The final internal network design in figure 5 demonstrates a marked improvement over the initial design found in figure 1. Bridges and hubs are removed and replaced with routers and switches to segment the network. Virtual LANs (VLANs) were implemented to further separate network traffic to and from workgroups and servers. Workgroup and enterprise servers were moved from the workgroup clouds, moved to a secure area and directly connected to the core router/switch with port security enabled. The internet router running access control lists (ACL) was replaced with a Cisco router with firewall IOS which was configured with context-based access control (CBAC) to harden the front line of defense. The public servers – Web, DNS, FTP and mail – were moved into a demilitarized zone (DMZ) and secured with ACLs. Finally, 802.1x security was configured on the workgroup servers.

DESIGN SCENARIOS AND CONSIDERATIONS

Throughout the rest of this paper – starting with the initial network design found in figure 1 – I will offer an analysis of the problems, threats and risks involved with the configuration of each design scenario. Additionally, I will demonstrate how the design will change to eliminate or minimize these and offer comments concerning the revised design.

The following figures and comments are meant to present a phased approach to arrive at a final configuration that will represent a more secure environment for the internal network. This approach is based on the premise that a fictitious company has the network shown in figure 1, or something similar. In reality, a company will probably have some combination of the figures I have presented here.

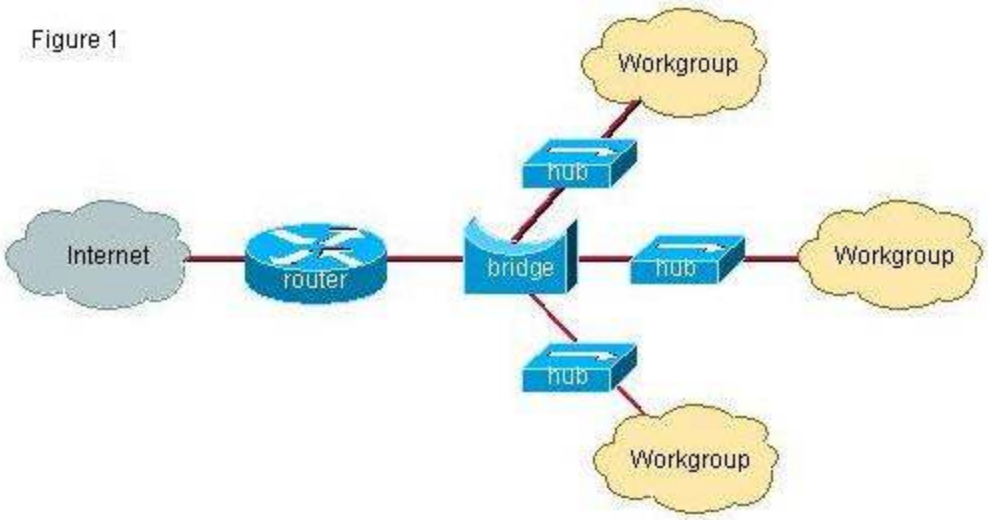
Design Figure 1

Summary

This design shows a network configuration employing an internet router and a bridged internal network. The workgroups are connected to the network via

hubs. Workgroup servers are co-located with the workstations in the workgroups. The internet router is configured with ACLs.

Figure 1



Detail

In consideration of this network design, it can be noted that a sniffer could be placed anywhere on the network to view network traffic. This poses a risk to the network since passwords could be retrieved. Since this is a bridged network, it is not possible to effectively isolate and protect the workgroups with ACLs or any sort of port security. The internet router does have ACLs but is not performing stateful inspection. Also, the inbound ACLs from the internet are configured to permit all traffic and only deny what the designer considered should be denied.

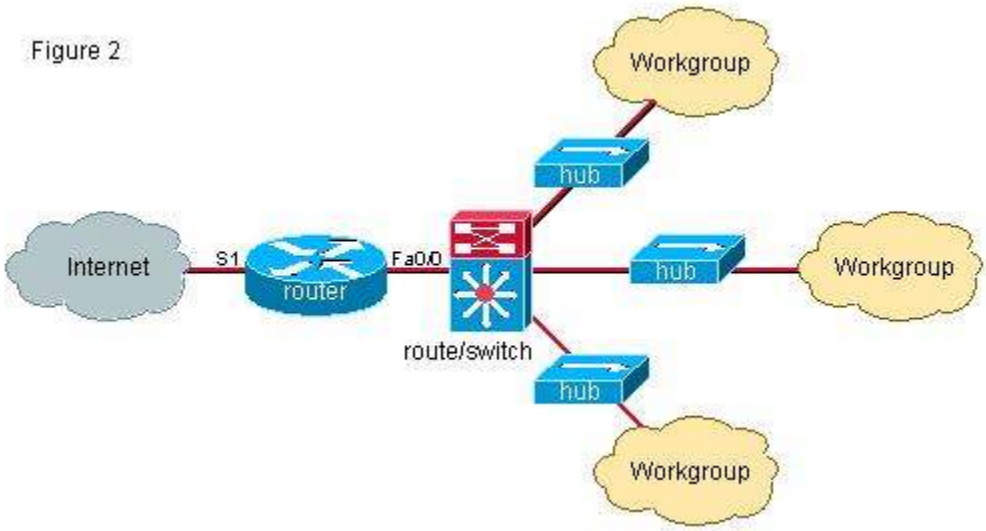
This approach leaves the internal network vulnerable to attacks that exploit any of the protocols and ports that are not denied in the ACL. Also, defense-in-depth is not present since there are no protections in place except for the ACLs in the firewall.

Design Figure 2

Summary

In this step, the bridge is replaced with a route/switch and the existing hubs are connected there. The router is configured to route IP and Appletalk. VLANs are implemented in the router's virtual interfaces as well as in the switch. ACLs[1] are also configured in the router as a second line of defense after the internet router.

Figure 2



Detail

The bridge is removed and replaced with a switch/router. In this case we will install a Cisco 6500 series switch/router to handle the routing. Cisco's Enhanced Interior Gateway Protocol (EIGRP)[2] is chosen as the routing protocol. IP EIGRP is configured on the router as shown in this configuration example"

```
router eigrp 111
 redistribute static
 network xxx.xxx.0.0
 no auto-summary
```

Zones are configured for the Appletalk devices as shown in this configuration example:

```
interface Vlan10
 description Engineering
 ip address xxx.xxx.10.1 255.255.255.0
 ip access-group 101 in
 ip access-group 102 out
 appletalk cable-range 10-10 10.1
 appletalk zone Engineering
 appletalk protocol eigrp

interface Vlan20
 description Marketing
 ip address xxx.xxx.20.1 255.255.255.0
 ip access-group 101 in
 ip access-group 102 out
```

```
appletalk cable-range 20-20 20.1
appletalk zone Marketing
appletalk protocol eigrp
```

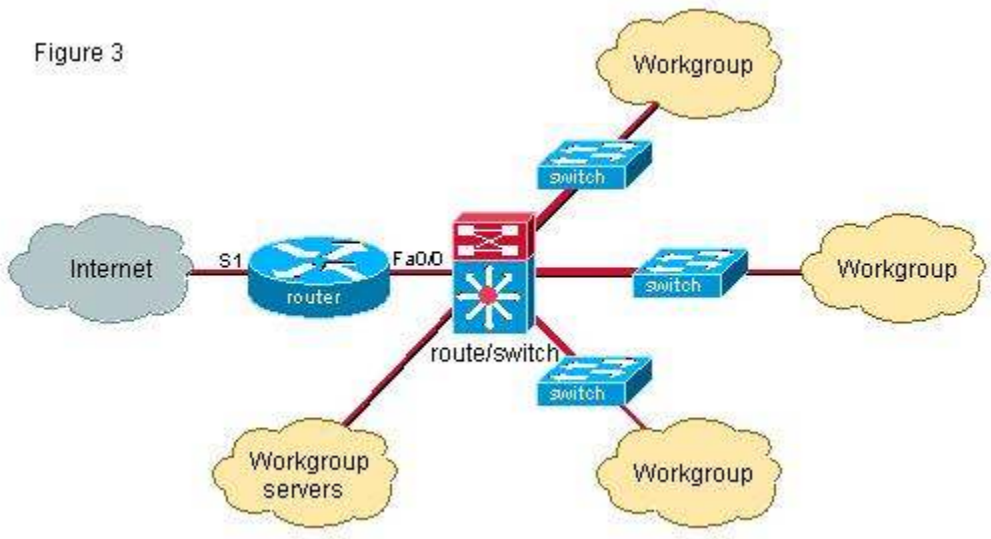
We will use a class B network address space with a mask of 255.255.255.0 and subnets are allocated for the various workgroups. The DHCP server is re-configured to reflect the new IP numbering plan as well as all hard-coded devices. The router is configured to pass the DHCP request to the server using helper-address entries in the router's virtual interfaces.

```
interface Vlan70
 description Sales
 ip address xxx.xxx.70.1 255.255.255.0
 ip access-group 101 in
 ip access-group 101 out
 ip helper-address xxx.xxx.13.11
 ip helper-address xxx.xxx.13.12
```

Design Figure 3

Summary

In this step, we replace the hubs with switches and move the workgroup server connections to the Cisco 6500 switch/router. We will implement port security[3] on the connections for the servers and 802.1x[4] security on the ports on the workgroup switches.



Detail

The hubs are removed and replaced with Cisco 4000, 3550 or 2950 series switches depending on network needs. I will concentrate on the Cisco 4000 series switch in this example. These switches are connected via gigabit uplinks to the core route/switch and trunks are configured on these connections to allow multiple VLAN support in the workgroups. The modules installed in the 4000 are of the type that provides in-line power in order to support devices such as wireless access points (WAP) without the need of supplying external power.

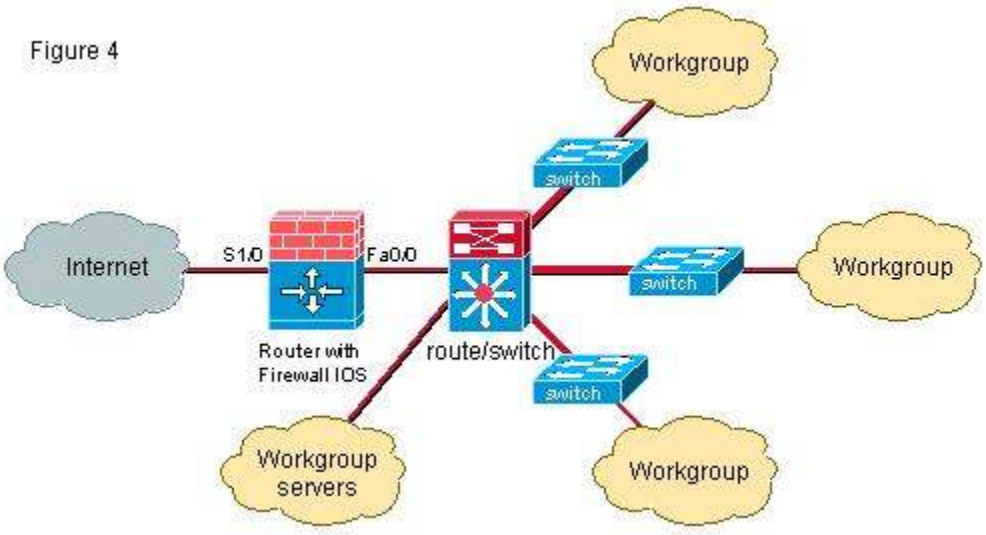
Workgroup servers are moved to a secure access area and directly-connected to the Cisco 6500 core route/switch. We will place the servers in a location where physical access is controlled and limited to authorized personnel. Port security is enabled on these connections to lock down the ports and all ports without an active connection are disabled.

On the Cisco 4000 workgroup switches, 802.1x security is enabled to secure these ports. Since 802.1x security is enabled on these ports, there is not a need to disable the unused ports on the switches. VLAN Access Control Lists (VACLs) were configured to provide an additional level of defense.

Design Figure 4

Summary:

In this step, we replace the internet router with a router with firewall feature set IOS.



Detail:

The internet router is replaced with a Cisco 3600 series router with firewall feature set IOS and Context-Based Access Control (CBAC)[5] is implemented on the router. CBAC will allow outbound traffic and will dynamically configure the inbound ACL on the internet side of the router to allow responding traffic back to the internal network. CBAC has extended the packet-filtering function to include the application layer which allows it to monitor the state of the individual sessions. CBAC can effectively combat denial-of-service (DoS) attacks by the use of session threshold and timeout settings. CBAC can drop half-open sessions, warn you of a dramatic increase in the number of sessions and also drop fragmented packets that are of a suspicious nature. CBAC can be configured to log session and network activity.

In addition to the use of CBAC, best practice policy will dictate the use of some additional protections such as:

- no ip redirect
- no icmp redirect
- no ip source-route
- no service finger
- no ip directed-broadcast
- no service tcp-small-services
- no service udp-small-services
- access-list <extended access list number> deny ip <internal network> any
- no cdp run

Note: If CDP is needed on the internal network, then instead of the global 'no cdp run' you can disable CDP on the external interface.

Please refer to http://www.iana.org/assignments/port-numbers[6] for a list of well known port numbers to aid in the configuration of the ACLs. IANA manages assigned ports in the range from 0 to 1023. An ACL is applied on the internet side inbound to the router and is configured to deny all traffic except what is explicitly permitted in the list.

Here is an example of how the ACL is configured, this list will be applied inbound on the external interface:

```
access-list 111 remark – Apply inbound on external interface
access-list 111 deny tcp any any
access-list 111 deny udp any any
access-list 111 remark – Permit necessary ICMP responses
access-list 111 permit icmp any any echo
access-list 111 permit icmp any any echo-reply
access-list 111 permit icmp any any time-exceeded
```

```
access-list 111 permit icmp any any traceroute
access-list 111 permit icmp any any unreachable
access-list 111 permit icmp any any packet-too-big
access-list 111 permit icmp any any administratively-prohibited
access-list 111 deny icmp any any
access-list 111 deny ip any any

! Router's external interface
interface serial 1/0
ip access-group 111 in
```

We must make sure the ACL on the internet side is configured to permit inbound traffic to the Web, FTP, DNS and e-mail servers[7] until they are moved as shown in figure 5. Here is a brief list of ports that will need to be permitted inbound from the internet.

Port #	Description
20	File Transfer [Default Data] -- FTP
21	File Transfer [Control] -- FTP
25	Simple Mail Transfer -- SMTP
53	Domain Name Service -- DNS
80	World Wide Web -- HTTP
443	http protocol over -- TLS/SSL

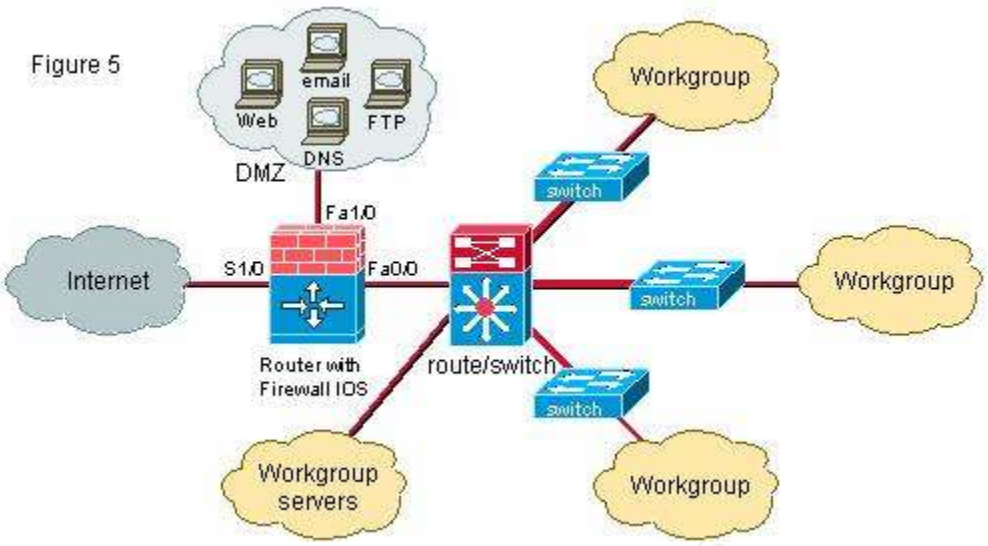
Configure the ACL inbound from the internet on the external interface to permit Web, FTP, SMTP and DNS traffic to the internal network. Configure the outbound ACL on the external interface to permit Web, FTP, DNS and SMTP destined for the internet on the internal network. In addition, configure the ACL to permit syslog to the internal syslog server or servers.

Design Figure 5

Summary

Create a DMZ[8] and move the Web, FTP, DNS and email servers there.

Figure 5



Detail

In this step, a DMZ[9] is created and devices such as web servers, FTP servers, e-mail servers and DNS servers are moved into this zone. These servers will reside in a secure area that is access controlled for only authorized personnel. This design is called a tri-homed DMZ and we will take one subnet from the internal class B and use it for this network in order for the devices in the DMZ to have public addresses.

NETWORK MANAGEMENT

CiscoWorks

The CiscoWorks2000 LAN Management Solution (LMS)[10] package is an excellent tool to monitor and manage a Cisco-based network. It has many features that will automatically execute or report on actions or faults occurring on the network.

Campus Manager

Campus Manager is a Web-based layer 2 management tool and is included with CiscoWorks2000. It can be used for monitoring and configuring devices in the network infrastructure. Campus Manager will perform layer 2 discovery and map all devices on the network and include the current user logged on to the device and maps the relationship to the Media Access Control (MAC) address and the switch down to port level. Layer 2 topology maps show the status and

connections of the devices and can be displayed in various ways. There is a menu selection to export topology maps to Visio.

Device Fault Manager

Device Fault Manager (DFM) is integrated with CiscoWorks2000 and monitors Cisco devices providing fault analysis and will send traps to the DFM alarm window or send to e-mail or pagers. DFM provides layer 2 and layer 3 support for Cisco devices and integrates with some enterprise network management systems.

Resource Manager Essentials

Resource Manager Essentials (RME) like Campus Manager, is a group of Web-based tools for Cisco devices. RME is accessed via a browser interface and provides access to important network information. RME provides information management on device configuration, device availability, configuration change audit, software image and inventory management.

CiscoView

CiscoView is another Web-based application that is included with CiscoWorks2000 and can be accessed via other applications such as Campus Manager. CiscoView will display a physical view of the device, such as a switch or router, and will allow monitoring and changes to be made by clicking the port involved. Ports are color-coded to indicate if they are up, down or disabled. Some of the changes possible are VLAN assignments, port speed and duplex settings. CiscoView also has a provision that allows access to Cisco's web site.

nGenius Real-Time Monitor

The nGenius Real-Time Monitor (RTM) application is included with CiscoWorks2000 via a Web interface. RTM provides access to information for troubleshooting, monitoring and analyzing the network. It has a packet analyzer and traffic monitor with graphic reporting capabilities. The devices that can be accessed to gather this information include RMON-enabled data from Catalyst switches, Network Analysis Modules (NAMs) and Switch Probes.

SECURITY POLICY

A security policy should be developed and approved to authenticate the features and measures presented in this paper. As an example, if the firewall is breached; What actions should be taken? Who should be notified? What is the procedure to follow to prevent a reoccurrence of the problem? If risks are

identified; What is the procedure to follow to manage or mitigate the risk? A well-written security policy would answer these questions and provide protection to all involved. If the work you do is not covered in a written official security policy, you should at least write a Personal Security Policy for yourself according to your job function.

PROBLEM RESOLUTION

The initial configuration that is shown in Figure 1, consisted of a bridged internal network with hubs connecting the workgroups and one router for connection to the internet. The router was configured with ACLs that permitted all traffic and to deny what was considered unwanted traffic. In addition, all the workgroup servers, as well as the servers requiring inbound access from the internet, were also connected to this bridged network.

The bridge was removed and replaced with a Cisco 6500 series switch/router which was configured with EIGRP Appletalk and IP routing. Zones and cable ranges were set up for the Appletalk network to define routing to for the workgroups. VLANs were configured on the switch/router to segment traffic to the workgroups

Next, the hubs were replaced with Cisco 4000 series switches with gigabit uplinks to the core 6500 switch. These connections were configured as trunks to allow multiple VLAN connections to the workgroups. The workgroup servers were moved to a secure area that is access-controlled and only authorized personnel are admitted. These servers were connected directly to the core 6500 switch and port security was enabled to secure their connection. The user connections to the 4000 switches were secured with the implementation of 802.1x configuration.

Finally, the existing router was replaced with a Cisco 3600 series router configured with firewall feature set IOS and a DMZ was created and devices such as the Web server, the FTP server, the e-mail server and the DNS server were placed there. CBAC was configured to permit outbound traffic from the internal network and only permit return traffic back in from the internet. An ACL was configured and implemented on the external interface inbound from the internet to deny all traffic and only permit specific traffic from the internet to the DMZ servers and deny internet-initiated traffic destined for the internal network. Another ACL was configured and applied inbound on the interface of the DMZ to permit traffic such as SSH and syslog to certain network management servers on the internal network.

CiscoWorks2000 was used as the Network Management solution to further enhance the security of the network. CiscoWorks2000 monitors version information of the software in the switches and routers and will maintain copies of

configurations which allow one to go back to the previous configuration in case a problem arises from the new version. Syslog information from routers, switches and servers is fed to the CiscoWorks2000 program for tracking and analysis.

CONCLUSION

In conclusion, the final network design has enhanced the security of the network. The problem of having a single line of defense that existed in the beginning was solved by adding a core switch/router that is configured with ACLs in the router as well as VACLs in the switch. Increased overall security was achieved by the addition of the Cisco 3600 series router running firewall feature set IOS and by the creation of the DMZ and locating the public-accessible servers there. Internal security was improved by physically locating the public-accessible servers and the workgroup servers to a secure location that is access controlled admitting only authorized personnel.

Security at the workgroup server level was strengthened by configuring and enabling port security on their connections to the core switch/router. Security at the workgroup user level was enhanced by the implementation of 802.1x on their connections to the workgroup switches.

The security course developed and presented by SANS for the GSEC security certification proved an invaluable aid in the configuration of the devices presented in this paper.

REFERENCES

[1] Configuring IP Access Lists
http://cisco.com/warp/public/707/confaccesslists.html

[2] Enhanced Interior Gateway Routing Protocol
http://www.cisco.com/warp/public/103/eigrp-toc.html

[3] Cisco Catalyst 6000 Series Switches – Configuring Port Security
http://www.cisco.com/en/US/products/hw/switches/ps700/products_configuration_guide_chapter09186a008007fa13.html

[4] Cisco Catalyst 4000 Series Switches – Configuring 802.1x Port-Based Authentication
http://www.cisco.com/en/US/products/hw/switches/ps663/products_configuration_guide_chapter09186a00800ddb0d.html

[5] Configuring Context-Based Access Control – Cisco
http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/secur_c/scprt3/sccbac.htm

[6] IANA assigned well known port numbers
http://www.iana.org/assignments/port-numbers

[7] Requirements for Internet client software, Telnet, FTP, SMTP, and DNS
http://www.cis.ohio-state.edu/cgi-bin/rfc/rfc1123.html

[8] Designing a DMZ
http://www.sans.org/rr/firewall/DMZ.php

[9] Building a Perimeter Security Solution with the Cisco Secure Integrated Software
http://www.cisco.com/warp/public/cc/pd/iosw/ioft/iofwft/tech/firew_wp.htm

[10] CiscoWorks LAN Management Solution
http://www.cisco.com/warp/public/cc/pd/wr2k/lnmn

Last Updated: May 27th, 2017

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Madrid 2017	Madrid, ES	May 29, 2017 - Jun 03, 2017	Live Event
SANS Atlanta 2017	Atlanta, GAUS	May 30, 2017 - Jun 04, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CAUS	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DCUS	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TXUS	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Milan 2017	Milan, IT	Jun 12, 2017 - Jun 17, 2017	Live Event
SEC555: SIEM-Tactical Analytics	San Diego, CAUS	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Charlotte 2017	Charlotte, NCUS	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Secure Europe 2017	Amsterdam, NL	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, COUS	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MNUS	Jun 19, 2017 - Jun 24, 2017	Live Event
DFIR Summit & Training 2017	Austin, TXUS	Jun 22, 2017 - Jun 29, 2017	Live Event
SANS Paris 2017	Paris, FR	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, AU	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MDUS	Jun 26, 2017 - Jul 01, 2017	Live Event
SEC564:Red Team Ops	San Diego, CAUS	Jun 29, 2017 - Jun 30, 2017	Live Event
SANS London July 2017	London, GB	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, JP	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, SG	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Los Angeles - Long Beach 2017	Long Beach, CAUS	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS ICS & Energy-Houston 2017	Houston, TXUS	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, DE	Jul 10, 2017 - Jul 15, 2017	Live Event
SANSFIRE 2017	Washington, DCUS	Jul 22, 2017 - Jul 29, 2017	Live Event
Security Awareness Summit & Training 2017	Nashville, TNUS	Jul 31, 2017 - Aug 09, 2017	Live Event
SANS San Antonio 2017	San Antonio, TXUS	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, CZ	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MAUS	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Hyderabad 2017	Hyderabad, IN	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UTUS	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NYUS	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Chicago 2017	Chicago, ILUS	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Adelaide 2017	Adelaide, AU	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Stockholm 2017	OnlineSE	May 29, 2017 - Jun 03, 2017	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced