Interested in learning more about security?

SANS Institute InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

No Budget, No Policy: Leading the Bull by the Nose or Thank God for the Cisco IOS Firewall Feature S

As much as we'd like to think, everyone else is as security conscious as the SANS' community, that's just not the case. I know, I come from one such organization. We are a small to mid size with approximately 90 users. One of our smaller programs secured a federal grant to do some work with HIV positive clients (HIPAA driven). Part of the grant requirements require network security be implemented to protect client identifiers. I was the network administrator at the time and our organization immediately decided to inclu...

Copyright SANS Institute

Author Retains Full Rights

AD

No Budget, No Policy: Leading the Bull by the Nose or Thank God for the Cisco IOS Firewall Feature Set

As much as we'd like to think, everyone else is as security conscious as the SANS' community, that's just not the case. I know, I come from one such organization. We are a small to mid size with approximately 90 users. One of our smaller programs secured a federal grant to do some work with HIV positive clients (HIPAA driven). Part of the grant requirements require network security be implemented to protect client identifiers.

I was the network administrator at the time and our organization immediately decided to include "network security" as part of my job description. I was sent to my first SANS conference (this was suggested by the grant proposal guidelines). There I got a real taste of security and what it means. Among the many things that were hammered into us at the conference was: you need CEO (top management) buy-in and that you have to do a "needs assessment" and turn that into a security policy.

This didn't seem all that bad as the grant proposal required that we develop a security policy. Upon returning, I was included in the security committee. We were tasked with the development of a policy for our organization. This process, by itself, could lead to another story but in summary let's just say we produced a watered down security policy. This was then presented to our CEO along with the Executive committee. After explaining risk management and assessment to them, they decide that the organization wide security policy would state, "we are not implementing any security measures and that if other programs within the organization needed additional protection they need to come up with their own security policy to cover them."

This is were it got interesting. When I told the Program that had secured the Grant that they needed to develop a security policy to cover themselves per the organizational policy. They replied back, we wrote in the grant that we have a written security policy. I informed them that the only "written policy" that the organization came up with was, in fact, that we don't have one. They then look at me and said, well … you're in charge of network security.

It was at this time that I was told that there was some money available for updating our network infrastructure. Everyone in our organization is addicted to two network applications, Internet browsing and email. So when I ask to spend the money on upgrading our perimeter Cisco router going into the Internet, I was given the green light.

I decided on a Cisco router 2651 with version 12.2.1 of the IOS with the following feature pack, ENTERPRISE/FW/IDS PLUS IPSEC 56 with additional RAM. So while the organization viewed this as getting a better router (which it was), I had tacked on (or piggy-backed) the ability to add security features onto our network. The Cisco IOS Firewall feature set adds the additional functionality of:

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

- Standard access lists and static Extended access lists – This allows you to do simple or complex packet filtering of network traffic based on TCP/IP protocols (layers 3 & 4 of the OIS model) or by network/host.
- Lock-and-Key (dynamic access lists) – Allows for temporary opening in the firewall for certain individuals after they have authenticated.
- Reflexive access lists – This will allow traffic into your network only if the session had originated from inside of your network.
- TCP Intercept – This watches for TCP sync flooding attacks (Denial of Service).
- Context-Based Access Control – This type of filtering not only examines Layers 3 & 4 but also the application protocols (i.e. FTP, POP, IMAP, HTTP, etc.). It maintains a table of state information for individual sessions. This table is then used to determine if traffic should be permitted and, if so, will make temporary holes in the firewall to allow it to pass through.
- Security server support – Allow router to be configured as a client for various types of security servers (TACACS, RADIUS, and Kerberos) which can then be used to control access.
- Network Address Translation – A means of cloaking your internal network by substituting a legitimate "public" IP address for your internal "private" IP addresses.
- Cisco Encryption Technology – Cisco's proprietary protocol that encrypts packets that travel across unprotected networks (Internet).
- IPSec network security – An open standard that provides for the encryption of data between two peers.
- Neighbor Router Authentication – Requires router to authenticate before accepting updates to the router table from them.
- Event Logging - automatically logs output from system error messages and other events to the console terminal.
- User authentication and authorization – Helps protect router from unauthorized access.

So now, with all this additional security functionality, what can I do given that our organizations security policy basically states, "everyone is allow to do everything".

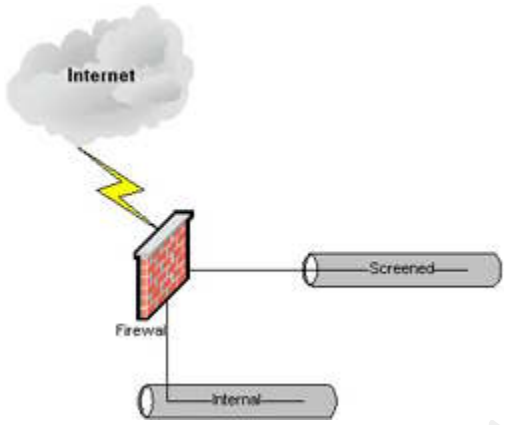
One of the first things that come to mind is Network Address Translation (NAT). RFC 1918 provides for non-routable (over the Internet) IP address that can be used on the internal network. With NAT, your internal non-routable IP addresses are substituted at the router for legitimate IP addresses and then are sent out to the Internet. When the packets return the router looks at its translation table to see where to send the packet internally. From a security perspective, this would hide your internal network from the Internet. The Internet side would only be able to see the legitimate IP addresses that the router was sending.

Next I decided to use Cisco's access lists to implement Egress and Ingress filtering. Egress filtering tells the router to only allow packets going out if the source address originated from the internal network. And Ingress tells the router to drop any packets

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

coming into our network that have our own internal IP address as the source. From a security perspective Egress stops Denial of Service attacks from being launched from our network and Ingress stops spoofed packets from getting into our network.

The next part involves setting up a firewall features on our router. Although I was told our user should be able to anything they want, I was not given any specific guidance on what should be allowed from the outside (Internet). I took the liberty in assuming that blocking outside access to our internal network would not violate our Policy. I further decided that traffic originating from our public servers (Screened segment) should not be able to initiate traffic back into the internal network or onto the Internet. Then should these servers (WWW or RealAudio) be compromised, hacker would not be able to launch an attack from them to either the Internet or our internal network. In simplistic terms we could view the network as such.

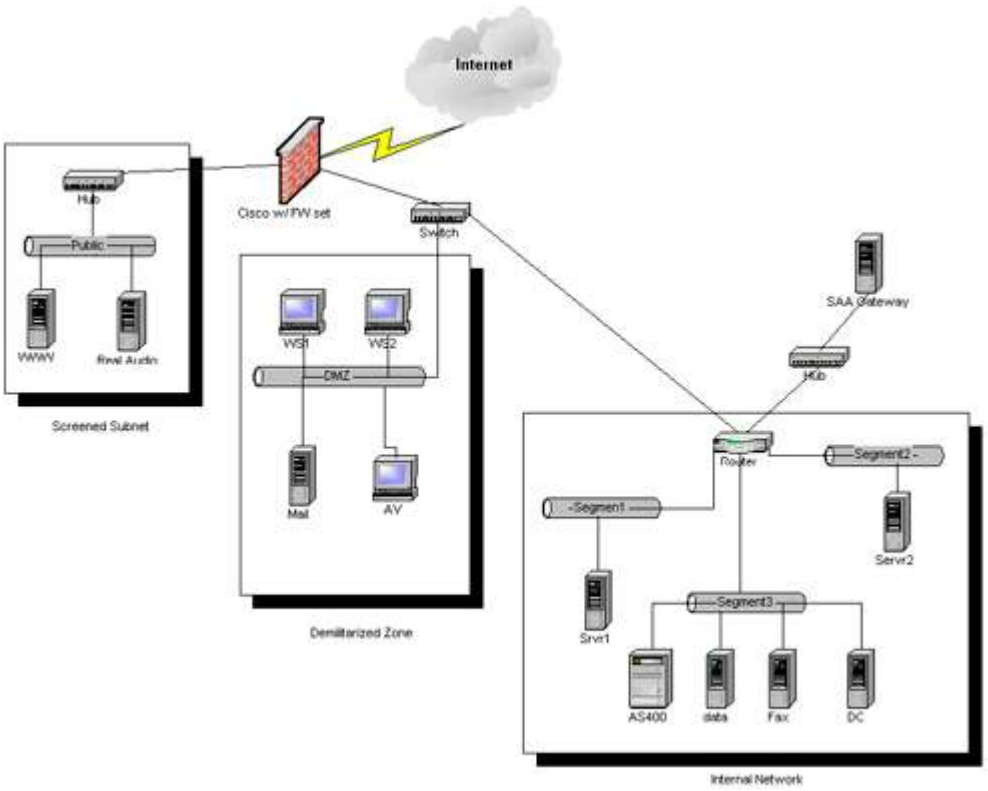


We can now make some generalizations regarding which segments can initiate traffic onto the other segments, and present this in table form. This will be helpful in both documenting and configuring the Firewall on the router.

	To **Internet**	To **Screened**	To **Internal**
Internet initiated	N/a	filtered	no
Screened initiated	no	N/a	no
Internal initiated	All	All	N/a

Please refer to network diagram below for sanitized representation of our network. The networked segment labeled “Public” below is the same on we referred to as “Screened” above. The commands for the Cisco Firewall set can be pretty intimidating. So if you are not a Cisco “guru”, I would suggest that you use Cisco’s ConfigMaker. Configmaker is a software application that uses the “wizard” approach.

© SANS Institute 2001, Author retains full rights.



Configmaker generated the following configuration for my perimeter router. Notice the "inspect" statements. These are commands for Cisco's Context-Based Access Control (CBAC). CBAC filters packets based on application-layer protocol session information. They can be used for general session maintenance, prevention of certain Denial of Service attacks, logging, and to open temporary holes in firewall for allowed traffic to pass through. Additional comments (documentation) provided by me are in purple.

```
!
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
! Turn off unnecessary services
!
! turn off tcp services not used
! Echo, Chargen, Discard, and Daytime
no service tcp-small-servers
! turn off udp services not used
! Echo, Chargen, Discard
no service udp-small-servers
! other services not needed that come
! turned on by default.
no service finger
no ip bootp server
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
!
hostname Perimeter_router
!
enable password xxxxxxx
!
no ip source-route
no ip name-server
!
ip subnet-zero
no ip domain-lookup
ip routing
!
! Context-Based Access Control
!
! start logging
ip inspect audit-trail
!
! General session maintenance
!
! Time to wait for TCP session to reach established
! state before dropping.
ip inspect tcp synwait-time 30
! Time TCP session will be managed after
! receiving FIN.
ip inspect tcp finwait-time 5
! Time TCP session will be manage after no activity.
ip inspect tcp idle-time 3600
! Time UDP session will be manage after no activity.
ip inspect udp idle-time 30
! Time DNS lookup session will be manage after no activity.
ip inspect dns-timeout 5
!
! DoS attack thresholds
!
! Defines the limits for triggering deletion of existing
! half-open sessions.
ip inspect one-minute low 900
ip inspect one-minute high 1100
ip inspect max-incomplete low 900
ip inspect max-incomplete high 1100
ip inspect tcp max-incomplete host 50 block-time 0
!
! IP inspect FastEthernet_0_0
! Will record the following application sessions
! and open up temporary holes in firewall.
! Will be applied to Fastethernet 0/0.
```

© SANS Institute 2001, Author retains full rights

```
!
no ip inspect name FastEthernet_0_0
ip inspect name FastEthernet_0_0 tcp
ip inspect name FastEthernet_0_0 udp
ip inspect name FastEthernet_0_0 cuseeme
ip inspect name FastEthernet_0_0 ftp
ip inspect name FastEthernet_0_0 h323
ip inspect name FastEthernet_0_0 rcmd
ip inspect name FastEthernet_0_0 realaudio
ip inspect name FastEthernet_0_0 smtp
ip inspect name FastEthernet_0_0 streamworks
ip inspect name FastEthernet_0_0 vdolive
ip inspect name FastEthernet_0_0 sqlnet
ip inspect name FastEthernet_0_0 tftp
!
! IP inspect Serial_0_0_1
! Will record the following application sessions
! and will open up temporary holes in firewall.
! Will be applied to Serial 0/0.1
!
no ip inspect name Serial_0_0_1
ip inspect name Serial_0_0_1 tcp
ip inspect name Serial_0_0_1 realaudio
ip inspect name Serial_0_0_1 smtp
!
interface FastEthernet 0/0
 no shutdown
 description internal network
 ! Subnet off private address space 10.x.x.x
 ip address 10.25.0.1 255.255.0.0
 ! Use Network Address Translation on
 ! this interface.
 ip nat inside
 ! Record session information to open
 ! temporary holes in the firewall, used by CBAC.
 ip inspect FastEthernet_0_0 in
 ! Apply Egress filtering.
 ip access-group 101 in
 keepalive 10
!
interface FastEthernet 0/1
 no shutdown
 description Screened subnet
 ! This subnet house services which we offer to Internet.
 ip address 209.20.146.135 255.255.255.224
 ! Stop traffic initiating on this interface to
```

© SANS Institute 2001, Author retains full rights

```
 ! Internet and internal network.
 ip access-group 100 in
 keepalive 10
!
interface Serial 0/0
 no shutdown
 no description
 no ip address
 encapsulation frame-relay
 frame-relay lmi-type ansi
!
interface Serial 0/0.1 point-to-point
 no shutdown
 description Internet
 ip address 209.20.128.145 255.255.255.252
 ! apply NAT translation to the Internet
 ip nat outside
 ! check for and record allowed traffic in
 ! from the Internet (CBAC)
 ip inspect Serial_0_0_1 in
 ! Apply Ingress filtering
 ip access-group 102 in
 frame-relay interface-dlci 19
!
! Access Control List 1
!
! For use by NAT
!
no access-list 1
access-list 1 permit 10.25.0.0 0.0.255.255
access-list 1 permit 10.1.0.0 0.0.255.255
access-list 1 permit 10.5.0.0 0.0.255.255
!
! Access Control List 100
! Applied to FastEthernet 0/1 in
!
no access-list 100
access-list 100 deny ip 10.25.0.0 0.0.255.255 any
access-list 100 deny ip 10.1.0.0 0.0.255.255 any
access-list 100 deny ip 10.5.0.0 0.0.255.255 any
access-list 100 permit udp any eq rip any eq rip
!
! Access Control List 101
! Applied to FastEthernet 0/0 in
!
no access-list 101
```

© SANS Institute 2001, Author retains full rights

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
access-list 101 deny ip 209.20.146.128 0.0.0.31 any
access-list 101 permit ip any any
!
! Access Control List 102
! Applied to Serial 0/0.1 in
!
no access-list 102
access-list 102 deny ip 209.20.146.128 0.0.0.31 any
access-list 102 deny ip 10.0.0.0 0.0.0.255 any
access-list 102 permit tcp any 209.20.146.128 0.0.0.31 eq 80
access-list 102 permit tcp any 209.20.146.128 0.0.0.31 eq 110
access-list 102 permit tcp any 209.20.146.128 0.0.0.31 eq 7070
access-list 102 permit tcp any 209.20.146.128 0.0.0.31 eq 25
!
! Dynamic NAT
! Configure for NAT
!
ip nat translation timeout 86400
ip nat translation tcp-timeout 86400
ip nat translation udp-timeout 300
ip nat translation dns-timeout 60
ip nat translation finrst-timeout 60
ip nat pool Org_rtr2-natpool-1 209.20.146.150 209.20.146.158 netmask
255.255.255.224
ip nat inside source list 1 pool Org_rtr2-natpool-1 overload
!
router rip
 version 2
 network 10.0.0.0
 network 209.20.146.0
 passive-interface Serial 0/0.1
 no auto-summary
!
!
ip classless
!
! IP Static Routes
ip route 0.0.0.0 0.0.0.0 Serial 0/0.1
no ip http server
snmp-server location ISP border
snmp-server contact Joe Routerman
!
line console 0
 exec-timeout 0 0
 password xxxxxx
 login
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
!
line vty 0 4
 password xxxxxx
 login
!
end
```

After implementing the above on my router, I launched into a crusade to increase awareness of security throughout my organization. Every time I got called into a meeting dealing with the network or security I brought diagrams of the firewall's implementation and pointed out to management that without any guidance, I implemented as much protection as I could without violating their written security policy. I explained to them how we were stopping spoofing (Ingress), stopping DoS attacks from originating from our network (Egress), cloaking our internal network IP address from the outside (NAT), and stopping the hackers from accessing our internal network from the Internet (CBAC). And all this was done without affecting our internal users. After selling this for the last couple of months, I now have the CIO referring to this as our Organization's security policy and he has started the process of documenting it so that it can be formalized into the written policy.

Looking back on this process I can see a couple of important lessons learned. Foremost, security is a very complex subject and a lot of smart people, for whatever reasons, just don't understand what it is, how important it is, or how to come up with or even get started with a security policy. You will constantly have to raise their awareness on this subject. Lastly, even if your organization fails to give you a good/any policy there are still a lot of security features that can be implemented onto any network without limiting what your users can do. In the above example I converted our perimeter router into a stateful firewall. Although the can hardly be considered as securing the subnet containing the Program that secured the Grant, it is none-the-less a very good first start.

From this stance it has been much easier to talk with the Program that secured the Grant, explaining what we have done and what we perceive to be their remaining risks. I'm happy to say that they have come up with their own draft Security Policy and funding to purchase a Firewall to be place between them and our internal network. For this reason, I am thankful that Cisco has a Firewall feature set that is capable of changing a normal router into a stateful firewall.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Resources

SANS Security Institute
URL:http://www.sans.org/newlook/home.htm

Health Care Financing Administration,
"The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Page"
URL:http://www.hcfa.gov/hipaa/hipaahm.htm

Cisco Systems
URL:http://www.cisco.com/

Cisco Systems, "Cisco IOS Firewall Feature Set Cisco IOS Firewall Feature Set"
URL:http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t3/fw7200.htm

Cisco Systems, "Access Control Lists: Overview and Guidelines"
URL:http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/secur_c/scprt3/scdacls.htm

Unix Workstation Support Group, "ISO/OSI Network Model"
URL: http://www.uwsg.iu.edu/usail/network/nfs/network_layers.html

Cisco Systems, "Lock-and-Key: Dynamic Access Lists"
URL: http://www.cisco.com/warp/public/69/13.html

Cisco Systems, "Configuring IP Session Filtering (Reflexive Access Lists)"
URL:http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113ed_cr/secur_c/scprt3/screflex.htm

Cisco Systems, "Configuring TCP Intercept (Prevent Denial-of-Service Attacks)"
URL:http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/secur_c/scprt3/scdenial.htm

Cisco Systems, "Context-Based Access Control"
URL:http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t5/iosfw2/iosfw2_2.htm

Cisco Systems, "Configuring TACACS and Extended TACACS"
URL:http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113ed_cr/secur_c/scprt2/sctcacs.htm

Cisco Systems, "Remote Authentication Dial-In User Service (radius)"
URL:http://198.69.98.2/~newwave/radius.html

© SANS Institute 2001, Author retains full rights.

Massachusetts Institute of Technology, “Kerberos: The Network Authentication Protocol”
URL:http://web.mit.edu/kerberos/www/

Cisco Systems, “Configuring Network Address Translation: Getting Started”
URL:http://www.cisco.com/warp/public/556/12.html

Cisco Systems, “Cisco IOS Software Feature: Network-Layer Encryption”
URL:http://www.cisco.com/warp/public/cc/so/neso/sqso/eqso/encrp_wp.htm

Cisco Systems, “IP Security Protocol (ipsec)”
URL:http://www.ietf.org/html.charters/ipsec-charter.html

Cisco Systems, “Neighbor Router Authentication: Overview and Guidelines”
URL:http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113ed_cr/secur_c/scprt5/scrouter.htm

Egevang, "The IP Network Address Translator (NAT)", May 1994.
URL: http://www.ietf.org/rfc/rfc1631.txt

Rekhter, “Address Allocation for Private Internets”, February 1996
URL: http://www.ietf.org/rfc/rfc1918.txt

Cisco Systems, “Configuring Access Control Lists”
URL:http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw_5_4/msfc/acc_list.htm

SANS Security Institute, “Cisco Anti-Spoof Egress Filtering”, March 2000
URL:http://www.sans.org/dosstep/cisco_spoof.htm

Ferguson, “Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing”, January 1998
URL:http://www.landfield.com/rfcs/rfc2267.html

Cisco Systems, “Cisco ConfigMaker”
URL:http://www.cisco.com/univercd/cc/td/doc/clckstrt/cfgmkr/

Cisco Systems, “The Cisco IOS Firewall Feature Set and Context-Based Access Control”
URL:http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113t/113t_3/firewall.htm

Cisco Systems, Inc. Cisco IOS 12.0 Network Security. Indianapolis, IN: Cisco Press, 1999

© SANS Institute 2001, Author retains full rights.

Last Updated: May 21st, 2018

Upcoming SANS Training

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

SANS Atlanta 2018	Atlanta, GAUS	May 29, 2018 - Jun 03, 2018	Live Event
SEC487: Open-Source Intel Beta Two	Denver, COUS	Jun 04, 2018 - Jun 09, 2018	Live Event
SANS Rocky Mountain 2018	Denver, COUS	Jun 04, 2018 - Jun 09, 2018	Live Event
SANS London June 2018	London, GB	Jun 04, 2018 - Jun 12, 2018	Live Event
DFIR Summit & Training 2018	Austin, TXUS	Jun 07, 2018 - Jun 14, 2018	Live Event
Cloud INsecurity Summit - Washington DC	Crystal City, VAUS	Jun 08, 2018 - Jun 08, 2018	Live Event
Cloud INsecurity Summit - Austin	Austin, TXUS	Jun 11, 2018 - Jun 11, 2018	Live Event
SANS Milan June 2018	Milan, IT	Jun 11, 2018 - Jun 16, 2018	Live Event
SANS Cyber Defence Japan 2018	Tokyo, JP	Jun 18, 2018 - Jun 30, 2018	Live Event
SANS Oslo June 2018	Oslo, NO	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Philippines 2018	Manila, PH	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS ICS Europe Summit and Training 2018	Munich, DE	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Crystal City 2018	Arlington, VAUS	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Minneapolis 2018	Minneapolis, MNUS	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS Cyber Defence Canberra 2018	Canberra, AU	Jun 25, 2018 - Jul 07, 2018	Live Event
SANS Paris June 2018	Paris, FR	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS Vancouver 2018	Vancouver, BCCA	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS London July 2018	London, GB	Jul 02, 2018 - Jul 07, 2018	Live Event
SANS Cyber Defence Singapore 2018	Singapore, SG	Jul 09, 2018 - Jul 14, 2018	Live Event
SANS Charlotte 2018	Charlotte, NCUS	Jul 09, 2018 - Jul 14, 2018	Live Event
SANSFIRE 2018	Washington, DCUS	Jul 14, 2018 - Jul 21, 2018	Live Event
SANS Cyber Defence Bangalore 2018	Bangalore, IN	Jul 16, 2018 - Jul 28, 2018	Live Event
SANS Malaysia 2018	Kuala Lumpur, MY	Jul 16, 2018 - Jul 21, 2018	Live Event
SANS Pen Test Berlin 2018	Berlin, DE	Jul 23, 2018 - Jul 28, 2018	Live Event
SANS Riyadh July 2018	Riyadh, SA	Jul 28, 2018 - Aug 02, 2018	Live Event
Security Operations Summit & Training 2018	New Orleans, LAUS	Jul 30, 2018 - Aug 06, 2018	Live Event
SANS Pittsburgh 2018	Pittsburgh, PAUS	Jul 30, 2018 - Aug 04, 2018	Live Event
SANS August Sydney 2018	Sydney, AU	Aug 06, 2018 - Aug 25, 2018	Live Event
SANS San Antonio 2018	San Antonio, TXUS	Aug 06, 2018 - Aug 11, 2018	Live Event
SANS Boston Summer 2018	Boston, MAUS	Aug 06, 2018 - Aug 11, 2018	Live Event
SANS Hyderabad 2018	Hyderabad, IN	Aug 06, 2018 - Aug 11, 2018	Live Event
Security Awareness Summit & Training 2018	Charleston, SCUS	Aug 06, 2018 - Aug 15, 2018	Live Event
SANS Amsterdam May 2018	OnlineNL	May 28, 2018 - Jun 02, 2018	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced