Global Information Assurance Certification Paper

Security Considerations for a Productive "Front Lobby Office"

Submitted for completion of the GIAC GSEC
Practical Version 1.4b
June, 2004

Ric Batty
SANS GSEC
Course: January 2004
Canton, MI

Table of Contents

List of Figures

List of Tables

Abstract

The Enterprise of today is making great strides in the use of networking internally to support employee productivity. Network based services available to employees include: file sharing, e-mail, print services and access to the Public Internet. These services are all delivered in a relatively secure fashion on the internal network using company provided IT resources. Most companies also have some level of collaboration tools in place to support employees internally, and the extended enterprise, i.e. the company plus a group of suppliers and partners. These tools provide e-mail exchange and extranet based collaboration, e.g. file exchange or more sophisticated tools such as eRoom or Lotus Notes, which can bring offsite partners and employees together on programs and projects.

An opportunity for collaboration that is often missed is when the outside partners relocate on-premise to perform their work for the Enterprise. For example, when today's companies extend their resources by hiring outside consultants to come "in" and work on-site to further the goals of a project, the level of resources made available is often roughly comparable to those they would have if the outside team setup in the front lobby as their "office". They have access to the building, heat (sometimes cooling), and light but little else! To further aggravate the situation the customer (the Enterprise) is often paying a premium for knowledge and the outside team may be working to very tight deadlines; productivity and efficiency are the watchwords. The outside team gains the effectiveness of face-to-face interaction and seeing the problems first hand, but looses the basic productivity tools and services that were taken for granted in their own home office or that which the Enterprise provides for its full-time employees.

This paper will outline some of the opportunities, challenges and considerations in providing baseline network-based services to an outside group of knowledge workers when they are working on-site, within the Enterprise. The goal is to provide as much service capability to the group of non-employees located in the "front lobby office" as possible, with a focused eye towards securing the Enterprise assets.

Document Conventions

When you read this practical assignment, you will see that certain words are represented in different fonts and typefaces. The types of words that are represented this way include the following:

`command`	Operating system commands are represented in this font style. This style indicates a command that is entered at a command prompt or shell.
`filename`	Filenames, paths, and directory names are represented in this style.
`computer output`	The results of a command and other computer output are in this style
URL	Web URL's are shown in this style.
Quotation	A citation or quotation from a book or web site is in this style.

Introduction

The Enterprise of today is making great strides in the use of networking internally to support employee productivity. Network based services available to employees include: file sharing, e-mail, print services and access to the Public Internet. These services are all delivered in a relatively secure fashion on the internal network using company provided IT resources. Most companies also have some level of collaboration tools in place to support employees internally, and the extended enterprise, i.e. the company plus a group of suppliers and partners. These tools provide e-mail exchange and extranet based collaboration, e.g. file exchange or more sophisticated tools such as eRoom or Lotus Notes, which can bring offsite partners and employees together on programs and projects.

An opportunity for collaboration that is often missed is when the outside partners relocate on-premise to perform their work for the Enterprise. For example, when today's companies extend their resources by hiring outside consultants to come "in" and work on-site to further the goals of a project, the level of resources made available is often roughly comparable to those they would have if the outside team setup in the front lobby as their "office". They have access to the building, heat (sometimes cooling), and light but little else! To further aggravate the situation the customer (the Enterprise) is often paying a premium for knowledge and the outside team may be working to very tight deadlines; productivity and efficiency are the watchwords. The outside team gains the effectiveness of face-to-face interaction and seeing the problems first hand, but looses the basic productivity tools and services that were taken for granted in their own home office or that which the Enterprise provides for its full-time employees.

The challenges faced will span technology, security, and policy. The advantages that can be gained are attractive, but the security requirements and today's available technology are not quite ready to deliver the new operating model for LAN connection and use.

This paper will outline some of the opportunities, challenges and considerations in providing baseline network-based services to an outside group of knowledge workers when they are working on-site, within the Enterprise. The goal is to provide as much service capability to the group of non-employees located in the "front lobby office" (FLO) as possible, with a focused eye towards securing the Enterprise assets.

The general approach will begin with identifying the baseline (typical) services to be considered for delivery to the FLO residents and also baseline (typical) policy that would be in place prior to adding the service access capability.

Baseline Services

A reference for the network-based services to be provided is the set of services that are available to an employee with full access to the internal Enterprise network, recognizing that it may not be possible to provide all of these to the "Front Lobby Office Resident" (FLOR). A comparison of services follows that sets expectations based on the services available to employees, and then possibilities for those provided to the FLOR. The services to be considered are:

Service	Details/Expectations
e-mail/calendar	Employee: Full access to individual mail account using a dedicated e-mail client (e.g. Outlook). Typical protocol needed is POP3 or IMAP. FLOR: Expectation would be the same full access and opportunity to use a dedicated client. Typical protocol needed is POP3 or IMAP. A less functional fall-back would be web-based e-mail, using HTTP. There not an expectation that employees and FLO residents would be able to schedule calendar events as if they were members of the same system.
File sharing	Employee: MS-Windows style file shares on a local file server. Uses basic MS-Windows protocols and presumes an Active Directory based authentication and authorization model. FLOR: Similar to employee. An alternative would be the available collaboration tools that are used when Enterprise employees interact with outside partners who are located off-site.
Print services	Employee: MS-Windows style print servers. Uses basic MS-Windows protocols and again presumes an Active Directory based authentication and authorization model. FLOR: Similar to employee. An alternative would be to consider printers supplied by the FLOR team and dedicated to their use.

Service	Details/Expectations
Public Internet access	Employee: Firewalled access to the Public Internet with support for authentication, authorization, and accounting. FLOR: Similar to employee, firewalled access to the Public Internet with support for authentication, authorization, and accounting.
Collaboration Tools	Employee: Collaboration tools that allow various types of interaction and information exchange. The most important of which include: • Document distribution (one way) • Document collaboration (means for multiple editors and revision control) • Light-weight work flow • Notification of information (document) availability and change status. The presumption is availability of collaboration tools that support this interaction between employees, and between employees and outside partners. An example would be an eRoom implementation that is supports Internet access (e.g. is hosted in a B2B networking environment); an extranet service. FLOR: Similar to employee. An alternative would be to use the Internet access mechanism for reaching the collaboration tools.

Table 1: Baseline Services

The general FLOR expectation is to have a fairly rich set of services available similar to those that would be available if the FLOR team were back in their own office facility, where interaction with the client (employees) would be through Public Internet based exchange of information and an extended enterprise type of approach. The goal is not necessarily to have the FLOR team gain the status of being fully integrated (but different) members of the Enterprise. More specifically for example, the FLOR team would not have e-mail accounts in the Enterprise's system.

Network Security Policy

The intent here is not to enumerate all security and controls policy that an Enterprise would have in place but rather to highlight specific areas of typical policy to draw attention to keys issues and challenges. The impact of these typical polices will be compared between the employees and FLO residents to understand their security and implementation requirements implications. These typical policies are numbered here for ease of reference.

P1	Only Company provided (therefore Company managed) computers may be connected to the internal network.
P2	Each employee has and uses a unique identity. Use of generic identities or the sharing of identities between employees is prohibited.
P3	Access to Company computing resources and services will be authenticated.
P4	Use of Company computing resources is auditable, requiring appropriate accounting mechanisms to be in place.
P5	All Company PC's will have anti-virus software installed, active, and routinely updated (virus signature files).

Table 2: Baseline Policies

This policy set is representative of a somewhat traditional corporate network and systems implementation approach. The first line of defense for the network is strict control (policy) over what can connect to it; quite a bit is dependant on P1. The presumption was that by strictly limiting the connecting devices (PC's etc.), and then managing those devices (P5), the security of the network and attached resources could be maintained. Providing an authentication means for all employees coupled with restricted network access gives the illusion of authorization and resource access control.

The weakness here of course is that the security model is basically that of "hardened walls" with relatively unprotected resources in the interior. This approach, although it served industry for many years, poses serious security and operational issues today. Most of the issues center around the need for a more granular access and authorization mechanism than simple, one level network access authentication provides. Operationally it is awkward as companies move towards mixing dedicated knowledge workers (i.e. salaried employees) and the sporadic access needs of other groups of workers (for example hourly

employees). Extending network access to non-employees only aggravates this situation further. The security weaknesses of this approach can be summarized from another domain[1]:

> *"If you entrench yourself behind strong fortifications, you compel the enemy to seek a solution elsewhere."*
>
> Carl Von Clausewitz, Military Theorist (1780-1831)

This perimeter defense approach to network, and therefore system, security was basic and evolved from the early notion that you were either "on the network" or not; once you were "on" you could reach anywhere the network went. This model is clearly become outdated for two fundamental reasons: first, it is very shallow from a defense-in-depth perspective; and second, today's business processes and collaborative needs are being restricted.

Revised Security Policy

Defense-in-depth security strategies would demand policy changes even if network access was still restricted to just employees. Alternate paths past or over the perimeter defense leave the Enterprise vulnerable even when it is just employees connected to the network. E-mail borne malware is today's trebuchet relative to the castle wall-like network perimeter defense approach.

Future networks need to be engineered to consider the following prior to letting devices (PC's etc.) gain an effective connection to network services:

Network Service	The "network" is a set of services that vary in performance, geographic availability, geographic reach, application services available, etc. These different network services require different levels of authorization and depend on the other characteristics below.
Who	The network must be aware of the identity, require the authentication of, and determine the authorization rights of a connection requesting client.
What	Beyond just authenticating the user, the network must be able to determine key characteristics of the connecting device. Including operating system, operational status of anti-virus software, on-device VPN capability, encryption capability, etc.

[1] Crume, Jeff. "Inside Internet Security". London: Person Education Limited, 2000, Chapter 20

How	The network services provided to a specific device, with an authenticated and authorized user, may vary depending on how the device is connecting; a Public Internet based connection may be provided less network "service" than an in-office LAN connected user.
When	Network service availability may be restricted at different times. For example, Front Lobby Office network access services may only be available from 8:00am-5:00pm.

Table 3: Network Access Considerations

All of these considerations exist in today's networks, but they generally occur after the user/device has connected to the network. In light of the above the previously stated security policy set is re-visited.

P1*	Computers requesting access to internal network will be connected to the appropriate network service set, depending on who, what, how, and when of the request. Recommendations and limitations for non-Company provided devices will be published, including employee purchased devices.
P2*	Any user requesting access to the network must have and use a unique identity. Use of generic identities or the sharing of identities between employees is prohibited. A network service set for administrative purposes exists to assist in initiating new users (identities).
P3*	Access to Company computing and network resources and services will be authenticated.
P4*	Use of Company computing and network resources is auditable, requiring appropriate accounting mechanisms to be in place.
P5*	All Company PC's will have proper security support capabilities (anti-virus software etc.) installed, active, and routinely updated (virus signature files, etc.). PC's and devices (Company provided or otherwise) which to not have the proper security support capabilities in place will received limited network access, or possibility none.

Table 4: Revised Security Policy

The revised policies (P1*) recognize that users and devices beyond those company-owned and managed could provide benefit to the company by being allowed access to the network and services it connects to. This would include

employee purchased cell phones and PDA's and also supplier and partner owned equipment. P2*-P4* emphasize the need for "AAA", authentication, authorization, and accounting, for all network service access. P5* recognizes the role that the connecting device plays in the overall security strategy.

There are two primary implications of all of this:

1. Network identity and Enterprise identity is converging[2] and further converging with a need to know identities in the Extended Enterprise (suppliers etc.).
2. Authorization for different levels of network services will be based on both user identity and device characteristics. Device characteristics being more involved than just device identity (MAC address, or connection port).

What is proposed here is making basic access to the network a managed process. As will be explained later numerous vendors in the network industry are moving in this direction. Network Access Management (NAM) will be used as a generic term for this capability to avoid confusion with specific vendor initiatives. The next step is to examine security and network technologies that can be brought to bear on the original problem of providing network-based services to the team members in the Front Lobby Office.

[2] Schacter, Phil. "Identity-Based Network Access Control and Security". Burton Group, June 3, 2004.

Network Access Management Technologies

Background

Several companies have announced intentions and products to address network access management inline with the considerations and policies previously discussed. Underlying most of these product and strategy announcements are a few key network and security technologies.

The initial problem to be solved is authenticating the user and obtaining device characteristics prior to admitting them to the network. The user device is obviously connected to some network equipment for this to proceed; by access (admission) we mean enabling the device to have its packets routed and be actively participating in some network-based service. A basic technology to support this has been around for some time—PPP[3]. The Point-to-Point Protocol his commonly used by dial-up Internet Service Providers as a means to authenticate a user prior to actually connecting them to the network.

For more flexibility in the authentication mechanism PPP was extended and now sitting inside of it is EAP, the Extensible Authentication Protocol. This move was to standardize extensions to allow other forms of authentication than just ID and password, for example one time password tokens or PKI (Public Key Infrastructure) certificates. To bring this into the Enterprise LAN one more technology comes into the mix—IEEE 802.1x Port-Based Network Access Control. IEEE 802.1x[4] defines EAP over a LAN (EAPOL) which is the needed capability beyond what PPP provides.

A simple example to explain the basics of 802.1x is shown below[5]. The requesting client is called the supplicant, the authentication server is the actual device performing the authentication, and finally the network device brokering the transaction (such as the wireless access point in the diagram) is the authenticator. Typically the authentication server is based on RADIUS for the most flexibility. Only after the supplicant as successfully authenticated will the access point "switch" the user's IP traffic onto the network. Prior to that, only the supplicants EAPOL generated packets are on the network; defense-in-depth, the switch is protecting the network until after the authentication succeeds.

[3] Snyder, Joel. "What is 802.1x?". Network World Global Test Alliance. Network World Fusion, May 6, 2002. URL: http://www.nwfusion.com/research/2002/0506whatisit.html
[4] LAN/MAN Standards Committee of IEEE Computer Society. "IEEE Standard 802.1X-2001, Port-Based Network Access Control". IEEE, July 13, 2001.EE 802.1x
[5] "802.1x". Network World Fusion URL:http://www.nwfusion.com/details/474.html

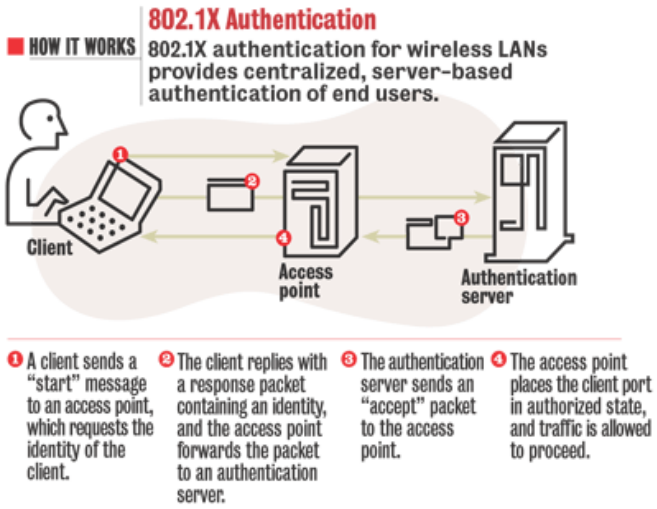

Figure 1: IEEE 802.1x Authentication

Effectively the 802.1x protocol has allowed the screening of the client from the network until it has met the network access management criteria, in this case authentication against a RADIUS server. If the supplicant and the authentication server were enhanced to include additional information in their exchange, specifically the device related information referenced in Table 3: Network Access Considerations, then the overall process of gaining access to the network could be managed to take into account both user identity information and also device characteristics. Identity based decisions could direct the network connection to a reduced service network for a non-employee for example. A device-status based decision could direct the connection to a "repair" network or holding pen, even for an employee client device, if it lacked the appropriate anti-virus controls for example.

If the network switch device in the authenticator role is VLAN (Virtual LAN) enabled then the overall flexibility of the solution is greatly enhanced. Between the user profile information available from the authentication server and device profile information from an agent on the supplicant device the user could be appropriately channeled to specific VLAN consistent with their state combination. At the same time unauthorized users, or rogue devices, could be shunted to a quarantine zone.

Industry Products

A number of vendors have announced product plans and strategies in the area of Network Access Management. A sampling is:

Alcatel	Introducing its Automated Quarantine Engine switch technology that works with intrusion-detection systems (IDS) to isolate worm-infected machines for remediation purposes. This is in addition to its authenticated VLANs[6].
Enterasys	Recently introduced its Automated Security Manager, which provides policy-based control on its switches through help from IDS; and this month the company will expand its quarantine mechanism through use of information from scanners and anti-virus policy enforcement. Enterasys is an early player in the authenticated VLAN product arena.
Cisco	It will enable its Catalyst switches to defend against worms and distributed denial-of-service (DoS) attacks. This goes along with announcements beginning late last year of Cisco Network Admission Control for its routers.
Nortel	Expands its support for 802.1x authenticating port-based security to both wired and wireless switches. Will partner with Sygate to deliver quarantine capability for non-compliant supplicants[7].

Table 5: Vendor Product Announcements[8]

All of these approaches depend on additional agents on the supplicant device (client) and major upgrades or change out of the existing network equipment.

[6] Hayes, Jeff. "CrystalSec: Alcatel Information Security Framework". URL: http://www.ind.alcatel.com/library/whitepapers/wp_CrystalSec.pdf
[7] Schacter, Phil. "Identity-Based Network Access Control and Security". Burton Group, June 3, 2004.
[8] Messmer, Ellen. "Switches taking on new security roles". Network World, June 14, 2004. URL: http://www.nwfusion.com/news/2004/0614switchsecurity.html

Cisco Network Admission Control

The most comprehensive product plan is probably Cisco's Network Admission Control (CNAC)[9].

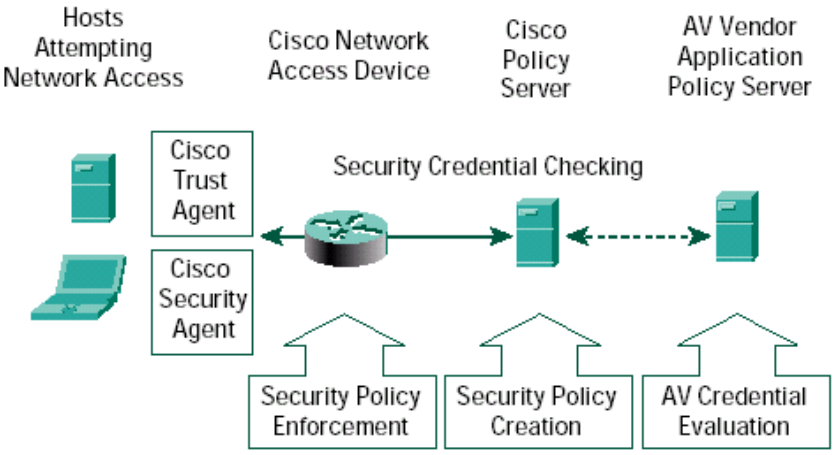

Figure 2: Cisco NAC

Cisco NAC has the following components:

- *Cisco Trust Agent—Software that resides on an endpoint system. The trust agent collects security state information from multiple security software clients, such as anti-virus clients, and then communicates this information to Cisco network access devices, which enforce admission control. Cisco has licensed trust agent technology to its anti-virus co-sponsors so that it can be integrated with their security software client products. The trust agent will also be integrated with the Cisco Security Agent to enforce access privileges based on an endpoint's operating system patch level. Cisco Security Agent, a day-zero host protection software solution, will assess the operating system version, patch, and hot fix information and will communicate this information to the Cisco Trust Agent. Hosts that are not running the proper patches may be given limited access or denied network access.*
- *Network access devices—Network devices that enforce admission control policy include routers, switches, wireless access points, and security appliances. These devices demand host security "credentials" and relay this information to policy servers, where network admission control decisions are made. Based on customer-defined policy, the network will enforce the appropriate admission control decision—permit, deny, quarantine, or restrict.*
- *Policy server—Evaluates the endpoint security information relayed from network access devices and determines the appropriate access policy for them to apply. The Cisco Secure Access Control Server (ACS), an authentication, authorization, and accounting (AAA) RADIUS server, is the foundation of the policy server system. It works in concert with Cisco NAC co-sponsor application servers that provide deeper credential validation capabilities, such as anti-virus policy servers.*
- *Management System—CiscoWorks VPN/Security Management Solution (VMS) provisions Cisco NAC elements, while CiscoWorks Security Information Manager Solution (SIMS) provides monitoring and reporting tools. Cisco NAC co-sponsors provide management solutions for their endpoint security software.*

[9] "Cisco Network Admission Control". URL: http://www.cisco.com/en/US/netsol/ns466/networking_solutions_white_paper0900aecd800fdd66.shtml

This appears to be a very powerful strategy, with every network device a point of security policy enforcement; Cisco would have all its switches NAC aware. Unfortunately, delivery of the capability across the needed product line is 6-12 months out[10].

NAM Technology Summary

So the major players in the network equipment industry have a strategy that is directly in line with the original problem of interest—supply some network based services to a group of non-employees in a way that does not compromise the security of the Enterprise intranet. There are a few drawbacks to this strategy however:

- The full set of the technology required is not ready.
- Significant equipment would need to be acquired/re-worked.
- Distribution of the trust agent software (CNAC solution and others).
- Cost/value proposition is not fully fleshed out. Especially for the FLO resident network access need.

[10] Hochmuth, Phil. "Cisco raising router security". Network World, June 21, 2004. URL: http://www.nwfusion.com/news/2004/062104cisco.html

Solution Proposal

Many of the individual network technologies discussed are available now at varying levels of capability relative to an overall integrated approach such as Cisco's NAC. Staying focused on Cisco equipment, the following is available:

1. 802.1x authentication exchange with a RADIUS server[11]
2. Integration of this authentication server with RSA SecurID one time password token use
3. Ability for selected switches and wireless access points to participate in a VLAN configuration

Recalling from earlier the goal was to provide basic capabilities to a group of "Front Lobby Office" residents via access to a restricted set of network services, below is possible compromise:

Service	Implementation for FLO Residents
e-mail/calendar	Provide Internet access that would allow POP3, IMAP, or HTTP to pass through.
File sharing	Use an Internet accessible tool such as eRoom.
Print services	Use dedicated printers supplied by FLO team.
Public Internet access	Provide access to an outbound firewall.
Collaboration Tools	Use an Internet accessible tool such as eRoom.

Table 6: FLO Resident Services

The approach above depends on providing the FLO team authenticated access to the Internet and then using existing (in many Enterprises) extranet accessible collaboration tools. An additional constraint on the solution is to comply with the set of polices that are listed in Table 4: Revised Security Policy. Some key requirements are:

- Ability to authenticate the FLO team
- Not compromise the intranet should the FLO team client devices contain viruses etc.
- Ability to deploy this solution incrementally, not requiring rewiring of entire office buildings

[11] "RSA SecurID Ready Implementation Guide: Cisco WLAN solution w/ PEAP". URL: http://rsasecurity.agora.com/rsasecured/results.asp?product_company=cisco

The solution recommended is a combination of technologies and equipment that is already present in many Enterprises and an approach designed to minimize the impact on the existing network infrastructure. Typically in-place technologies are referenced in the details below:

1. For authentication use RSA SecurID one time password tokens. Administratively link the RSA ACE Server database (user authentication database) to an existing business partner directory or create procedures to add/delete FLO users.
2. Create separate access groups in the ACE Server database for each separate FLO team.
3. Create a separate VLAN for each FLO team and allocate a VLAN-enabled wireless access point to the FLO team.
4. Issue specially encoded wireless access cards (e.g. Cisco Aironet 350 PCMCIA cards) that are configured for the dedicated access point and the VLAN configuration.
5. Insure the outbound Public Internet proxy is reachable from the dedicated VLAN setup in 3. above.

Use of the SecurID tokens provides authentication and accountability, but avoids the overhead and concerns with entering non-employees into corporate directory implementations such as Active Directory coupled with Exchange. Its use can leverage existing familiarity and some of the support processes.

Use of wireless LAN technology such as Cisco's Aironet family provide high security, network access switching (802.1x Protected EAP), and the ability to be configured for specific VLAN connection. The driver for using wireless equipment is to minimize the amount changes to the network equipment plant installed in the office area where the FLO team will be working. The FLO team would still be prohibited, by policy, from connecting to the wired LAN whose ports are unchanged. Their means of connection would be over basically a dedicated WLAN, tied to the configuration of the wireless cards and access point provided (the access point would be installed by an Enterprise network group). Once properly authenticated they would be switched onto a dedicated VLAN, their team only.

The SecurID tokens and WLAN cards would have to be managed; allocated to a team on their arrival, reclaimed on departure. The supporting RSA ACE server logs would require review and it would be prudent to monitor the VLAN activity.

Next steps for such a solution proposal would be in-lab proof of concept.

References

1 LAN/MAN Standards Committee of IEEE Computer Society. "IEEE Standard 802.1X-2001, Port-Based Network Access Control". IEEE, July 13, 2001.

2 Snyder, Joel. "What is 802.1x?". Network World Global Test Alliance Network World Fusion, May 6, 2002. URL: http://www.nwfusion.com/research/2002/0506whatisit.html

3 "802.1x". Network World Fusion URL: http://www.nwfusion.com/details/474.html?def

4 Crume, Jeff. "Inside Internet Security". London: Person Education Limited, 2000

5 Schacter, Phil. "Identity-Based Network Access Control and Security". Burton Group, June 3, 2004.

6 Messmer, Ellen. "Switches taking on new security roles". Network World, June 14, 2004. URL: http://www.nwfusion.com/news/2004/0614switchsecurity.html

7 Hochmuth, Phil. "Cisco raising router security". Network World, June 21, 2004. URL: http://www.nwfusion.com/news/2004/062104cisco.html

8 Hayes, Jeff. "CrystalSec: Alcatel Information Security Framework". URL: http://www.ind.alcatel.com/library/whitepapers/wp_CrystalSec.pdf

9 "Cisco Network Admission Control". URL: http://www.cisco.com/en/US/netsol/ns466/networking_solutions_white_paper0900aecd800fdd66.shtml

10 "Q & A: Cisco Network Admission Control". URL: http://www.cisco.com/en/US/netsol/ns466/netqa0900aecd800fdd6f.html

11 "Implementing Network Admission Control: Phase One Configuration and Deployment". URL: http://www.cisco.com/application/pdf/en/us/guest/netsol/ns466/c654/cdccont_0900aecd800fdd7b.pdf

12 Convery, Sean , Miller, Darrin , Sundaralingam, Sri. "Cisco SAFE: Wireless LAN Security in Depth". URL: http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/networking_solutions_white_paper09186a008009c8b3.shtml

13 "RSA SecurID Ready Implementation Guide: Cisco WLAN solution w/ PEAP". URL: http://rsasecurity.agora.com/rsasecured/results.asp?product_company=cisco

14 "Network Access Quarantine Control in Windows Server 2003". URL: http://www.microsoft.com/windowsserver2003/techinfo/overview/quarantine.mspx

Last Updated: September 21st, 2017

Upcoming Training

Community SANS New York SEC401*	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
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
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
Mentor Session - SEC401	Minneapolis, MN	Oct 03, 2017 - Nov 14, 2017	Mentor
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 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	
Community SANS Omaha SEC401	Omaha, NE	Oct 23, 2017 - Oct 28, 2017	Community SANS
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
Community SANS Colorado Springs SEC401**	Colorado Springs, CO	Nov 06, 2017 - Nov 11, 2017	Community SANS
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
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
SANS San Francisco Winter 2017	San Francisco, CA	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 London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
SANS Austin Winter 2017	Austin, TX	Dec 04, 2017 - Dec 09, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Dec 04, 2017 - Dec 09, 2017	Community SANS
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event