Global Information Assurance Certification Paper

EVALUATION OF MANAGI NG CISCO PIX FIREWAL L WITH CISCO SECURE POLICY MANAGE R

by

Elaine Yeung

SANS SECURITY ESSENT IALS (GSEC) PRACTICA L ASSIGNMENT

VERSION 1.3

Abstract

Nowadays network security administrators are faced with increasingly complicated and heterogeneous security products. The need for a centralised management system for these products is also increasing. This paper aims to test and evaluate one of these management systems, Cisco Secure Policy Manager (CSPM) in managing a Cisco PIX firewall. Benefits of this product are discussed, including its easy -to-use user interface, its ability to use policies to manage up to 500 security devices and its notification and reporting functions. The scope of the test includes the following:

- Installation of the hardware and software;
- Creation of network topology in CSPM;
- Configuration and implementation of specific security policies;
- Configuration of Cisco PIX firewall using CSPM and
- Maintenance of the CSPM.

The test results show that CSPM is quite s imple to set up in general. It also provides a good tool for documentation of security policies. However its inaccuracies in configuring the Cisco PIX firewall and the unsatisfactory backup and restoration process lead to a conclusion that CSPM is only s uitable when the security administrator, with sufficient knowledge in PIX firewall, is required to manage multiple firewalls. It is recommended that further investigations should be conducted on the PIX configuration function, the reporting function and t he restoration function of this software.

TABLE OF CONTENTS

1. INTRODUCTION

With the increasing threats of disruption, theft and damage to information assets, network security has become an especially hot topic. According to a November 2001 report by market researcher Gartner Inc.

> *The tragic events of 11 September have altered the landscape of the security software market as enterprises re-prioritize security initiatives, moving them from the IT wish list to the list of IT 'must haves'.* [1]

The security initiatives have caused the increase in the variety and numbers of network security products in the market. Accompanying the increased supply of network security products is the complexity of managing these products. Network security administrators are challenged with the need to grasp the knowledge of new emerging security technology, to deploy the new technologies and to streamline the management of all these technologies. While a number of network management tools exist to manage a variety of network devices, the market for centralized security management tools is still emerging, according to Sidel[2]. Sidel further explained that the security management products in the existing market are not engineered to centrally monitor and control heterogeneous third-party security devices.

This paper evaluates one of these centralized security management tools by Cisco Systems Inc. – Cisco Secure Policy Manager (CSPM). It was designed to provide "a scalable, policy-based security management system for Cisco Systems firewalls, IP Security (IPSec) virtual private network (VPN) routers, and Intrusion Detection System (IDS) sensors." [3] While CSPM can be used to manage various Cisco network devices, the focus of this paper will be on using CSPM to manage Cisco PIX firewalls.

1.1. Purpose of Information Security Management

As information and knowledge becomes more valuable in business nowadays, the importance of protecting a company's knowledge assets has also increased dramatically. A company should establish and maintain a security system that ensures confidentiality, integrity and availability[4]. As a security management system, CSPM uses the access control model[5] to achieve the three goals. The access control model uses a set of rules that specifies which subject can perform which operations on which objects. This model ensures:

- Confidentiality – unauthorized persons cannot access private information;
- Integrity – information cannot be changed by intentional or accidental unauthorized changes;
- Availability – authorized use of information cannot be disrupted.

---

[1] Flash, C. "Security Product of the Year 2001"

[2] Sidel, S. "Centralised Management"

[3] Cisco Systems Inc. "Data Sheet - Cisco Secure Policy Manager 2.3"

[4,5] Harold, F. T. & Krause, M. "Handbook of Information Security Management"

2. WHAT IS CISCO SECURE POLICY MANAGER

Cisco Secure Policy Manager, also known as CSPM, is a centralised management system for Cisco firewalls, Virtual Private Network (VPN) gateways and intrusion Detection System (IDS) sensors. It can be used to document a network topology and define policies associated with the devices in the topology. These policies can then be converted into Cisco device configurations and applied to the Cisco devices. It also provides a graphical user interface to define the topology and the policies.

2.1. Benefits of using CSPM

Some of the benefits of using CSPM to manage Cisco PIX firewalls include:

- *Cisco firewall management – defines perimeter security policies for Cisco Secure PIX Firewalls;*
- *Security policy management – uses network-wide policies to manage up to 500 Cisco security devices without requiring extensive device knowledge and dependency on the command-line interface (CLI);*
- *Notification and reporting system - provides auditing tools to monitor, alert, and report Cisco security device and policy activity, keeping network administrators readily informed of network-wide events;*
- *Windows NT-based system – provides an easy-to-use, Windows-based user interface.* [6]

One of the steps involved in setting up a security system is to determine what needs to be protected, i.e. the objects and the subjects in the access control model. The core function of CSPM is to assist in defining the objects to be protected, the subject to perform certain operations on the objects and the type of operations. The objects and the subjects are defined in "network topology" [7] in CSPM. The set of rules is determined by "security policies" [8] in CSPM.

3. TEST DRIVE

The scope of this test is to evaluate the management of Cisco Secure PIX firewall with CSPM. The functions to be evaluated include:

1. Installation and Configuration
2. Report Generation
3. Maintenance

Due to limited time and resources, the functions were only tested with two Cisco Secure PIX firewalls with the failover feature. Hence the efficiency of using CSPM to manage multiple firewalls has not been fully investigated. The notification function of CSPM is also not included in this test.

---

[6] Cisco Systems Inc. "Data Sheet - Cisco Secure Policy Manager 2.3"

[7] Cisco Systems Inc. "Cisco Secure Policy Manager Administrator's Guide: Network Topology Definition"

[8] Cisco Systems Inc. "Cisco Secure Policy Manager Administrator's Guide: Policy Development and Enforcement"

The test involves setting up CSPM version 2.3.2f on a Windows NT server. Figure 1 shows the network that has been set up for this test purpose. The topology included the following items:

- one Windows NT server with CSPM software;
- two Cisco Secure PIX 525 firewalls with the failover feature;
- one Cisco 1603 router to connect to ISP;
- one Cisco 2924 switch for connecting all the devices;
- one web server and
- four personal computers.

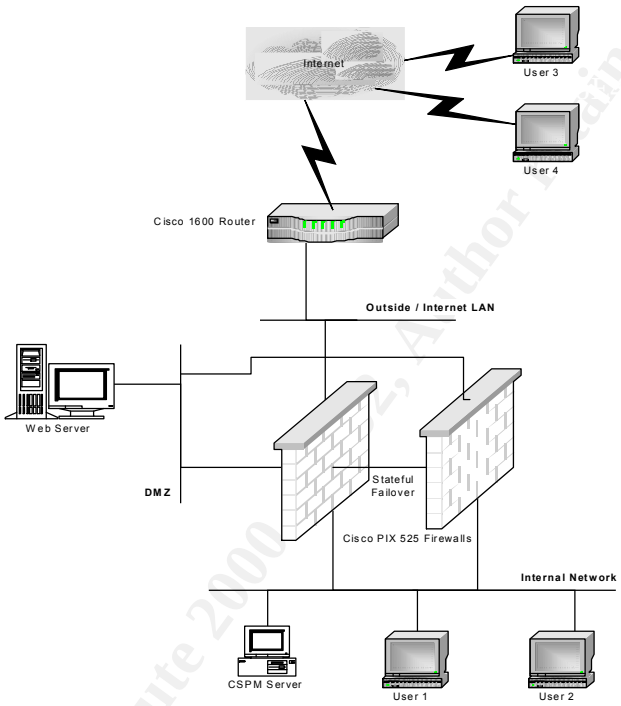

Figure 1. Test Environment Network Diagram

Three VLANs were created on the Cisco 2924 switch for the "Outside LAN", "Internal Network" and DMZ shown above.

The policies used in this test included the following:

1. Allow various devices from the Internet to only browse the content of the web server using HTTP;
2. Only allow the web server to use HTTP and HTTPS to browse the content of devices in the Internet;
3. Only allow various devices from the Internal Network to use the web server as a proxy server to perform web browsing.

The duration of the test was for a total of two weeks.

3.1. Installation

The following are the basic hardware and software requirements for installation of CSPM version 2.3.2f:

Hardware Requirement

- 600 MHz Pentium II Processor (or 400 MHz for CSPM GUI only);
- 256 MB of RAM memory (or 96MB for CSPM GUI only);
- 8 GB free hard drive spac e (or 2GB for CSPM GUI only);
- 10 Mbps network interface card;
- 1024x768 video adapter card capable of at least 256K colour;
- CD-ROM drive (preferably Autorun -enabled);
- Modem (optional for pager notifications);
- Mouse;
- SVGA colour monitor.

Software Requirement

- Service Pack 6a for Windows NT;
- Microsoft Internet Explorer 5.5;
- HTML Help 1.32 Update;
- Microsoft XML Parser (MSXML3);
- NTFS file partition;
- TCP/IP protocol stack. [9]

In this test, CSPM was installed on a HP NetServer with 933MHz, 640MB SDRAM and 18Gb Hard Disk. Windows NT Server software was installed with service Pack 6a and IE 5.5.

Before installation of the CSPM, the NT server was logged in as Administrator of the local computer and was configured with an ip address, subnet mask and gateway.

3.2. Configuration

The tasks involved in configuration of CSPM include creation of a network topology tree and security policies. A topology has to be built before the policies can be built. There are two options of building the network topology tree:

1. Autodiscovery;
2. Manual.

For this test purpose, the manual option was used to populate the network topology tree.

3.2.1. Definition of devices and network

CSPM uses objects for the definition of networks or devices in the topology tree. There are five most common types of objects in CSPM:

- Internet – included in the topology by default; used to identify the unknown network connected via the ISPs and to act as the default gateway from the trusted network into the ISP's router;
- Cloud Network – identifies a collection of networ ks of which the devices / hosts "in interest" will be defined;
- Hosts – identifies a device with specific ip address, subnet mask and default gateway;

[9] Cisco Systems Inc. "Data Sheet - Cisco Secure Policy Manager 2.3"

- Gateway – identifies network device such as router, firewall or intrusion detection engine;
- Network Object Group – represents a logical group of objects, which can be used as the source or destination of network services in a security policy. [10]

In this test, the following items were defined in the network topology tree:

- Internet;
- Internet router as a gateway;
- PIX firewall as a gateway;
- DMZ as a cloud network;
- Web server as a host;
- Internal Network as a cloud network;
- User 1, 2, 3 and 4 as hosts;
- User 1 and User 2 as network object group called web_users.

All of the above items were configured with a name, ip address (or network address) and subnet mask. Furthermore, the PIX 525 firewall was configured to be a "Managed Device". More definitions, such as interface ip address, software version and network address translation for specific hosts or networks, are required for a 'Managed Device". This definition is vital for the correctness of policy enforcement in CSPM. It determines logical relationship of different hosts or devices with the firewall or routers. Only the devices / hosts that are included in the security policy are required to be defined in the network topology tree.

3.3. Implementation of Security Policy

As this test illustrates a simplified representation of Internet access for a company, the following three sets of rules were used in order to test the creation, modification and removal of policies in CSPM and to test the accuracies of CSPM in configuring the PIX firewall for different policies:

First Rule Set:

1. All users in the Internal Network are allowed to use the web server as a proxy server to perform internet browsing;
2. Only the web server is allowed to perform web browsing on devices in the Internet;
3. All devices in the Internet are allowed to browse the web site on the web server in the DMZ.

Second Rule Set:

1. Only User 1 and User 2 are allowed to use the web server as a proxy server to perform internet browsing;
2. All users from the Internal Network are allowed to browse the web content in the web server using HTTP and HTTPS;
3. Only the web server is allowed to browse the web content in all devices in the Internet using HTTP and HTTPS;

[10] Cisco Systems Inc. "Cisco Secure Policy Manager Administrator's Guide: Network Topology Definition"

4. Only User 3 and User 4 are allowed to browse the web site on the web server in the DMZ using HTTPS.

Third Rule Set:

1. Only User 2 is allowed to browse the content of all devices in the internet;
2. Only User 3 is allowed to browse the web content on User 1 PC;
3. All devices in the Internet are allowed to browse the content of the web site on the web server using HTTP and HTTPS.

Before converting the rules above into security policies in CSPM, the rules were translated into the following table, which contained details of Transport Layer and Network Layer information in the OSI model:

Source Address	Source Port	Translated Source Address	Destination Address	Destination Port	Translated Destination Address	Comment

3.3.1. Definition of services

After the traffic details of the rules are determined, "network services" [11] need to be determined in CSPM. A network service consists of the type of protocol (e.g. TCP, UDP) and the particular feature of the protocol (e.g. port number for TCP). A few services can be grouped together into "network service bundles" which provide a shortcut method for referencing a group of common services (such as web and mail services) without having to create individual rule for individual service. In this test, a network service, called "proxy_service", was created to reference TCP port 8080.

3.3.2. Development of Policy Components

When implementing policies on Cisco PIX firewalls, CSPM uses the logic of "deny all traffic" except the traffic defined in the security policy. In defining the security policy, it uses if-then-else logic framework. Following is the summary of the policies created by the first rule set defined above:

1. If source is **Internal Network**
   and destination is **web server**
   and service is **proxy_service**
   then **permit**

2. If source is **web server**
   and destination is **Internet**
   and service is **http**
   then **permit**

3. If source is **Internet**
   and destination is **web server**
   and service is **http**
   then **permit**

[11] Cisco Systems Inc. "Cisco Secure Policy Manager Administrator's Guide: Policy Development and Enforcement"

The content of the security policies in CSPM were then changed to test the other two rule sets described earlier.

3.4. Configuration of PIX firewalls

Before CSPM can be used to manage PIX firewall, the PIX firewall is required to have basic configuration, such as ip addresses for the interfaces and routing information. Once the security policies in CSPM are saved and updated, CSPM will translate the policies into PIX specific commands and "push" the commands to the PIX firewall.

3.5. Report Generation

CSPM provides certain report templates to allow administrator to gather traffic statistics on the PIX firewall. This feature was tested by generating reports on most frequently accessed web sites in the thirty minutes prior to the generation of the report.

3.6. Maintenance

As the core of CSPM is a database that contains the configuration data and audit records, a major part of maintaining this software is the operation of performing backup and recovery. Cisco recommends that the Policy Database should be backed up whenever a major change to the CSPM configuration is performed[12]. The backup task is GUI-driven and takes approximately three minutes to perform. The recovery task is performed from the command line. The command will convert the primary Policy Database to a backed-up version of the same database on the primary Policy Database server[13]. During the period of the test, the procedures of backup and recovery were undertaken three times.

4. EVALUATION RESULTS

As more security threats emerge, the complexity in securing a network has also increased. It is often difficult enough for IT professionals to convince management to purchase security products. It is even more difficult to purchase the right tool so that the tool yields cost effective benefits. In order to measure the effectiveness of the CSPM software, the following criteria have been considered:

- Complexity;
- Usability;
- Security;
- Suitability.

Avolio mentioned that "security and complexity are often inversely proportional".[14] He also mentioned that "the more cryptic the instructions and procedures, the more room for misunderstanding and misapplication." When the software is too complicated to deploy, mistakes are more likely to be created and users get frustrated in learning and correcting

[12] Cisco Systems Inc. "Cisco Secure Policy Manager Administrator's Guide: System Configuration and Maintenance"
[13] Cisco Systems Inc. "Cisco Secure Policy Manager Administrator's Guide: System Configuration and Maintenance"
[14] Avolio, F. M. "Best Practices in Network Security"

the mistakes. This may lead to users not implementing the tool correctly . It is often dangerous to have a false sense of security - companies believe that they have the tool in place to perform the protection but the tool is actually not performing as it should be, due to the difficulty in deployment. Hence a good security m anagement tool should be simple and easy to use.

When a security management system is compromised, it could also mean that the security devices managed by this system are all affected. The negative effect can be traumatic. Therefore one of the important aspects under consideration is the vulnerability level of CSPM.

Finally, each security management system has certain features that may fit the security objective of a company more than the other systems. When the security administrator selects a product, the decision criterion is often based on the specifications provided by the vendor. Hence this paper has used this test to verify the benefits documented by Cisco Systems Inc. (outlined in earlier sections).

4.1. Complexity

Using security management softwar e involves deployment and maintenance of the software. The following sections describe the evaluation of complexity in deployment and maintenance of the CSPM.

4.1.1. Deployment

This software is a good starting tool for users who do not have experience in managi ng Cisco PIX firewall. The tasks involved in configuring the topology and the policy are quite straightforward. Cisco has equipped users with detailed manuals and examples on setting up CSPM to be used with the various Cisco devices. It also "translate s" all the "if-then-else" rules from the GUI-interface into PIX commands. Hence enforcement of the security policy on the PIX firewall does not totally rely on technical skills of the administrator of the firewall.

However, there are a few limitations of using CSPM to configure the PIX firewall automatically. The results of the test shows that CSPM tends to miss some configurations required to enable the firewall to allow certain traffic. The tester often had to go through the command line configuration to verify the entries created by CSPM. This increased the complexity of troubleshooting.

CSPM provides options to enter commands manually through the GUI interface so that these commands can be added to the PIX firewall after CSPM has generated the commands from the policy defined. The test results show that a lot of network address translation commands have to be entered manually to rectify the problems mentioned above.

4.1.2. Maintenance

During the set up of the server for this test, the server was partitioned in two logical drives: C and D. C drive was configured to have 4 GB of disk space and D drive was configured to have 14 GB of disk space. When CSPM was first installed on the server, it was installed on the C drive. After the implementation of CSPM, a few changes were made to the security policies, resulting in the software becoming unstable and Dr. Watson errors being frequently created. This problem was later rectified by re-installing CSPM on D drive. This seems to indicate that CSPM does require a lot of hard disk space although the security policy used in this test was a more simplified policy as compared to a real world scenario.

This paper has tested one of the major tasks in maintaining the software – performing backup and restoration of the CSPM Database. During this test, three backups were performed. The first two restorations were performed very smoothly and very quickly. Unfortunately the third one caused the software to be totally non-functional. Re-installation of the software was performed after the third restoration. However, un-installation of the software caused the content of the whole D drive to be erased. This problem was not encountered during the first un-installation of the software.

It was found that an easier way to keep a copy of the configuration is to use the function of "exporting and importing configuration files" in CSPM. This function enables users to "export a copy of the view of the GUI client to a location that the user specifies". [15] The disadvantage of using the "export and import" function is that the copy of configuration exported "does not contain a history of traffic that has occurred across the network or any reports that have been generated regarding the status and use of the network."[16] The benefit of using the export function is that it keeps a copy of the current topologies and policies created. If there is a problem with the software and with the process of restoring the database from the backup copy, the software can be re-installed and the copy of the configuration can be imported into the newly installed software.

4.2. Usability

As mentioned above, Cisco has equipped users with detailed on-line manuals and examples to use this software. The GUI interface provides good, plain information about the details of security rules and the topologies set up. This allows users with no or little experience on PIX firewall to understand what rules are currently configured on the firewall. However, details of the security rules can only be printed one rule at a time. There is no easy way to print out all the rules. Hence users cannot use CSPM to generate an automatic report on all the existing rules.

The report function of CSPM provides some basic traffic statistics on the PIX firewall. However the report template cannot be tailor-made to obtain further details, such as traffic involving a specific TCP port.

---

[15] Cisco Systems Inc. "Cisco Secure Policy Manager Administrator's Guide: System Configuration and Maintenance"

[16] Cisco Systems Inc. "Cisco Secure Policy Manager Administrator's Guide: system Configuration and Maintenance"

As compared to the task of configuration, the process of backup maintenance was found to be trickier as the same process has shown to produce different results. This process should definitely be tested and proved to be stable before the software is introduced into the environment.

4.3. Security

CSPM uses TCP port 1467, named "PIX Secure Telnet" [17], to manage the Cisco PIX firewall. In this test, the PIX firewall has been configured to allow telnet traffic from two hosts using the command:
telnet <host ip address> <interface name>.

Only one of the hosts had CSPM installed. When the test was performed, the preliminary understanding of the tester was that TCP port 23 and TCP port 1467 were allowed to be used by the CSPM server to connect to the firewall but the server without CSPM configured can only use TCP port 23 to connect to the firewall. The test result indicated that the non-CSPM server could actually use both TCP port 23 and TCP port 1467 to connect to the PIX firewall. Furthermore, when a password was configured on the firewall and TCP port 23 was used to connect to the firewall, the PIX firewall required authentication information to be entered. However no authentication information was required to connect to the firewall via TCP port 1467. This increases the risk of the PIX firewall being compromised when unauthorized users are using TCP port 1467.

During observation of the actual configuration commands generated by CSPM in this test, it shows that certain unnecessary rules have been created on the PIX firewall by CSPM. These rules include allowing icmp unreachable and icmp echo-reply on all interfaces. This increases the security risks as the icmp messages can provide hackers or unauthorized users information about the infrastructure, which can be used for exploiting the infrastructure.

4.4.Suitability

Although the documentation provided by Cisco Systems Inc. specifies that "extensive device knowledge and dependency on the command-line interface (CLI)" [18] are not required, the test results indicated otherwise. As the test results show, there are still flaws in the way CSPM configures the PIX firewall. Users without sufficient knowledge of PIX firewall will find it difficult to troubleshoot the rules. Hence it is believed that the benefit of efficiency in implementation of security policy can only be achieved if there is a requirement for managing numerous PIX firewalls and if the administrator has average knowledge of configuring PIX firewalls.

When there is a requirement for managing numerous PIX firewalls, the GUI-interface of CSPM also provides a centralized and easier documentation of the rules implemented on all the PIX firewalls. The reporting feature of the software provides the administrator

[17] Cisco Systems Inc. "Cisco Secure Policy Manager Administrator's Guide: Network Topology Definition"
[18] Cisco Systems Inc. "Data Sheet - Cisco Secure Policy Manager 2.3"

with statistics of the traffic traversing the PIX firewall. However, the feature does not provide flexibility in customising the report to specific traffic analysis.

Another limitation of this software is the incompatibility with non-Cisco products. Hence it is only suitable for a company with major investment in Cisco security products.

5. CONCLUSION

With the complexity and the varieties of the security products nowadays, security administrator needs a centralised management system that is easy to use and provides a focal point of management. Cisco Secure Policy Manager was designed to provide such benefits. Its GUI-interface allows the users to focus more on identifying the systems to be protected and developing the high-level security policies without having to worry too much about converting the policies into configurations of the security devices. Because the security policies are defined in plain English, it assists the users in documenting and reviewing rules that have been implemented. The reporting features also allow users to have ready-made reports on traffic statistics. The major limitations of CSPM seem to lie in the technical aspects. These limitations include the following:

- The software is inaccurate in configuring the PIX firewall;
- The software is unstable in the backup and restoration process;
- The software induces unnecessary rules on the PIX firewall, which can increase security risks.

These limitations have hugely reduced the benefits of the software. If CSPM is the remote-control device for the PIX firewall, this remote-control device can only provide basic control of the devices and is good to "kick-start" all the devices if there are numerous Cisco devices. However, to fully control the firewall, a lot of "manual" effort is still required before the device can function properly.

It is believed that CSPM will benefit the security administrator most in the following scenarios:

- The network environment consists of many Cisco devices;
- The security administrator has sufficient knowledge of the PIX firewall and is required to manage several Cisco PIX firewalls in a short time frame;
- The network environment does not have any other management tools that are compatible with Cisco devices;
- The security administrator requires some "off-the-shell" product to provide basic documentations about the network security environment, such as the security policies implemented on the network devices and Internet traffic statistics.

It is recommended that further investigation should be conducted to determine the limitations of using CSPM to configure the PIX firewall. The notification and reporting functions of the CSPM should be further explored to ensure that the administrator can take full advantage of these functions. Finally, a backup plan should also be documented and tested to ensure that the Policy Database can be restored.

Glossary

CSPM	Cisco Secure Policy Manager
LAN	Local Area Network
VLAN	Virtual Area Network
DMZ	Demilitarized Zone
GB	GigaByte
GUI	Graphical User Interface
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure (over Secure Socket Layer)
TCP	Transmission Control Protocol
UDP	User Datagram Protocol

References

Avolio, F. M. " Best Practices in Network Security". Network Computing. 20 March 2000. URL: http://www.networkcomputing.com/sh ared/printArticle?article=nc/1105/1105f2full.html&pub=n wc (20 April 2002)

Cisco Systems Inc. "Cisco Secure Policy Manager Administrator's Guide: Network Topology Definition". Version 2.3f. March 2001. URL: http://www.cisco.com/univercd/cc/td/doc/product/ismg/policy/ver23f/topodef/index.htm (21 Feb 2002)

Cisco Systems Inc. "Cisco Secure Policy Manager Administrator's Guide: Policy Development and Enforce ment". Version 2.3f. March 2001. URL: http://www.cisco.com/univercd/cc/td/doc/product/ismg/policy/ver23f/poldev/index.htm (1 March 2002)

Cisco Systems Inc. "Cisco Secure Policy Manager Administrator's Guide: System Configuration and Maintenance". Version 2.3f. March 2001. URL: http://www.cisco.com/univercd /cc/td/doc/product/ismg/policy/ver23f/scmag/index.htm (3 March 2002)

Cisco Systems Inc. "Data Sheet - Cisco Secure Policy Manager 2.3". 9 April 2001. URL: http://www. cisco.com/warp/public/cc/pd/sqsw/sqppmn/prodlit/spmgr_ds.htm (7 Jan 2002)

Cisco Systems Inc. "Release Notes for Cisco Secure Policy Manager Version 2.3.2f". 2 July 2001. URL: http://www.cisco.com/univercd/cc/td/doc/product/ismg/policy/ver23f/rn232f.htm#xtocid220174 (7 Jan 2002)

Flash, C. "Security Product of the Year 2001". Datamation. 19 February 2002. URL: http://itmanagement.earthweb.com/secu/article/0,,11953_976721,00.html (31 March 2002)

Fraser, B. "Site Security Handbook". Network Working Group. September 1997. URL: http://www.ietf.org/rfc/rfc2196.txt?number=2196 (13 April 2002)

Harold, F. T. & Krause, M. "Handbook of Information Security Management". CRC Press LLC. Fall 1997. URL: http://www.detectiondesintrus.com/Documents/HISM/019 -021.html#Heading2 (14 April 2002)

Sidel, S. "Centralized Management". Information Security. Jan 2002. URL : http://www.infosecuritymag.com/2002/jan/features_command.shtml (22 Apr 2002)

The Computer Language Company Inc. "TechEncyclopedia". TechWeb. URL: http://www.techweb.com/encyclopedia/ (22 Apr 2002)

Last Updated: September 24th, 2017

Upcoming Training

Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS New York SEC401^	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
SANS DFIR Prague Summit & Training 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VA	Oct 14, 2017 - Oct 21, 2017	Live Event
SANS Tokyo Autumn 2017	Tokyo, Japan	Oct 16, 2017 - Oct 28, 2017	Live Event
CCB Private SEC401 Oct 17	Brussels, Belgium	Oct 16, 2017 - Oct 21, 2017	
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201710,	Oct 23, 2017 - Nov 29, 2017	vLive
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
Community SANS Vancouver SEC401^	Vancouver, BC	Nov 06, 2017 - Nov 11, 2017	Community SANS
Community SANS Colorado Springs SEC401~	Colorado Springs, CO	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS St. Louis SEC401	St Louis, MO	Nov 27, 2017 - Dec 02, 2017	Community SANS
Community SANS Portland SEC401	Portland, OR	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Dec 04, 2017 - Dec 09, 2017	Community SANS
SANS Austin Winter 2017	Austin, TX	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Bangalore 2017	Bangalore, India	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201712,	Dec 11, 2017 - Jan 24, 2018	vLive