Global Information Assurance Certification Paper

Compartmented Network Design

By
Weihan Chang
GSEC Version 1.4b
Administrivia 2.8
6/27/2004

Abstract

Traditional large enterprise network designs focus on performance, availability, and manageability. Security is often an add-on or afterthought. Retrofitting security measures to existing network architecture are lengthy projects requiring extensive resources. In some cases, it is done at the expense of sacrificing network performance and manageability. The traditional network designs of yesterday can not keep up with the pace of change today while maintaining a sufficient level of security. The goal of this paper is to look at a network design that has security built-in from the ground up. The approach is to distribute security policy enforcement to strategic locations within the network by segmenting the network into compartments each with its own predefined security policy, performance, and availability needs. We will focus on the security aspect of the design and look at a high level implementation strategy.

Table of Contents

Challenges of Traditional Network Security Model

Many of today's corporate networks can be characterized as having a hard perimeter and a soft inside. The perimeters are well protected and monitored. Companies today are aware of the risks of connecting corporate networks to the Internet without security measures in place to delineate and protect the perimeters. Network traffic that crosses the perimeter is monitored and controlled by the use of firewalls, IDS (Intrusion Detection Systems) and other countermeasures. The network traffic that crosses the perimeters is understood and any new traffic patterns are scrutinized. Inside the perimeters the story is different. Internal network traffic is generally not monitored or controlled. For most organizations, the internal network is wide open. Any one device on the network can access any other resources connected to the network via the IP layer. The security ramifications are:

1. Attack/Infection in one part of the network is not easily contained.
2. Breach in any part of the network exposes the entire network.
3. Difficult to detect attacks from internal sources.

In today's IT environment, systems, applications, and data no longer operate in isolation. The fundamental change in IT is an increase in the dependencies of systems, applications, and data. This dependency is not just within the enterprise but extends to business partners and external providers. The need to share information with external entities has caused the paradigm to shift from "security by exclusion" to "security by inclusion"[1]. The question that challenges the security staff has changed from how to keep other people out to how to provide controlled access to a diverse set of users with varying levels of access needs to a wide range of company information while maintaining confidentiality, integrity, and availability. Add to that the proliferation of wireless access, VPN (Virtual Private Network), extranet, telecommuting, and hoteling cubicles; the perimeter has become porous and tenuous. The internal corporate network can no longer be considered trusted.

In today's business climate, mergers, acquisitions, partnerships and restructurings are common occurrences. Each of these organizational changes impacts IT systems and the network. To complicate things further, as more services and e-commerce become available on the Internet, they are increasingly falling under regulatory governance all over the world. The corporate network not only has to adapt to all these changes but it has to maintain an acceptable level of security to protect the company's information assets under increasing stringent budgetary constraints. The traditional "hard shell/soft center" network design can no longer keep up with the pace of change today.

Compartmented Network Design

[1] Blum.

Conceptually, there are two components to the compartmented network design. First, break up the network into smaller segments. Organize these segments based on some combination of business needs, functional requirements and security. We will call these network compartments. Second, define security policies for each compartment and have policy enforcement points[2] at each compartment to enforce these security policies. Essentially, the idea is instead of having centralized firewalls enforcing security policies at the perimeters of the company network, we are distributing security policy enforcement points inside the network at strategic places. The collection of systems in each network compartment together with their security policies forms a policy domain[3]. By dividing up a large monolithic enterprise policy domain into a collection of smaller policy domains, finer access control and granular security control can be achieved. The benefits of this distributed security model are:

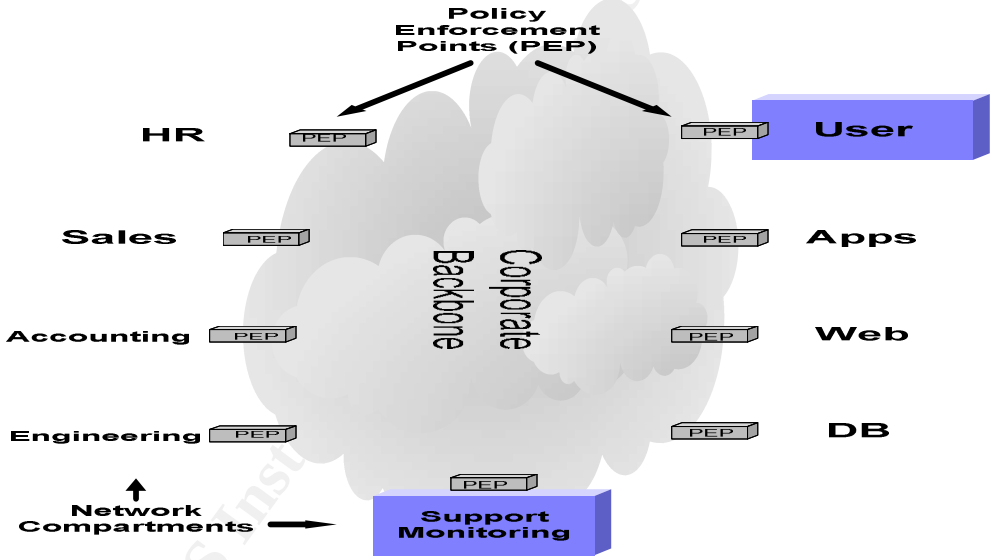
1. Aligns with defense in depth security strategy. Penetrating the perimeter firewalls does not give free access to the rest of the network.
2. Reduces the chance of a complete security breach. Compromising any single device limits access to just its compartment.
3. Protection against threats that originate from inside the network. E.g. disgruntled employees.
4. Minimizes the time to detect and react to intrusion and attacks. Better monitoring and understanding of the internal network traffic means anomalies are detected and alerted. Having policy enforcement points at each compartment enables modification of policy to track or deter attacks.
5. Ability to isolate and contain intrusion or worm/virus outbreaks. Having policy enforcement points at each of the compartments gives the ability to control traffic into or out of any compartment. By doing the work upfront to create network compartments and understand the network traffic between the compartments, the effect of isolating a compartment is understood before hand.
6. Eases add/move/change/delete to network topology. Any add/move/change/delete server to one compartment does not affect others. On a larger scale, consider the scenario of acquisition of a company. To quickly bring the acquired company into the parent company's network has always been a lengthy and involved process. With compartmented network design, make the new acquired company its own compartment with its own security policies to control flow of traffic between the two networks. That way, the parent company as well as the acquired company's security is preserved.

Even though the primary driving force for compartmented network design is security, the fact that your company runs its business on your network means that any network design has to provide capacity, flexibility, and security. Security

[2] Westerinen.
[3] Westerinen.

measures have to add value and enable the conduct of business, not hinder. The design has to encompass:

1. **Usability** - The reason why a network exists is to support the business. The design has to add value to achieving business goals and facilitate deployment of business initiatives.
2. **Security** - A predefined security policy for each compartment based on data classification and risk assessment. Policy could include cryptographic needs, physical security, access and authorization controls, business continuity, audit requirements, etc.
3. **Scalability** - A sound solution must be extensible and meet the ever-increasing demand of network resources.
4. **Modularity** - Adding or removing of a compartment follows predetermined templates for fast deployment. Adding or removing components within a compartment should have minimal impact to other compartments.
5. **Integration** - All compartments are managed consistently and will follow established problem/change management processes[4].



The value proposition of this network design is clear. It is the next logical evolutionary step in enterprise network design.

Implementation Strategy

To segment the network takes planning and restructuring of your current network as well as devices connected to the network. Chances are you already have a running corporate network that has to stay up to conduct your business. Chances are you can't just shut down your network for the period of time it takes to re-architect your network. The strategy of implementing network compartments has

[4] Hewlett-Packard Development Company.

to be an evolution of your current network infrastructure, not a disruption[5]. To successfully design and implement a compartmented network, you have to start with a good understanding of your current IT and business processes. From there, a future desired state is defined. Gaps are identified. Tasks needed to get to the future state are created, prioritized and ordered. Ownerships of the tasks are assigned. Implementation plan can then be created. The following outlines the major tasks from planning to implementation.

1. Gather information. Assemble the following documents. Identify ownership, custodian, and subject matter experts with each.

   - Network diagrams – Logical and detailed diagrams of the entire company network including any WAN and VPN connections.
   - Business processes – Functional entities of the company such as sales, HR, legal, manufacturing, etc. They will come into play with defining the compartments.
   - Server types – Lists of servers by platform, location, applications, and ownership.
   - Data classification – Document of how your company data is classified.
   - Application types – Major applications that the company uses to conduct business or applications that are used internally. Some examples are E-Commerce, PeopleSoft, sales portal, etc.
   - Data types – Lists of data by type, location, data classification, and ownership. This information will help define the compartments you need as well as the security policies. Different class of data will require different measure to protect. Many of the new legislations today focus on the protection and privacy issues with certain types of data.
   - Risk assessment, business impact analysis – These will be part of the consideration that will help define the compartments and their security requirement.
   - Problem/Change management procedures – Implementation of this design will impact these procedures and supporting areas. They need to be documented so that support of the new network design will continue with minimal disruption.

   Other information to consider include security policies, budget, projects that may have impact or input into segmentation design and business plans.

2. Overall plan/timeline.

   Determine the scope of the effort using the information collected in step 1 and resource/budget constraints. Determine high level objectives with milestones and map to a timeline. The nature of compartmented network design involves many different areas of an organization from technical to

[5] Hewlett-Packard Development Company.

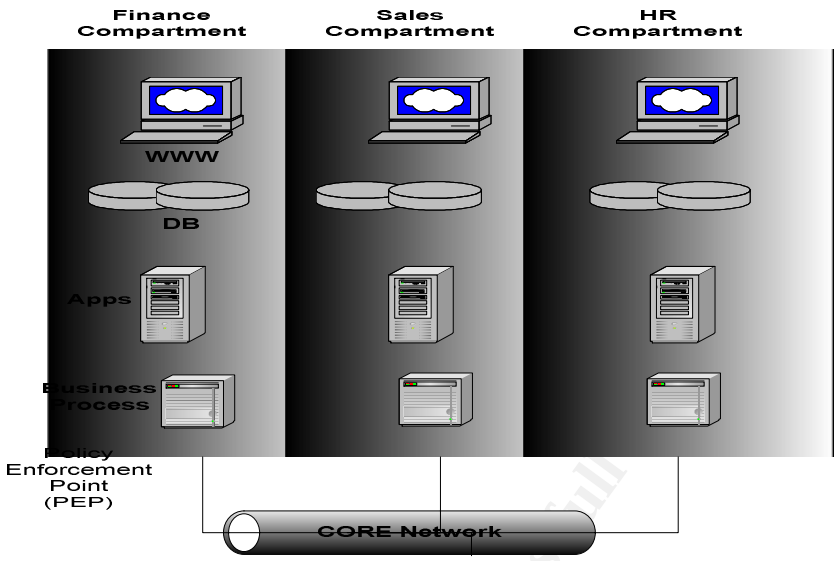
business. It is truly a multidisciplinary effort that will need input and buy-in from all parts of the organization. An effective way to execute a project like this is to use the Macro team concept which consists of a small core team and a number of virtual task teams[6]. The small core team will oversee the entire effort from design to implementation and engage the virtual task teams to get owner and subject matter experts' involvement from different areas of the company. Having a dedicated core team will ensure a consistency in overall designs.

3. Develop network design.

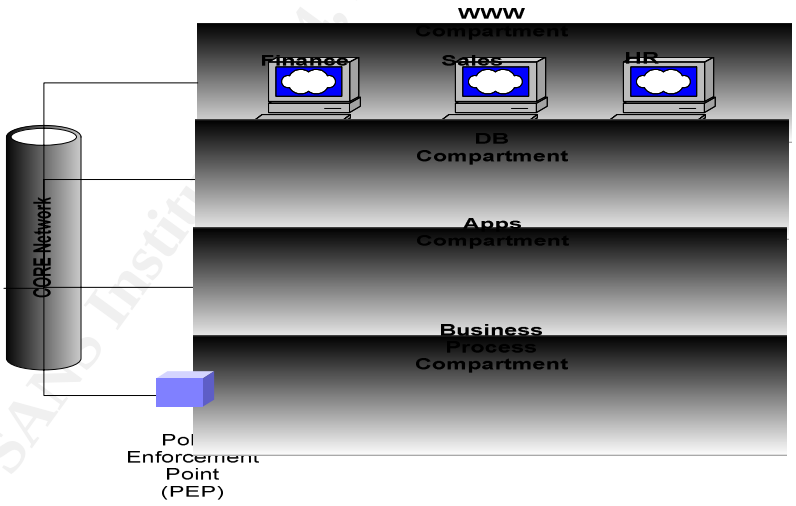
   The goal here is to define the network compartments and map them to your current network layout. The assumption is that you will migrate over time from your current network to the future compartmented network with minimal disruption. There are no hard and fast rules on how to define the compartments. There are many factors unique to your organization that will influence the compartment designs. Generally there are business, system, application, security, and cost considerations that will have to be weighed. This is not an easy task for any organization with even moderately complex IT infrastructure or size.

   Let's look at an example. A company has three business departments; finance, sales, and HR. Each department has four system components; web servers, databases, application servers, and business process servers. Currently every server in all departments resides on one class C subnet in their data center. The company decides to segment its network into compartments. If we use business function as the criterion to define the compartments, then we have three compartments corresponding to each business departments. Within each compartment there are four system components which belong to the department. They translate into three subnets with policy enforcement points at the ingress/egress points into the core of the company network. The advantages of this design are each business department maintains its own security policy and disruption in one compartment does not affect other business areas. A disadvantage is that the security policy at each compartment is likely to be complex.

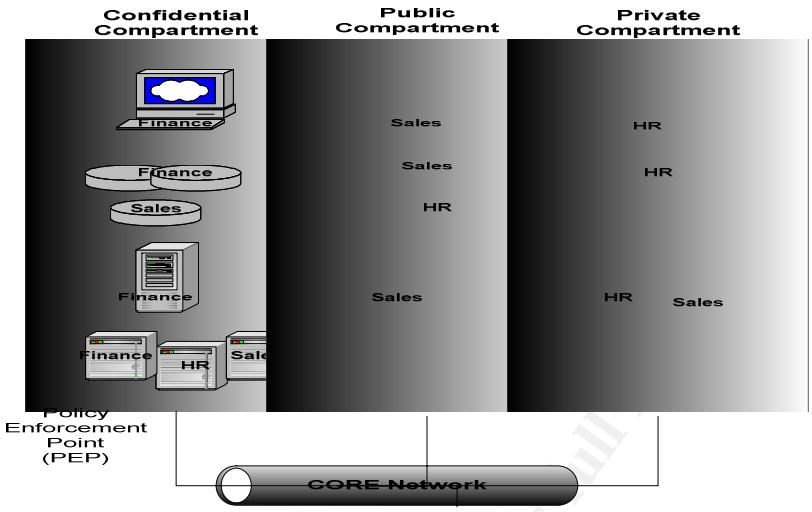
[6] Morris.



If we use the system components as the criterion to define the compartments, we will have four compartments corresponding to the four types of systems we have which gives us four subnets with policy enforcement points. Some advantages of this approach are the security policy at each compartment is simplified and there is a potential for consolidation of servers. One disadvantage is disruption in one compartment potentially impacts all business units.



If we use information classification as the criterion to define the compartments (for the purpose of illustration, let's say the company has confidential, private, and public classes of information) then we have three compartments corresponding to the three classes of information. One advantage here is all information of the same classification is handled uniformly. One disadvantage is we probably will not have an optimized network traffic flow. (I.e. place the servers that access each other the most closely on the network for better performance.)



It is unrealistic to use any single type of criterion to determine the network compartments. A holistic approach using security, technical and business needs are called for here. To illustrate that point, sometimes business plans can affect how the compartments are defined. For example, if you have a near term business goal to outsource all of human resource functions to a third party HR provider than it may be a good idea to segment out the entire HR processing into its own compartment. This way the scope and the impact of outsourcing HR are isolated upfront. The core team has to analyze information collected to determine the appropriate set of criteria that will work best for your organization and your needs. Working from the set of criteria, list and prioritize all the compartments needed. Lay out the newly defined compartments onto your current network architecture. Re-use as much of the IP addressing schemes as practical and assign new subnets to accommodate the compartments. Keep in mind the migration issues from your current network to the new compartmented network at this phase of the work. Given unlimited resources, you can have 100% compartmented network but in real life you will have to content with the top compartments that will give you the most benefits for the money.

4. Define security policies.

   Once the overall compartmented network design is done, we can define security policies for each compartment as well as mechanisms for enforcing the security policies (e.g. firewalls, router access control lists, intrusion prevention system) and monitoring of compliance with the security policies (intrusion detection systems, network sniffers). There are two parts to security policies at each compartment. They are network and host. For the network part, determine the types of traffic that will come into and out of each compartment. They will translate to firewall rules or access control lists to filter the traffic coming in and out of a compartment.

Pay careful consideration to where you actually filter the traffic, layer 2 or layer 3. Traditionally policy enforcement takes place in layer 3 or the router layer; the trend now in the security industry is to push policy enforcement closer to the end devices. A number of vendors are coming out with a "network admission" concept where security policy is enforced at the switch layer[7]. While that gives the most granular access and policy control, the drawbacks are cost and administration. Lack of maturity with these offerings may be a concern. However, layer 2 enforcement may be a great option for some compartments. For example, if you have a compartment that covers an office building with all different types of users from internal company personnel to external consultants to visiting guests, then a combination of layer 2 authentication like 802.1x with admission control which determines, based on authentication, what VLAN the user will be placed and what security policy will be enforced for the user will be a great fit. That way, an authenticated internal user using a company issued laptop with up to date antivirus definitions can have full access everywhere while a visiting guest gets assigned to a rate-limited VLAN with access to the Internet only.

For layer 3 filtering, in a typical Core-Distribution-Access network architecture, filtering at the access layer will give you the most granular control but it will require more policy enforcement devices and heavier management needs. Filtering at the core will take fewer devices but with less granular access control and the effect of miss-configuration has the potential to cause wide spread network outage. Filtering at the distribution layer can be a good middle ground if your network design fits. Once these decisions are made and network traffic to each compartment analyzed, feed that information to tune the monitoring tools to reduce false alerts.

On the host security side, create a profile for servers that reside in each compartment. Include policies on OS hardening, system integrity, host-based intrusion detection/prevention, support methods, auditing, and backup/restore requirement. Use business impact analysis, risk analysis, and information classifications when making these decisions. Having consistent host policies will also help in recovery scenarios where a server has to be rebuilt from scratch.

It is important to balance security with performance, manageability, and cost when deciding the security policies. Generally the tighter the security policy, the more negative impact on network performance and manageability at an increased total cost. Good risk analysis and business impact analysis will help you make the right choice.

5. Implementation.

[7] Cisco Systems.

The overall network design with all the compartments and their respective security policies define the desired future state of your network. Compare that with your current network and do a gap analysis. From the gap analysis, identify tasks that will have to be completed and the order of their execution to get from the current state to the future state. Identify the tasks that are on critical path and ones that can be done in parallel. Create a project timeline for all the efforts to accomplish the tasks. Assemble virtual task teams for each of the efforts, since many of the tasks will involve different areas of the company to collaborate. The byproduct of using virtual task teams is by getting different areas of the company involved up front, we can get buy-in and education of the new segmented network design from all levels of the organization.

A number of newer routers and switches have some abilities in filtering traffic or even intrusion detection capabilities. The prospect of not having to invest money in buying new equipment to do network segmentation may seem attractive but there is a lot of hidden cost in the form of support and maintenance. Doing traffic filtering in a distributed fashion inside of the network poses a large potential risk if the management and change controls are not in place. A simple miss-configuration of a filtering rule has the potential of impacting large portion of the network and users. An enterprise strength policy management tools is a must. There are a number of appliances on the market from different vendors which are targeted for internal network segmentation use with enterprise management consoles. Here are some key features to look for with these devices:

1) Rule-based or policy-based configuration management.
2) High availability capable, both policy enforcement points and management console.
3) Tiered management architecture for better scalability. Role-based access control to give different privileges to different support users.
4) Good network performance under complex rule sets. The security devices can not be a point of failure in the network.
5) VLAN capable. Not just VLAN aware but the ability to filter traffic based on VLANs with virtual instances of firewall for each VLAN.
6) Switch and router modes. Ability to apply rules both in layer 3 and 2.

If the decision is to use existing equipment to enforce segmentation, then it's important to make sure you have a good way to manage the security policies on a wide scale. If the decision is to deploy new equipment for segmentation, then it's important to integrate the new devices into your existing security change/problem management process, procedures and support structure. Getting the best equipment without the organizational support to run and maintain on an ongoing bases will quickly become a source of failure.

6. Maintenance and management.

   The temptation for many people is to look at information security as a collection of tools with graphs and blinking colored lights. The fact is security is a process. Tools when implemented well and used appropriately can greatly facilitate that process. Maintenance and management are part of the process that makes up the entire security lifecycle. The scope of any security project has to include impact to that process.

   One challenge with any architecture change such as this is how to maintain the original design goal in the long run. In other words, you have built an infrastructure according to a set of blueprints (architecture), as days go on, new pieces are added or existing structures modified, and eventually you end up having something that's quite different from what you started with. To maintain the original design goals of the compartmented network, we have to rely on education and re-engineering of the change management and support structure to ensure the preservation of network segmentation or policy domains. For example, educate the network designers and project managers on the whole concept of compartmented network design so that new systems are built accordingly to not just fall in line but also take advantage of the new network design. Re-engineer the change management process so that adding a new server goes through a security policy evaluation to determine the correct compartment to place the new server and the impact to the security policies currently enforced on the target compartment. Create new processes to take advantage of the new capabilities with compartmented network. For example, a suspected intrusion or a worm outbreak in one compartment triggers IDS alerts which lead to modification of filtering rules on the compartment to quarantine the affected compartment while the rest of the network keeps working. Explore proactive measures with this network design. For example, a CERT alert on a new Acme database vulnerability starts a process to create a new IDS signature for compartments that have Acme database servers so that any attempts to exploit the vulnerability can be alerted.

Conclusion

The traditional security model of "hard shell/soft center" can no longer cope with the pace of change today and the ever higher demand for information security. Today's businesses require more sharing of information within the enterprise as well as with external partners through the corporate firewalls. This trend exposes more systems and devices to external threats than ever. In addition, internal threats are also on the rise with more lethal consequences. To address the new

business environment, the answer is a compartmented network design where collections of IT resources are grouped into compartments each with its own set of security policies. By breaking up large enterprise infrastructure into multiple smaller policy domains, finer access control and granular security can be achieved. The results of this layered approach provides flexible and scalable security solutions to deliver the right amount of protection where needed. In addition, this design enables the enterprise to take greater advantage of connectivity methods like MPLS or shared IP portals by lessening the dependencies on a secured wide area network infrastructure. The value proposition of this design is apparent. Organizations should begin looking at this approach as the next logical evolution of their network design.

References

1. Hewlett-Packard Development Company. “Adaptive Network Architecture (ANA)”. July 2003.
   URL: ftp://ftp.hp.com/pub/services/network/info/ana_wp.pdf (8 July 2004).

2. Clark, Paul, Meissner, Marion, Vance, Karen. “Secure Compartmented Data Access over an Untrusted Network Using a COTS-based Architecture”.
   URL: http://www.acsac.org/2000/papers/71.pdf (8 July 2004).

3. Convery, Sean, Trudel, Bernie, Abelar, Greg, Halpern, Jason. “SAFE: A Security Blueprint for Enterprise Networks”. 2004.
   URL:
   http://cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/networking_solutions_white_paper09186a008009c8b6.shtml (8 July 2004).

4. Nortel Networks. “Unified Security Architecture for Enterprise Network Security”. 2002.
   URL:
   http://www.nortelnetworks.com/solutions/security/collateral/nn102060-0902.pdf (8 July 2004).

5. Juniper Networks. “Network Segmentation”. 2004. URL:
   http://www.juniper.net/products/integrated/virtual_system_arch.html (14 May 2004).

6. Bhatnagar, Atul. “How to protect the network from the inside out”. Computerworld Magazine. 13 May 2004.
   URL:
   http://www.computerworld.com/securitytopics/security/story/0,,92920,00.html?SKC=security-92920 (14 May 2004).

7. Morris, Alan. “Next Generation Team”. Cranfield University. April 2001.
   URL: http://www.cranfield.ac.uk/coa/macro/nextgen/newpage3.htm (8 July 2004).

8. Westerinen, A., Schnizlein, J., Cisco Systems, Strassner, J., Intelliden Corporation, Scherling, M., xCert, Quinn, B., Celox Networks, Herzog, S., PolicyConsulting, Huynh, A., Lucent Technologies, Carlson, M., Sun Microsystems, Perry, J., Network Appliance, Waldbusser, S.. “RFC 3198 Terminology for Policy-Based Management”. November 2001.

9. Blum, Dan. “Directory and Security Strategy Overview”. May 2003. URL:
   http://www.burtongroup.com/research_consulting/doc.asp?docid=424 (8 July 2004).

10. Cisco Systems. “Implementing Network Admission Control Phase One Configuration and Deployment”. Version 1. 2001. URL: http://cisco.com/application/pdf/en/us/guest/netsol/ns466/c654/cdccont_0900aecd800fdd7b.pdf (8 July 2004).

Last Updated: May 30th, 2017

Upcoming Training

SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event