SANS Institute
InfoSec Reading Room

Microsoft Vista Firewall; Dissected

, or a single vendor solution may have some organizations considering a change....

“Microsoft Vista Firewall; Dissected”

Phil Kostenbader & Bob Rudis

Overview

The firewall provided by Microsoft has pretty much gone unchanged since windows 2000. Their release of the firewall included with Vista, however, has seen a few new and useful features. Under the right environment, it may be possible for large organizations to make use of this facility. But why would an organization consider dropping their current solution? Flexibility in the rule construction, the ability to apply a specific policy based on 'domain' authentication, multiple methods of policy distribution, or a single vendor solution may have some organizations considering a change.

The Firewall

What is provided by Microsoft is a basic, simple, old fashion, traditional packet blocking, port based firewall. Like many third party firewall solutions, Microsoft now allows rule creation based on application, port, interface and IP Address based rules. For example one can create a rule to restrict access by IP Address and port to a service:

```
allow inbound from 192.168.0.0/32 TCP port 800 to
C:\cygwin\user\sbin\sshd.exe
```

There is little in the area of packet inspection, although it does recognize various protocols for example IGMP, GRE, and ESP.

```
Previous Microsoft firewalls could detect various
protocols, but only be configured to allow/deny.
```

While similar to the previous versions, protocols now can be restricted or bound to applications and an IP address range. In addition the ICMP protocol is now specifically supported allowing filtering by ICMP type.

The Vista Firewall configuration breaks rules into three separate groups: input, output and connection security. The input and output groups are used for input and output packets respectively. The connection security group allows authentication between two devices and communications via IPsec.

Two GUIs and a command line interface allow for manipulation of the firewall; a general configuration via the control panel and *windows firewall with advanced features*, available through the control panel -> administrative tools. By using the *firewall with advanced features* GUI it is observed that many rules are already defined. The first useful feature of the Vista firewall is the import/export policy facility. This can be done through the GUI or command line

```
netsh advfirewall export “c:\poo.wfw”
```

Exporting the existing default rules can be done should one consider starting over.

```
Exporting of the policy will include all three rule groups and
all configured options
```

The command line interface also allows the use of a reset, which also brings the firewall back to its default rules.

```
netsh advfirewall reset
```

The pain staking task of removing the default rules will be necessary in order to start from a clean slate. Once done, saving or exporting this blank policy may be useful if testing is expanded to other devices. Without any defined rules an important characteristic can now be tested; a tool such as nmap can be used to verify the default action of the firewall – inbound blocked and outbound traffic and protocols are allowed. These defaults can be changed through *windows firewall properties* area in the advanced GUI.

The following assumptions will be made in order to highlight the key feature of this firewall:

- active directory is supported
- all outbound traffic from the PC will be permitted
- all inbound traffic will be blocked using the default settings
- the organization has special needs in the area of file sharing among PCs and the support of various service oriented applications.
- VPN software to allow remote access.
- PC with LAN and WLAN interfaces
- backed WLAN test segment. This segment is NOT connected to the organization's primary network.
- Backed LAN test segment. This segment is NOT connected to the organization's primary network.
- A fixed firewall policy allowing all inbound traffic when authenticated to a DOMAIN and all inbound blocked when not.

Input and output rule groups can now be populated, starting with outbound. Rules can be created to allow all outbound TCP, UDP and ICMP traffic or the *windows firewall properties* can be set to allow outbound.

Inbound rules can now be defined, which reveal an interesting new feature offered by this firewall solution. Any rule, regardless of the group it is defined in, can be activated under 3 scenarios or *profiles*.

- DOMAIN, where a computer is configured to be part of a domain. If a computer is able to authenticate to it's configured domain, rules defined with this *profile* will be active
- PUBLIC, all networks when a DOMAIN is not in use
- PRIVATE, networks as defined by the user

Simply stated, the Vista firewall can activate different rule *profiles* based on if DOMAIN authentication is successful or not. Typically a DOMAIN suggests a friendly work or educational environment. These environments may provide a better overall security posture; for example through the use of Intrusion Prevention systems or Network Access Controls to check and enforce minimum patch or anti-virus signature versions of PCs joining the network. This would allow for a

more flexible firewall policy. A single rule will be added to all inbound TCP traffic when one is connected to a DOMAIN:

```
allow inbound TCP all for profile DOMAIN
```

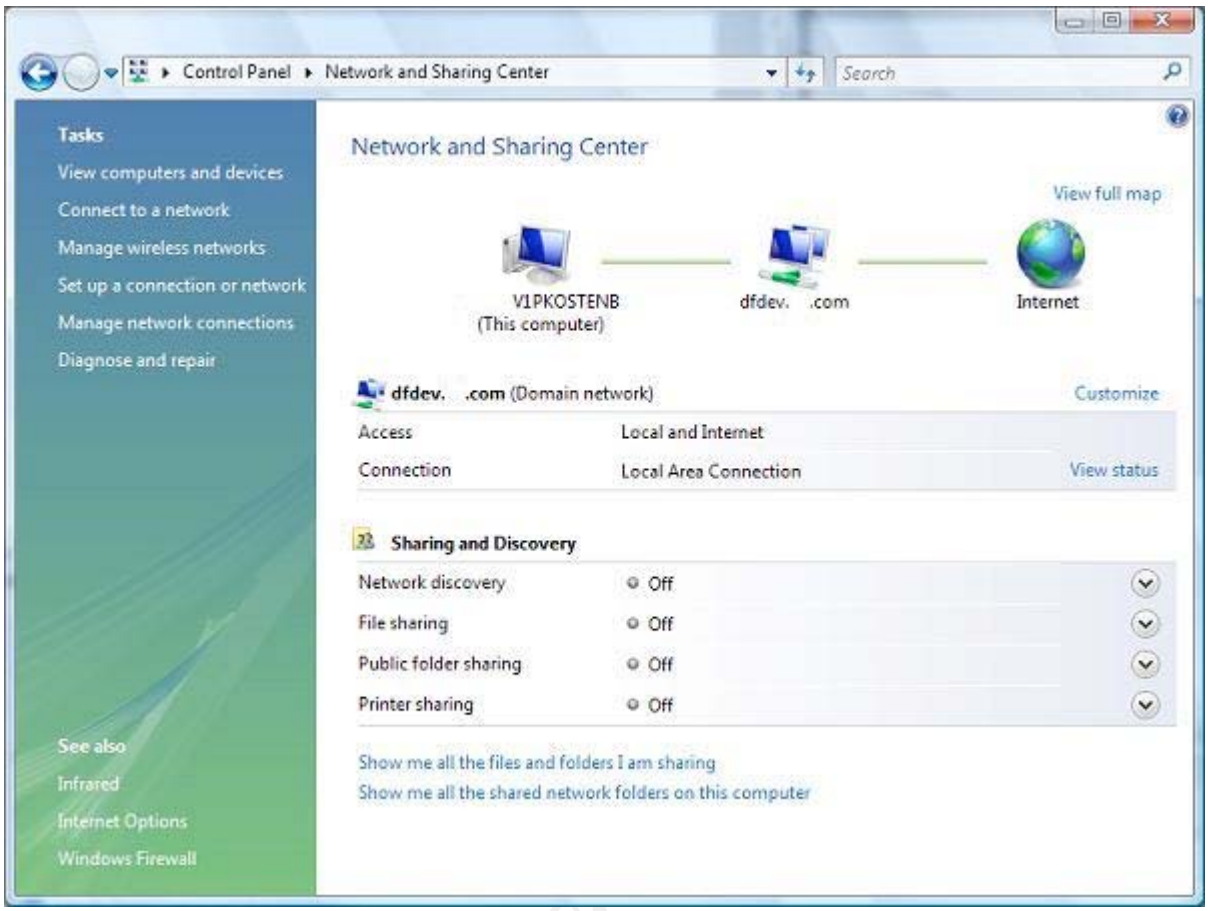
The result of this rule would allow all inbound TCP when one is considered on site (or authenticated to a DOMAIN) and block all inbound when offside. It is noted that there is no sense of rule priorities, however a rule created, `block inbound TCP all for profile PUBLIC,` in addition to the use of a default setting of block inbound, as described above, will take precedence over all other rules including any `allow inbound` rules.

Testing the Environment

Domain profile Activation

Interesting features of the Vista firewall start to show up during basic tests. First, a test of the DOMAIN detection. Referencing the "Network location-aware host firewall" section of the TechNet article:
http://technet2.microsoft.com/WindowsVista/en/library/19b429b3-c32b-4cbd-ae2a-8e77f2ced35c1033.mspx?mfr=true

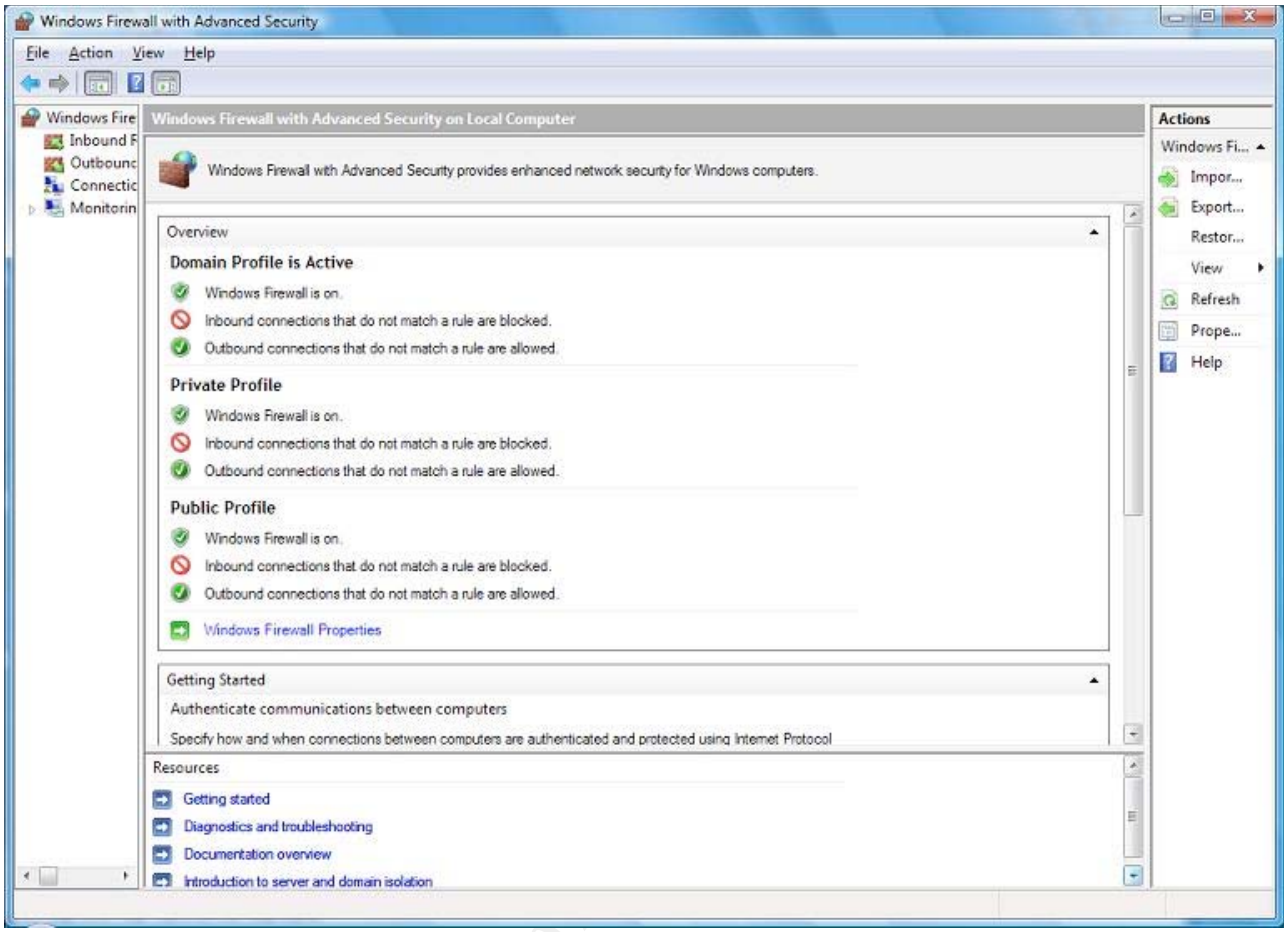
suggests that all active interfaces must be authenticated to a domain for the DOMAIN *profile* to be applied. A laptop is connected via the LAN interface to the organizations network and authentication occurs. We can verify DOMAIN connectivity by opening the control panel -> network and sharing center.



Indicated in the interface information is "Domain network"

Next, the active *profile* can be verified in the advanced firewall GUI or through the command line:

```
netsh advfirewall show currentprofile
```



NMAP scans against the LAN interface of this machine will indicate all TCP ports open. The machine is then disconnected from the LAN and placed on an isolated backed LAN network. The machine does not authenticate to a DOMAIN and the PRIVATE *profile* is selected. NMAP scans confirm all inbound TCP ports are closed. The machine is reconnected to the LAN, it authenticates to the domain, the firewall selects the DOMAIN *profile* and all ports open again. The WLAN interface is activated (in addition to the LAN interface) and is attached to the backed WLAN segment. As suggested in the TechNet article, the PRIVATE *profile* is selected by the firewall (all ports closed) as only 1 of the 2 network interfaces can authenticate to the domain.

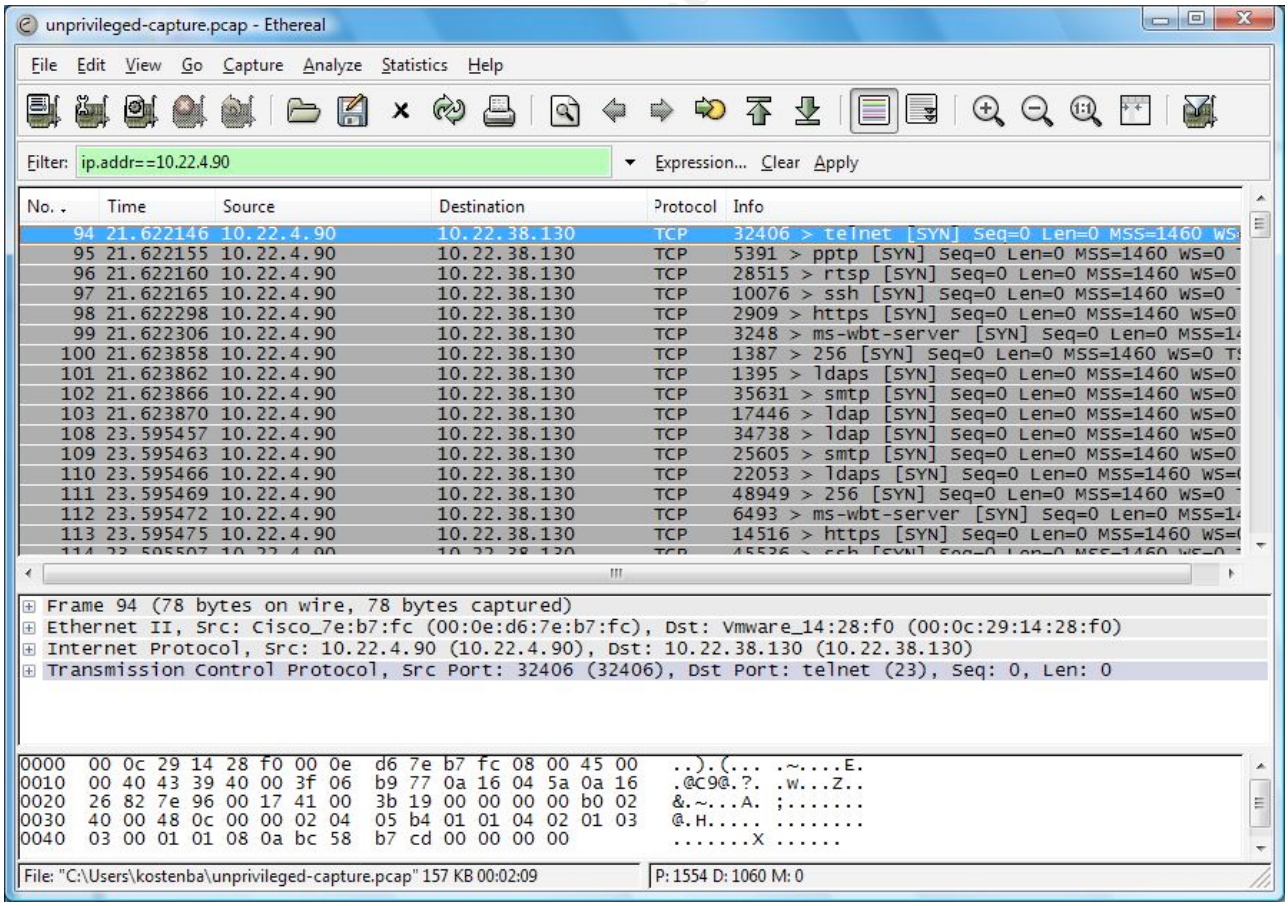
Any software that creates a virtual network interface (some VPN software does this) may run into issues if all interfaces are required to authenticate. Organizations may use VPN in supporting remote access. If a virtual NIC is created, it will, in most cases, have an IP address supported by the remote site. The physical NIC would retain the address supported by the home network. The Vista firewall will detect both network interfaces, and activate the PRIVATE *profile* as only 1 of the 2 network interfaces will be able to authenticate to a DOMAIN. A more visible example would be if a PC is connected to multiple networks, for example one connection to the primary work network and the second to a backed lab type network. Only 1 interface will authenticate and again the PRIVATE *profile* would be used.

UDP and FTP

An improvement over earlier versions, Microsoft's Vista firewall properly handles outbound UDP state and 'active FTP'. By default inbound UDP traffic will be blocked. Under previous versions this would create a difficulty for legitimate outbound traffic. As UDP is a stateless protocol, outbound state of a UDP packet is not recorded creating problems for inbound UDP replies. Active FTP is where the FTP server will initiate a connection back to the client to do the actual transfer of data. Previous versions and some 3rd party firewalls will not properly track the connection and block the transfer of data.

Scans and Firewall Logs

In the advanced firewall GUI under the *Windows Firewall Properties* section one can configure or customize logging. Logging can not be configure by rule but only by allow or deny. For all groups and *profiles* the default Vista firewall settings are configured to log all dropped packets and not log successful connections. Using the default Vista log settings and NMAP set for either SYN and full connect scans reveal that the only packets logged were ones dropped by the firewall against listening ports. Dropped packets against inactive ports were not logged. Going one step further, WinPcap and Wireshark are installed and the traffic of an NMAP full connect scan is captured. It is noted that all scan traffic generated by NMAP is captured by Wireshark. This means PCAP sees the traffic before the Vista firewall can block it. While PCAP and Wireshark were installed with privileges, the capture was done without:



An excerpt of the Vista firewall log:

```
#Version: 1.5
#Software: Microsoft Windows Firewall
#Time Format: Local
#Fields: date time action protocol src-ip dst-ip src-port dst-port size tcpflags
tcpsyn tcpack tcpwin icmptype icmpcode info path

2007-06-15 10:47:52 DROP ICMP 10.22.4.90 10.22.38.130 - - 28 - - - - 8
2007-06-15 10:47:53 DROP ICMP 10.22.4.90 10.22.38.130 - - 28 - - - - 8
2007-06-15 10:49:08 DROP TCP 10.22.4.90 10.22.38.130 35326 135 64 S
2007-06-15 10:49:09 DROP TCP 10.22.4.90 10.22.38.130 34024 135 64 S
2007-06-15 10:50:11 DROP TCP 10.22.4.90 10.22.38.130 9352 445 64 S
2007-06-15 10:50:12 DROP TCP 10.22.4.90 10.22.38.130 33877 445 64 S
2007-06-15 10:53:22 DROP TCP 10.22.4.90 10.22.38.130 45256 139 64 S
2007-06-15 10:53:23 DROP TCP 10.22.4.90 10.22.38.130 10977 139 64 S
```

The unexpected results lead back to a previous article and this exact situation in the "Wormhole-tunneling with PCAP" section of:

http://www.securityfocus.com/infocus/1831

Privileges

One can view the firewall configuration without being part of any group, however this can only be done at the command line and not using the GUI. Other functions like import/export and reset are also not available. If application notification were enabled, one would be able to block an application inbound connection request, but not be able to allow a connection. To create and remove rules one must be part of the *Network Configuration Operators* group; but all functions are still not available. For example one cannot view the logs, import/export, or reset from the GUI or command line. The settings, as described below are also not configurable by users that are only part of the NCO group.

Settings and Options

Vista does not offer too much in the way of settings, but what is offered is available through the advanced GUI under the section *Windows Firewall Properties*. Each Profile has its own customizable settings in addition to a section for IPSEC. As stated above, logging options include file location, maximum file size and enabled logging of dropped packets or successful connections.

One of our assumptions is a fixed or standard policy; referencing the article "Standards in Desktop Firewall Policies" at http://www.securityfocus.com/infocus/1867. In the general settings area one is allowed the option of disabling the notification of an application being blocked from receiving inbound connections. Allowing the user to respond "yes" to this prompt, effectively permits the adding an application rule to the currently active *profile*. An additional option exists to prevent unicast response to multicast or broadcast packets. Finally, options exist which can not be configured through command line or the advanced GUI which allow one to disable *rule merge* by the local administrator or disabling the ability to add firewall rules. This option can be accessed and used if the firewall policy is part of the GROUP POLICY. If the GROUP POLICY is used to distribute the firewall configuration, and *rule merge* is disabled, non of the settings for the 3 *profiles* (domain, private and public) will be changeable. Use of the GROUP POLICY will allow the impression that the local administrator can still add individual rules to the 3 *profiles*, but further investigation will prove otherwise. A rule added by the local administrator will appear in the *inbound/outbound* area of the advanced GUI, but not show up as part of the current active profile as displayed in the *monitoring* section of the same GUI. . Use of Group Policy will also prevent the local administrator from disabling the firewall either through the command line `netsh firewall set opmode disable` or through the GUI. The use of import/export works much the same way as an administrator attempting to add a rule. An export will work, but the firewall rules as defined by the Group Policy will not be part of the exported file. Only locally defined rules, which wouldn't be active, would be exported.

Policy Distribution

Much like the 3rd party firewall solutions, the Vista firewall can be centrally managed through the use of Microsoft's Group Policy. This would allow for policy deployment or updates and the ability to apply different policies based on groupings of users. It would only allow for a one-way type communication where the firewall policy is downloaded but no information or data from the PCs firewall is obtained; such as firewall logs. Microsoft's Systems Management Server or other software distribution facilities could be used for policy distribution. Simple scripts could be written to import policies or obtain the firewall log files.

Conclusion

The Vista firewall provides simple and effective protection and clearly is not intended to be a single security solution. It's cost effective as being distributed as part of the OS and offers a sense of purity in what it does. Combined with other facilities such as anti-virus and patch management, it can still be thought of as that 3rd piece of an overall PC protection posture. On the down side, trouble shooting can be difficult due to limitations in logging. This would include the ability to control what is put in the logfile and Microsoft's choice to only record events involving ports that are listening. The Domain Aware feature, while extremely useful, is inflexible in its ability to

decide which adapters are involved with authentication. Like most other 3rd party firewalls, it offers no protection against programs or facilities that can be installed in such a way that network traffic can be processed before it has a chanced to be examined by the firewall. Overall there are no features or characteristics that would prevent an organization from adopting the Vista firewall. With organizations eventually migrating to Vista and those that already support Active Directory and Global Policy, this may provide the perfect solution.

Last Updated: December 14th, 2017

Upcoming SANS Training

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

SANS Security East 2018	New Orleans, LAUS	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS Amsterdam January 2018	Amsterdam, NL	Jan 15, 2018 - Jan 20, 2018	Live Event
Northern VA Winter - Reston 2018	Reston, VAUS	Jan 15, 2018 - Jan 20, 2018	Live Event
SEC599: Defeat Advanced Adversaries	San Francisco, CAUS	Jan 15, 2018 - Jan 20, 2018	Live Event
SANS Dubai 2018	Dubai, AE	Jan 27, 2018 - Feb 01, 2018	Live Event
SANS Las Vegas 2018	Las Vegas, NVUS	Jan 28, 2018 - Feb 02, 2018	Live Event
Cyber Threat Intelligence Summit & Training 2018	Bethesda, MDUS	Jan 29, 2018 - Feb 05, 2018	Live Event
SANS Miami 2018	Miami, FLUS	Jan 29, 2018 - Feb 03, 2018	Live Event
SANS Scottsdale 2018	Scottsdale, AZUS	Feb 05, 2018 - Feb 10, 2018	Live Event
SANS London February 2018	London, GB	Feb 05, 2018 - Feb 10, 2018	Live Event
SANS Southern California- Anaheim 2018	Anaheim, CAUS	Feb 12, 2018 - Feb 17, 2018	Live Event
SANS Secure India 2018	Bangalore, IN	Feb 12, 2018 - Feb 17, 2018	Live Event
SANS Dallas 2018	Dallas, TXUS	Feb 19, 2018 - Feb 24, 2018	Live Event
SANS Brussels February 2018	Brussels, BE	Feb 19, 2018 - Feb 24, 2018	Live Event
SANS Secure Japan 2018	Tokyo, JP	Feb 19, 2018 - Mar 03, 2018	Live Event
Cloud Security Summit & Training 2018	San Diego, CAUS	Feb 19, 2018 - Feb 26, 2018	Live Event
SANS New York City Winter 2018	New York, NYUS	Feb 26, 2018 - Mar 03, 2018	Live Event
CyberThreat Summit 2018	London, GB	Feb 27, 2018 - Feb 28, 2018	Live Event
SANS London March 2018	London, GB	Mar 05, 2018 - Mar 10, 2018	Live Event
SANS San Francisco Spring 2018	San Francisco, CAUS	Mar 12, 2018 - Mar 17, 2018	Live Event
SANS Secure Osaka 2018	Osaka, JP	Mar 12, 2018 - Mar 17, 2018	Live Event
SANS Secure Singapore 2018	Singapore, SG	Mar 12, 2018 - Mar 24, 2018	Live Event
SANS Paris March 2018	Paris, FR	Mar 12, 2018 - Mar 17, 2018	Live Event
SANS SEC460: Enterprise Threat Beta	OnlineCAUS	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced