IT Audit:
Security Beyond the Checklist

Copyright SANS Institute

Author Retains Full Rights

This paper is from the SANS IT Audit site. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"20 Critical Security Controls: Planning, Implementing and Auditing (SEC440)"
at http://it-audit.sans.orghttp://it-audit.sans.org/events/

TunnelGuard Service and Administrative Plane on Contivity Secure IP Services Gateway Platform: An Administrator's Report

GIAC System and Network Auditor
Practical Version 2.1 (amended July 5, 2002)
Option 1

Alejandro Buschel
February 26, 2004

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004 As part of GIAC practical repository Author retains full rights

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

TABLE OF CONTENTS

Abstract ***4***

Assignment 1 – Research in Audit, Measurement, Practice and Control ***5***

Identify the system to be audited **5**

Computer Model, Operating System and Software Version **5**

Network Diagram **5**

Evaluate the Risk to the System **7**
Background 7
Methodology 7
Table 1- Values for Risk Assessment 8
Table 2 - Vulnerabilities 9

Operations **9**

Network **9**
Table 3 – Threats 9

Impact Determination and Overall Risk Rating **10**
Table 4 – Impact Values and Risk Values 10

Discussion of Risk Value Assignments **13**
Table 5 – Management plane and TunnelGuard vulnerabilities 13

Current State of Practice **14**
Figure 2 – TunnelGuard operation 16

Assignment 2 – Create an Audit Checklist ***17***

Introduction **17**
Audit Task 1 - Test network services available via the public interface 18
Audit Task 2 – Test network services available via the private interface 18
Audit Task 3 – Configuration of local and remote logging 19
Audit Task 4 – Auto Backup is configured and working 20
Audit Task 5 – Time synchronization 20
Audit Task 6 – Unnecessary services 21
Audit Task 7 – TunnelGuard Policy Enforcement 21
Audit Task 8 – Test External Client DHCP service 22
Audit Task 9 - Configuration of SNMP Traps 22
Audit Task 10 –External User Authentication Service 23
Audit Task 11 – SANS Top 20 – OpenSSL implementation is vulnerable 23

Assignment 3 – Audit Evidence ***24***

Results of the Audit **24**
Audit Task 1 PASS 24
Audit Task 2 FAIL Finding 1 25
Audit Task 3 PASS 26
Audit Task 4 PASS 27

© SANS Institute 2004 As part of GIAC practical repository Author retains full rights

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Audit Task 5 PASS ____ 30
Audit Step 6 FAIL Finding 1 ____ 30
Audit Task 7 PASS ____ 31
Audit Task 8 PASS ____ 36
Audit Task 9 PASS ____ 36
Audit Task 10 PASS ____ 39
Audit Task 11 FAIL Finding 2 ____ 40

Measurement of Residual Risk ____ 41

Is the System Auditable? ____ 41

Assignment 4 - Risk Assessment ____ 42

Summary ____ 42

Background ____ 42

Audit Recommendations ____ 44

Costs ____ 45

References ____ 45

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004 As part of GIAC practical repository Author retains full rights

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Abstract

This paper will look at the configuration options of TunnelGuard service, the administrative context of managing the Contivity platform and other efforts by various vendors to provide similar functionality.

The audit will focus on the feasibility of using TunnelGuard as part of a Defense in Depth approach to security. In addition, the management plane of the VPN gateway was audited. A solid framework is required for managing the entry point into an enterprise, in this case by remote users communicating over the Internet.

The audit was conducted using equipment loaded with the most current software release available at that time. The system has not been deployed into production. This audit will provide the framework used to deploy this system and create a checklist to work with as the system gets put into operations and gets upgraded. This checklist can also be used to compare this system to potential replacements, should the need arise.

The audit is structured in four sections. The first section describes the system, analyzes its risks and describes the current state of practice. The second section is the audit checklist. The third section documents the audit. The fourth section is the report of the audit findings, including the controls available to mitigate the risks, if any, found during the audit.

© SANS Institute 2004, Author retains full rights

© SANS Institute 2004 As part of GIAC practical repository Author retains full rights

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Assignment 1 – Research in Audit, Measurement, Practice and Control

Identify the system to be audited

The system being audited functions as an IPSec VPN Gateway. This device is used to terminate client-initiated IPSec VPN tunnels. This system is therefore a controlled entry point into the network.

The gateway provides several configuration options for the VPN clients, as well as several options for its own management.

The goal of this audit is to evaluate the options available for management of the system as well as extending the Defense in Depth framework to the client computers while connected to the network via this system.

TunnelGuard is the mechanism available to configure, provide and enforce a set of policies that clients must comply with at all times in order to gain access to the network remotely.

Computer Model, Operating System and Software Version

The system being audited is a Nortel Networks' Contivity 2700 Secure IP Services Gateway.
This system is running server software version 4_80.124.
The version of TunnelGuard running in the client is 1.1.1.0.0.082. This version ships with the server software.
The client software version is not relevant, as TunnelGuard works independently of the client software.

The system is configured with the default options: Two Ethernet 10/100 network cards and one serial port.

TunnelGuard is a Windows-only application. JRE 1.4.1_02 (Java Runtime Environment) or later is required for TunnelGuard installation.

Network Diagram

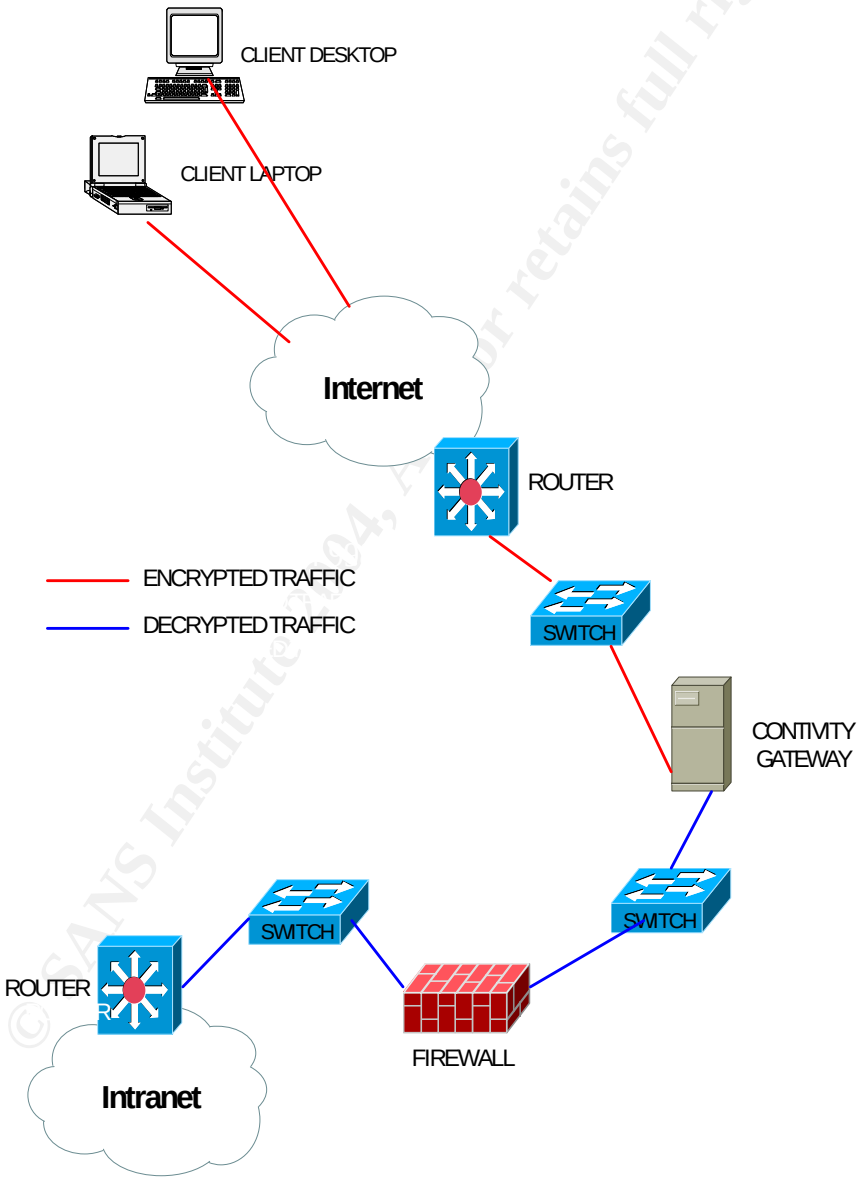
The gateway is located at the edge of the network. The gateway is connected to the internal network via a firewall. This firewall analyzes the traffic after the gateway decrypts it. In addition, the firewall is used to restrict access to the management plane of the gateway.

All external servers that the gateway communicates with are located behind the firewall.

© SANS Institute 2004 As part of GIAC practical repository Author retains full rights

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Figure 1 – Network Layout



© SANS Institute 2004 As part of GIAC practical repository Author retains full rights

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Evaluate the Risk to the System

Background

The VPN gateway is directly exposed to the Internet via its public interface. No administrative services should be configured for use over that interface.

The VPN gateway provides mission-critical access for external users into the corporate network. For this reason, its availability and reliability are crucial. Users rely on the service provided by this system to conduct their daily business. On the other hand, if the VPN gateway fails to apply the defined security policies to the clients connecting there is a risk that a network-based attack like a worm could burrow its way into the corporate network.

TunnelGuard is a recent addition to the Contivity IP Gateway server software. This software allows the gateway administrator to define policies that need to be met to gain and retain access to the network via the gateway.

Methodology

This audit is not specific to a company. The policies and guidelines to be followed during this audit take into account the role the VPN gateway plays on a network, enabler of remote access to users. The management plane, the ways and means to control the configuration of this system, is of outmost importance. The management plane is considered to carry confidential information; therefore the outmost care should be applied to this plane.

Research into best practices for handling the configuration of systems that provide mission-critical services was conducted. Personal experience related to the use of secure channels for service configuration was also used to evaluate the risks scenarios and to develop a checklist that will capture those risks.

The Webster dictionary defines Risk as the possibility of suffering loss. In terms of computer systems, loss means several things: denial of service is a type of loss, data modification is another type. To analyze the risks a computer system faces there is a need to take into account several factors. The best way to quantify these factors is to assign them values.

The methodology used in this audit to evaluate risk is based on the analysis presented by Dr. Donald R. Peebles at the 1997 National Information Systems Security Conference [1]. A simplified mathematical matrix was used, but the main idea used is the definition of risk as a combination of several factors.

[1] Peeples, Donald. "The Foundations of Risk Management." May 6 1997 http://csrc.nist.gov/nissc/1997/proceedings/577slides.pdf (December 15, 2003)

© SANS Institute 2004 As part of GIAC practical repository Author retains full rights

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

RISK = VULNERABILITY X THREAT X IMPACT

The values assigned to each category allow for all possible combinations. Table 1 provides details on how the overall risk rating is achieved.

Table 1- Values for Risk Assessment

	LOW	MEDIUM	HIGH	CRITICAL
Vulnerability	4	3	2	1
Threat	4	3	2	1
Impact	4	3	2	1
RISK	**64 or HIGHER**	**27-64**	**8-27**	**1-8**

A Threat cannot be realized if there is no Vulnerability. The Threat could be present but there must be Vulnerability for the Threat to lead to an Impact and therefore a specific Risk.

A similar matrix is used by SANS to create the CVA (Critical Vulnerability Analysis)[2].

The risk assessment methodology is applied to a system for which there is no baseline audit information. No assumptions can be made on the security controls in place. The risk assessment is concerned with the availability, reliability and ability of the system to perform the duties it was designed for: provide IPSec services to remote users over the Internet while enforcing Corporate Policies at the clients' computer via TunnelGuard.

The audit scope will include areas of activity that could lead to risks. These areas are: environment, operations, network and operating system.

In order to catalog the risks the VPN gateway faces, the following process will be used to create the audit checklists:

a. Identify vulnerabilities and assign them a value.
b. Identify threats and assign them a value.
c. Verify which Threats can be realized via which Vulnerabilities.
d. Assign an Impact value to the Threats that can be realized.

[2] http://www.sans.org/newsletters/cva/#process (January 14, 2004)

© SANS Institute 2004 As part of GIAC practical repository Author retains full rights

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The values to be assigned are based on Table 1 above.

Table 2 - Vulnerabilities

Environment	Value	
Data Center Viability dependency	Critical	1
Physical Access to the System	High	2
Operations		
System Hardware failure	Critical	1
Failure to detect system malfunction	High	2
Failure to detect system change	High	2
Failure to detect system overload	Medium	3
Network		
Failure of network elements in Data Center	Critical	1
Failure of communication with external User Authentication	Critical	1
Failure of communication with external client IP address assignment services	Critical	1
Failure of communication with external syslog services	High	2
Operating System		
Failure to enforce TunnelGuard policy	Critical	1
Failure to detect erroneous information from TunnelGuard Agent	High	2
Unnecessary services enabled	High	2
TunnelGuard policy is not built properly	High	2
Vulnerable SSL (Secure Socket Layer) implementation	High	2

Table 3 – Threats

Environment	Value	
Data Center suffers catastrophic loss	Low	4
Data Center suffers temporary loss (cooling, power, water, fire)	Medium	3
Operations		
System Theft	Low	4
System Hardware failure	Low	4
Unauthorized Administrative access	Critical	1
Administrative error	Critical	1
System Overload	Medium	3

© SANS Institute 2004 As part of GIAC practical repository Author retains full rights

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Unauthorized client software distribution	Medium	3
Network		
Denial of service attack on management interface	Low	4
Denial of service attack on public interface	Low	4
Operating System		
Abuse of unneeded services	Medium	3
Abuse of HTTPS service	Medium	3

Impact Determination and Overall Risk Rating

Using the data collected in Tables 2 and 3, an Impact Value and Risk Rating can be derived for each Threat that can be realized. To simplify the organization of the data, the risk rating is sorted by Vulnerability.

The audit checklist will be based on the vulnerabilities that are specific to the VPN gateway and therefore under the Administrator's control.

Table 4 – Impact Values and Risk Values

Vulnerability	Threat	Impact	Vulnerability Value	Threat value	Impact Value	Risk Value
Data Center Viability as an operating environment	Catastrophic Facility Loss	Medium to Long Term Denial of Service, Business and Productivity Loss	1	4	1	4 - CRITICAL
	Temporary Environmental Loss (power, fire, water)	Short Term Denial of Service, Business and Productivity Loss	1	3	2	6 - CRITICAL
Physical access to the system	Theft of the system	Short Term Denial of Service, Business and Productivity Loss	2	4	1	8 - HIGH

© SANS Institute 2004 As part of GIAC practical repository Author retains full rights

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

	Unauthorized Administrative Access	Potential Denial of Service, Potential of unauthorized remote access	2	4	1	8 – HIGH
System Hardware Failure	Catastrophic Hardware Failure	Short to Medium Term Denial of Service, Business and Productivity Loss	1	4	1	4 – CRITICAL
Failure to Detect System Malfunction	Administrator Error Hardware Failure	Denial of Service, Business and Productivity Loss	2	1	1	2 – CRITICAL
Failure to Detect System Configuration Changes	Administrator Error Compromise	Potential for Unauthorized Remote Access, Potential for Denial of Service	2	1	2	4 – CRITICAL
Failure to Detect System Overload	System Overload Transient Hardware Failure	Transient Denial of Service, Potential Business and Productivity Loss	3	3	3	27 – MEDIUM
Failure of Network Elements in Data Center	Network Administrator Error Hardware Failure Compromise of network element	Denial of Service, Productivity Loss, Intermittent Service	1	3	2	6 - CRITICAL

© SANS Institute 2004 As part of GIAC practical repository Author retains full rights

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Failure of communication with External User Authentication Service	Administrator error Hardware Failure Attacker compromise	Denial of service, Productivity Loss. The end user will not be able to gain access if he cannot authenticate	1	3	1	3 – CRITICAL
Failure of communication with external DHCP Service	Administrator error Hardware Failure Attacker Compromise	Denial of Service, the user will not be able to access the network	1	3	1	3 – CRITICAL
Failure of communication with external syslog server	Administrator error Hardware Failure Attacker Compromise	Loss of monitoring capability	2	4	2	16 – HIGH
Failure to enforce TunnelGuard Policy	Administrator Error Attacker Compromise Operating System Bug	Unauthorized Access, users could access the network with machines that could pose a threat to the environment	1	4	2	8- HIGH
Failure to detect erroneous information from TunnelGuard agent	Attacker compromise Agent software bug	Unauthorized Access, users could access the network with machines that could pose a threat to the environment	1	4	3	12 – MEDIUM

© SANS Institute 2004 As part of GIAC practical repository Author retains full rights

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Unnecessary Services enabled in VPN gateway	Attacker Compromise Administrator Error Unauthorized Access	Denial of Service Unauthorized remote access to the network	1	3	2	6 – CRITICAL
Clear Text Management Services	Attacker Compromise	Potential for configuration destruction, Potential provisioning of unauthorized service	1	2	2	4- CRITICAL
Vulnerable SSL (Secure Socket Layer) implementation	Attacker Compromise	Denial of Service, Loss of management capability	1	2	2	4 – CRITICAL

Discussion of Risk Value Assignments

Risk Assessment helps us prioritize the finite resources available in an organization. Risks cannot be avoided yet they can be mitigated. The analysis of the risks that the VPN gateway operates under is the first step towards designing and implementing mitigating controls.

The audit will focus only on vulnerabilities that lead to high and critical risks. To further concentrate on the VPN gateway management plane and TunnelGuard, The audit checklist will be developed with a focus on those vulnerabilities that directly affect these functions.

Table 5 lists the specific vulnerabilities that are high and/or critical and apply to the management plane and TunnelGuard.

Table 5 – Management plane and TunnelGuard vulnerabilities

Reference	Vulnerability	Risk Value
V1	Failure to Detect System Malfunction	CRITICAL
V2	Failure of Communication with External User Authentication Service	CRITICAL
V3	Failure of Communication with External DHCP	CRITICAL

© SANS Institute 2004 As part of GIAC practical repository Author retains full rights

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

	Service	
V4	Failure of Communication with External syslog service	HIGH
V5	Failure to enforce TunnelGuard Policy	CRITICAL
V6	Unnecessary services enabled	CRITICAL
V7	SANS Top 20- Clear text management services enabled	CRITICAL
V8	Failure to Detect System Configuration Changes	CRITICAL
V9	SANS Top 20 – OpenSSL implementation is vulnerable	CRITICAL

These vulnerabilities must be interpreted as an integral part of the management plane. Administrator errors are one of the main threats for the management plane. Often times human error and the lack of sanity checks by the system operating system lead to Denial of Service scenarios.

Current State of Practice

Information Security Auditing is a field that has attracted significant attention lately. There are standards developed by a variety of organizations. Some of the more commonly used and referenced are listed below.

- COBIT (http://www.isaca.org/cobit.htm) (Registration required)
- ISO 17799, BS 7799 (http://www.bspsl.com/17799/) (Purchase required)

The ITU has published a draft document that provides a high-level matrix that can be used as a functional basis for an Information Security Audit (http://www.ietf.org/IESG/LIAISON/itut-sg17-ls-x805-end2end-communications.pdf) (January 14,2004)

The scope of this audit is quite specific, yet many of the papers available in the SANS Reading Room (http://www.sans.org/rr) proved useful. SANS GIAC posted practicals for the GSNA certification proved invaluable sources, in particular the paper titled "Auditing a Corporate E-mail Gateway Running Postfix on Linux: an Administrator's perspective" by William Karwich[3]. William wrote a comprehensive paper that was used as an example for data structure and flow. Although the scope of this audit is different from his paper, some of the same considerations apply to this environment.

Nortel Networks (http://www.nortelnetworks.com) publishes detailed operational guides and configuration guides for Contivity and TunnelGuard. Those documents were reviewed extensively to ascertain the controls available and to

© SANS Institute 2004 As part of GIAC practical repository Author retains full rights

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

understand the limitations of the system. No independent papers were found that dealt specifically with TunnelGuard.

Other vendors of VPN hardware and software provide similar functionality to what Nortel offers. Microsoft provides a service called Quarantine with its Internet Authentication Service (IAS)[4]. This service works in conjunction with Windows 2003 and Remote Access Services provided on that platform.
Cisco provides a similar service called Network Admission Control, part of their Self-Defending Network [5].

Corporations and vendors are becoming increasingly aware that a VPN connection extends the perimeter to the client computer that is allowed to connect into the network. The location of the VPN gateway, as well as the network controls applied to the traffic routed by the VPN gateway, are of outmost importance.

A natural extension to the logic of only allowing authorized users into the network is to conduct a real-time assessment of the client computer against corporate policies. The policies that are most relevant in this case relate to AntiVirus software and related definitions, operating system patches and personal firewalls. Additional policies can be enforced, based on the needs of the user.

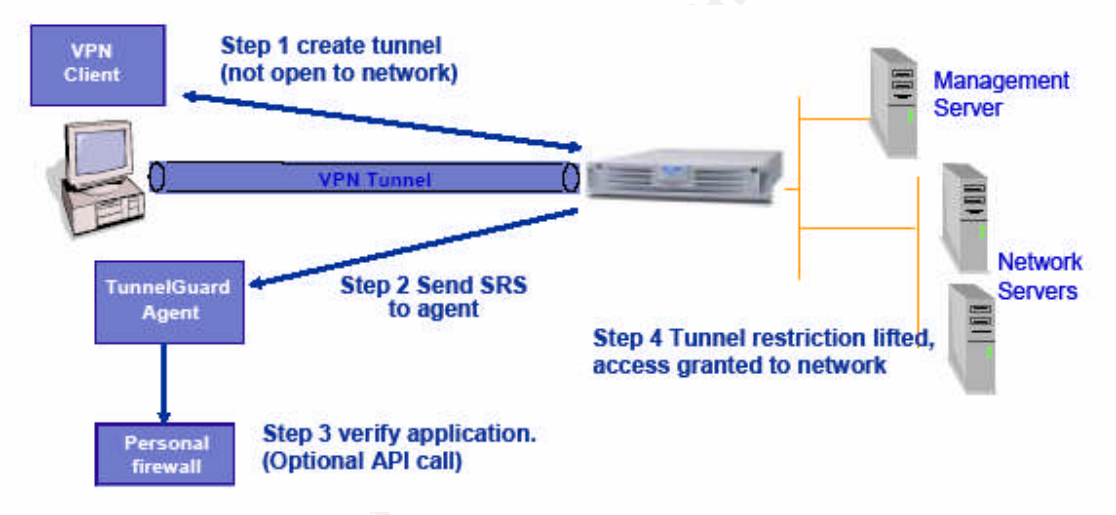
[3] http://www.sans.org/practical/GSNA/William_Karwisch_GSNA.pdf (January 14, 2004)
[4] http://www.microsoft.com/windowsserver2003/techinfo/overview/quarantine.mspx (January 14, 2004)
[5] http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns413/networking_solutions_package.html (Janaury 14, 2004)

© SANS Institute 2004 As part of GIAC practical repository Author retains full rights

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The TunnelGuard agent exists as a separate component and not as a part of the Contivity VPN Client application. The TunnelGuard agent assumes an authenticated VPN tunnel connection to a gateway but requires neither a specific VPN client nor any specific functionality of a particular VPN client. Figure 2 below describes the order of the actions that take place before a user is vetted and can obtain network access. It is important to emphasize that further access controls can be enforces by either the firewall in the VPN gateway or the firewall that connects the gateway to the Intranet.

Figure 2 – TunnelGuard operation



Source: Nortel Network documentation
http://www.nortelnetworks.com/promotions/2003b/apac/sync/collateral/contivty48features_pss5.pdf (January 14, 2004)

© SANS Institute 2004 As part of GIAC practical repository Author retains full rights

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Assignment 2 – Create an Audit Checklist

Introduction

The Risk Assessment process from Assignment 1was used to create Table 5. The Audit checklist contains audit tasks that can be mapped to one or more of the vulnerabilities references in Table 5.

Each audit task consists of five sections:

Control Objective
Risk
Compliance
Test procedure
Test type

Each test procedure can be either objective or subjective. Objective procedures are binary: either the system passes or fails. Subjective procedures involved a value judgment by the administrator, based on his personal experience and other mitigating factors that may exist.

The audit tasks will be used to ascertain the options available for secure management of the system. A report will be issued addressing the deployments options that follow best practices and how to reach a secure configuration.

The VPN gateway will be called vpn1.acme.com. This is a fictitious name.

To investigate the state of the systems, commands will be run on a variety of platforms, including the console of the VPN gateway. These commands will be formatted with Times New Roman font, bold type. The responses will be in Times New Roman font, regular type.

Examples:

Command: **show version**

Response: Software Version: V04_80.124

© SANS Institute 2004 As part of GIAC practical repository Author retains full rights

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Audit Task 1 - Test network services available via the public interface

Control Objective: Validate that no administrative services are available on the Internet-facing network interface

Risk: V6, V7, V9. The VPN gateway has well defined private and public interfaces. Exposing any services on the public interface except the IPSec service could lead to denial of service and compromise of the system

Compliance: Binary compliance. Nmap will be use to scan the external interface on all TCP and UDP ports.

Test procedure: Launch the scan from a machine that has Internet connectivity. Use the IP address assigned to the public interface of the VPN gateway. Log the results to a file, based on the type of scan performed.

1. Test all TCP ports with SYN Stealth method:

   nmap –v –sS –sV –P0 –p 1-65535 –oG external-scan-tcp.txt vpn1.acme.com

2. Test all UDP ports:

   nmap –v –sU -sV –P0 –p 1-65535 –oG external-scan-udp.txt vpn1.acme.com

Test Type: Objective, Stimulus Response

Audit Task 2 – Test network services available via the private interface

Control objective: Validate that only the required administrative services are available via the private interface. Only HTTPS should be enabled.

Risk: V6, V7, V9. The private interface is used for all routine management of the VPN gateway. In addition, this interface is used to communicate with the external supporting services like DNS, IP services and Authentication services. Unnecessary services could lead to remote compromise or denial of service.

Compliance: Binary compliance. Nmap will be used to scan the internal interface on all TCP and UDP ports.

Test procedure: Launch an nmap scan from a machine that has connectivity to the private interface of the VPN gateway. Log the results to a file, based on the type of scan performed.

© SANS Institute 2004 As part of GIAC practical repository Author retains full rights

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

3. Test all TCP ports with SYN Stealth method:

   nmap –v –sS –sV –P0 –p 1-65535 –oG internal-scan-tcp.txt vpn1-internal.acme.com

4. Test all UDP ports:
   nmap –v –sU –P0 –p 1-65535 –oG internal-scan-udp.txt vpn1-internal.acme.com

Test type: Objective, Stimulus response

Audit Task 3 – Configuration of local and remote logging

Control objective: Confirm that local logging is configured and that there are remote syslog servers defined.

Risk: V1, V4, V8. Remote logs are needed in case the local logs are either compromised or erased. Local logs are more extensive than remote logs and are needed to assist in debugging and troubleshooting.

Compliance: Binary compliance. Local logging is configured and active, remote logging is configured and entries exist in the remote logs.

Test procedure:

To verify local logging: at the VPN gateway console, in admin mode, issue the commands:

show logging syslog
show event-log-size
show data-collection-interval
show compress-files
show log-file-lifetime

To verify remote logging: at the VPN gateway console, in enable mode, run:

CES#config t
CES(config)# show syslog-host

At the remote log server, verify the configuration of /etc/syslog.conf. Verify the existence of the files defined in /etc/syslog.conf.

Test type: Objective, Stimulus response

© SANS Institute 2004 As part of GIAC practical repository Author retains full rights

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Audit Task 4 – Auto Backup is configured and working

Control Objective: Verify that the system and configuration files are saved on a set schedule to an external server. Optionally, verify that the log files are saved following a schedule.

Risk: V1. Failure to auto backup the configuration files could be an indicator of a system malfunction.

Compliance: Variable compliance. There are 4 possible definitions for auto backup schedules. At least one needs to be set up.

Test procedure:

At the VPN console, in enable mode, run:

CES#config t
CES(config)# show exception backup

At the remote ftp server, verify that the server is configured to accept the connection from the VPN gateway and that the backup files exists.

Test type: Objective, Stimulus response

Audit Task 5 – Time synchronization

Control Objective: Ensure that NTP (Network Time Protocol) servers are configured and working properly.

Risk: V1. Clock drift, if left unattended, could affect severely the accuracy of system logs as well as the IPSec policies that are time-specific, if they are being used.

Compliance: Binary compliance. The gateway clock can be queried for the needed information. Log files can be used to confirm ntp updates.

Test procedure:

At the VPN gateway console type the commands:

show clock details
show ntp associations

Test Type: Objective

© SANS Institute 2004 As part of GIAC practical repository Author retains full rights

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Audit Task 6 – Unnecessary services

Control Objective: Determine which services are running on the private and public interfaces of the VPN gateway. The only management protocol that is allowed is HTTPS (secure http) on the private interface.

Risk: V6, V7. Clear text management protocols like telnet and ftp could lead to the disclosure of sensitive information, in this case the settings of the VPN gateway and the administrator's credentials.

Compliance: Binary compliance. Either only HTTPS is enabled or more services are enabled.

Test procedure:

On the VPN gateway console issue the following command:

show services management

Test Type: Objective

Audit Task 7 – TunnelGuard Policy Enforcement

Control Objective: TunnelGuard policies must detect changes in the agent environment and take appropriate action, as defined in the policy.

Risk: V5. TunnelGuard is used to extend the reach of the network perimeter to the client machine. If the policy is not enforced, a breach of the network perimeter has occurred. The client machine could be used to send malicious traffic to the internal network.

Compliance: Binary Compliance. The TunnelGuard service must detect a change of the agent state.

Test Procedure: On the VPN gateway, define a TunnelGuard Policy. Use a client machine with the TunnelGuard agent loaded; connect to the VPN gateway. After a successful connection, unload from the client machine one of the programs that the TunnelGuard policy is monitoring. Review the client logs and the VPN gateway logs for evidence that the TunnelGuard policy for Policy Failure was followed.

Test Type: Objective, Stimulus Response

© SANS Institute 2004 As part of GIAC practical repository Author retains full rights

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Audit Task 8 – Test External Client DHCP service

Control Objective: Confirm proper configuration and operation of DHCP Relay service

Risk: V3. Without an external DHCP server, VPN clients will not be able to join the network.

Compliance: Binary compliance. The DHCP proxy feature should be configured. Options are to configure the local IP address pools in the gateway.

Test Procedure: On the VPN gateway console, type the command:

show ip dhcp proxy-server

Test Type: Objective

Audit Task 9 - Configuration of SNMP Traps

Control Objective: Confirm that SNMP Traps are configured to relay hardware and service status and failures.

Risk: V1, V3, V8. Detection of service degradation, service failure and service state change is critical.

Compliance: Variable compliance. There are many traps available, not all may be configured.

Test Procedure: On the VPN gateway console, issue the following commands:

show snmp-traps trap-host
show snmp-traps trap-group hardware
show snmp-traps trap-group service
show snmp-traps trap-group server
show snmp-traps trap-group ietf
show snmp-traps trap-group attack

Test type: Objective

© SANS Institute 2004 As part of GIAC practical repository Author retains full rights

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Audit Task 10 –External User Authentication Service

Control Objective: Confirm that RADIUS, the chosen external user authentication service, has been enabled and configured. Confirm that the communication with the RADIUS server is operational.

Risk: V3. The only method of authentication for external VPN users is RADIUS. A failure to define, test and monitor the communication with this service could lead to a denial of service.

Compliance: Variable compliance. Several RADIUS servers are available.

Test procedure: On the VPN gateway console, issue the command:

show radius-server group "/Base" all

Test type: Ojective, Stimulus Response

Audit Task 11 – SANS Top 20 – OpenSSL implementation is vulnerable

Control Objective: Verify that the gateway operating system is using the latest version of the OpenSSL libraries.

Risk: V9. Vulnerable versions of the OpenSSL libraries could lead to remote compromises and remote denial of service.

Compliance: Binary compliance. Testing will show a threat of a remote exploit or the lack thereof.

Test procedure: Launch Lightning, a nessus front-end. Configure it with Web policy, including DOS plugins. Lightning is available from Tenable Security (http://www.tenablesecurity.com). The version of nessus used is 2.0.9, with the latest plugins available at the time of the testing.

Test type: Objective

© SANS Institute 2004 As part of GIAC practical repository Author retains full rights

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Assignment 3 – Audit Evidence

Results of the Audit

The audit was conducted at several times in December 2003 and January 2004. The version of server software (VPN gateway code) is 4_80.124. Even though an update was release during testing, the server was not upgraded.

Tests were performed mainly from a local network. Tests were performed from an external network only when the 'public' (Internet-facing) interface was involved.

As mentioned before, the tests outlined in Assignment 2 were considered the most relevant to the operation and management of the server and the TunnelGuard feature set. Additional testing was conducted in regards to other sections of the Audit (Environmental and Physical controls) but they are not included.

Audit Task 1 PASS

Test network services available via the public interface

The public interface of the VPN gateway was scanned from an Internet based scanner. All ports, both TCP and UDP, were found closed.

nmap –v –sS –sV –P0 –p 1-65535 –oG external-scan-tcp.txt vpn1.acme.com

nmap 3.00 scan initiated Fri Jan 16 15:27:13 2004 as: nmap -v -sS -sV –P0 –p 1-65535 -oG external-scan-tcp.txt 1vpn1.acme.com
All 65535 scanned ports on vpn1.acme.com (x.y.z.2) are: filtered

Nmap run completed at Fri Jan 16 15:30:21 2004 -- 1 IP address (1 host up) scanned in 1888.385 seconds

nmap –v –sU –sV –P0 –p 1-65535 –oG external-scan-udp.txt vpn1.acme.com

nmap 3.00 scan initiated Sat Jan 17 12:00:13 2004 as: nmap -v -sU -sV –P0 –p 1-65535 -oG external-scan-udp.txt 1vpn1.acme.com
All 65535 scanned ports on vpn1.acme.com (x.y.z.2) are: filtered

Nmap run completed at Sat Jan 17 15:20:21 2004 -- 1 IP address (1 host up) scanned in 12008 seconds

These results meet the expectation. The public interface should be configured to only accept IPSec connections from clients. This audit task passes.

© SANS Institute 2004 As part of GIAC practical repository Author retains full rights

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Audit Task 2 FAIL Finding 1

Test network services available via the private interface

An nmap scan as root was launched from a host in the local network, adjacent to the VPN gateway. The results are:

#nmap -v -sS -sV –P0 –p1-65535 –oG internal-scan-tcp.txt vpn1-internal.acme.com

```
Starting nmap 3.50 ( http://www.insecure.org/nmap/ ) at 2004-01-29 18:07 EST
Host vpn1-internal.acme.com(10.13.145.1) appears to be up ... good.
Initiating SYN Stealth Scan against vpn1-internal (10.13.145.1) at 18:07
Adding open port 23/tcp
Adding open port 80/tcp
Adding open port 443/tcp
The SYN Stealth Scan took 209 seconds to scan 65535 ports.
Initiating service scan against 3 services on 1 host at 18:11
The service scan took 72 seconds to scan 3 services on 1 host.
Interesting ports on vpn1-internal (10.13.145.1):
(The 65530 ports scanned but not shown below are in state: filtered)
PORT    STATE  SERVICE VERSION
22/tcp  closed ssh
23/tcp  open   telnet?
53/tcp  closed domain
80/tcp  open   http?
443/tcp open   https?

Nmap run completed -- 1 IP address (1 host up) scanned in 281.220 seconds
```

#nmap -v -sU -sV –P0 –p1-65535 –oG internal-scan-udp.txt vpn1-internal.acme.com

```
Starting nmap 3.50 ( http://www.insecure.org/nmap/ ) at 2004-01-29 19:01 EST
Host vpn1-internal.acme.com(10.13.145.1) appears to be up ... good.
Initiating UDP Scan against vpn1-internal (10.13.145.1) at 19:01

The UDP Scan took 5009 seconds to scan 65535 ports.
 (The 65535 ports scanned but not shown below are in state: open)

Nmap run completed -- 1 IP address (1 host up) scanned in 5009.241 seconds
```

Although all UDP ports show as open, there is no service answering on any of the ports.

This audit task fails because the only service that should have been open is

© SANS Institute 2004 As part of GIAC practical repository Author retains full rights

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

https. Notice that nmap was not able to gather the version of any of the open services. The version was requested using the switch '-sV'. Nmap has an extensive database of service fingerprints. This scan was conducted with the latest service fingerprint database available at the time.

Audit Task 3 PASS

Configuration of local and remote logging

The following commands were issued on the VPN gateway, in enable mode:

Local logging

CES#show logging history
Logging history level is ALL

CES#show event-log-size
Event Log Size: 2000 entries

CES#show data-collection-interval
Data Collection interval: 2 minutes

CES#show compress-files
File Compression: enabled

CES#show log-file-lifetime
Log File Lifetime: 60 days

Remote logging, gateway configuration

Switch to config mode

CES#config t
Enter configuration commands, one per line. End with Ctrl/z.

CES(config)#show syslog-host

Status	Host	Level	Filter-Facility	Tagged-Facility	Port
Enabled	10.13.145.79	ALL	ALL	LOCAL2	514
Enabled	10.13.145.79	ALL	TUNNELGUARD	LOCAL3	514
Disabled		NORMAL	ALL	KERN	514
Disabled		NORMAL	ALL	KERN	514

Remote logging, remote location

© SANS Institute 2004 As part of GIAC practical repository Author retains full rights

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Verify the configuration of the remote syslog server. Review the entries for LOCAL2 and LOCAL3 in the /etc/syslog.conf file.

As root in the remote syslog server, the following command was entered:

 # grep local /etc/syslog.conf
…….
local2.err /array/4/vpn1-test-local2
local3.err /array/4/vpn1-test-local3
……..

tigereye:/array/4#ls -lst *local*
1376 -rw-r--r-- 1 root other 689264 Feb 29 18:41 vpn1-test-local2
4176 -rw-r--r-- 1 root other 2126785 Feb 29 18:34 vpn1-test-local3

tigereye:/array/4#head vpn1-test-local2
Feb 27 16:36:41 vpn1 24461 02/27/2004 16:36:39 tcli0 0 : DbSysLog.WriteToFile changed from 'TRUE' to 'TRUE' by user 'admin' @ '10.13.145.79'

tigereye:/array/4#head vpn1-test-local3
Jan 7 10:26:51 vpn1 24461 01/07/2004 10:26:35 tEvtLgMgr 0 : TUNNELGUARDd [13] Agent 63.146.13.107: Bringing down tunnel, re-authentication FAILED - SRS - Test Client Definition

The steps taken at the gateway and the remote syslog server show that logs were being kept locally as well as remotely. Log retention locally was set for 60 days, the maximum available. In addition, data collection is being done locally every 2 minutes. This setting means that every 2 minutes data is written to a file from memory buffers.
There are 4 entries for syslog servers. Only one server was being used with two different Filter facilities and different remote syslog facilities.This audit task passes.

Audit Task 4 PASS

Auto Backup is configured and working

Local configuration

Switch to configuration mode

CES#config t
Enter configuration commands, one per line. End with Ctrl/z.

© SANS Institute 2004 As part of GIAC practical repository Author retains full rights

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
CES(config)#show exception backup
 Backup FTP Server 1
  Server Address :  10.13.145.79
  Server Enabled :  ENABLED
  Backup Filepath:  ces/vpn1-backup
  Server Username:  tunnel
  Server Status  :  Success
  Specific Time  :  02:36
  Backup Type    :  Partial (Configuration Files, Log Files)
  Backup Days    :  Su Mo Tu We Th Fr Sa

 Backup FTP Server 2
  Server Address :  10.13.145.79
  Server Enabled :  ENABLED
  Backup Filepath:  ces/vpn1-backup-sys
  Server Username:  tunnel
  Server Status  :  Success
  Specific Time  :  03:36
  Backup Type    :  Partial (System Files)
  Backup Days    :  Su Mo Tu We Th Fr Sa

 Backup FTP Server 3
  Server Status  :  Not Configured
  Backup Interval:  5
  Server Username:
  Backup Type    :  Full
  Backup Days    :  Su Mo Tu We Th Fr Sa
```

Remote configuration

At the backup server, issue the commands:

```
tigereye$pwd
/export/home/tunnel/ces

tigereye$ls -lst *backup*
vpn1-backup:
total 2
   2 drwxr-xr-x  15 tunnel   other       512 Aug  7  2003 sn24461

vpn1-backup-sys:
total 2
   2 drwxr-xr-x  11 tunnel   other       512 Jul 10  2003 sn24461

tigereye$pwd
```


© SANS Institute 2004 As part of GIAC practical repository Author retains full rights

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

/export/home/tunnel/ces/vpn1-backup/sn24461

tigereye$ls -lst

```
total 352
   4 drwxr-xr-x   2 tunnel   other       1536 Feb 29 02:36 LOG
   4 drwxr-xr-x   2 tunnel   other       1536 Feb 29 02:36 DCLOG
   2 drwxr-xr-x   2 tunnel   other       1024 Feb 28 02:36 CONFIG
   2 drwxr-xr-x   2 tunnel   other        512 Feb 28 02:36 ACCTLOG
   2 -rw-r--r--   1 tunnel   other         12 Feb 15 02:38 version.dat
  16 -rw-r--r--   1 tunnel   other       8025 Feb 15 02:37 fwscope.dat
 134 -rw-r--r--   1 tunnel   other      67736 Feb 15 02:37 filelist.dat
 168 -rw-r--r--   1 tunnel   other      85536 Feb 15 02:37 desmac.dat
   2 -rw-r--r--   1 tunnel   other         38 Feb 15 02:36 boot.dat
   2 drwxr-xr-x   4 tunnel   other        512 Aug  7  2003 CERT
   2 drwxr-xr-x   3 tunnel   other        512 Aug  2  2003 KEYS
   2 drwxr-xr-x   2 tunnel   other        512 Jul 10  2003 RADACCT
   2 drwxr-xr-x   7 tunnel   other        512 Jul  7  2003 SLAPD
   2 drwxr-xr-x   5 tunnel   other        512 Jul  7  2003 PYTHON
   2 drwxr-xr-x   3 tunnel   other        512 Jul  7  2003 PKIX
   2 drwxr-xr-x   3 tunnel   other        512 Jul  7  2003 LDAP
   2 drwxr-xr-x   6 tunnel   other        512 Jul  7  2003 FW
   2 drwxr-xr-x   2 tunnel   other        512 Jul  7  2003 DHCP
```

tigereye$pwd

/export/home/tunnel/ces/vpn1-backup-sys/sn24461

tigeyere$ls -lst

```
total 358
   2 -rw-r--r--   1 tunnel   other         12 Feb 15 03:42 version.dat
  16 -rw-r--r--   1 tunnel   other       8025 Feb 15 03:36 fwscope.dat
 168 -rw-r--r--   1 tunnel   other      85536 Feb 15 03:36 desmac.dat
 134 -rw-r--r--   1 tunnel   other      67736 Feb 15 03:36 filelist.dat
   2 -rw-r--r--   1 tunnel   other         38 Feb 15 03:36 boot.dat
  20 drwxr-xr-x   9 tunnel   other       9728 Aug 11  2003 MANAGE
   2 drwxr-xr-x   2 tunnel   other        512 Jul 10  2003 SCRIPT
   2 drwxr-xr-x   7 tunnel   other        512 Jul 10  2003 SAFE
   2 drwxr-xr-x   5 tunnel   other        512 Jul 10  2003 PERL
   2 drwxr-xr-x   2 tunnel   other        512 Jul 10  2003 PROV
   2 drwxr-xr-x   2 tunnel   other        512 Jul 10  2003 LMM
   2 drwxr-xr-x   3 tunnel   other        512 Jul 10  2003 FLOPPY
   2 drwxr-xr-x   2 tunnel   other        512 Jul 10  2003 COMMAND
   2 drwxr-xr-x   2 tunnel   other        512 Jul 10  2003 BIN
```

The gateway is configured to backup its configuration and log files daily at 02:36 AM. The system files are backed up daily at 03:36 AM. Some files have not

© SANS Institute 2004 As part of GIAC practical repository Author retains full rights

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

changed since the system was loaded; others change regularly. The backup is done over ftp. The audit task passes.

Audit Task 5 PASS

Time synchronization

At the VPN gateway console, in enable mode, run:

CES#show clock detail
19:25:29 EST Thu Jan 29 2004
Time source is NTP

CES#show ntp associations
NTP Servers: (* active server)

```
    remote          local       st poll reach  delay   offset    disp

==================================================================
   192.5.41.209     5.0.0.0    16 64   0      0.00000 0.000000  0.00000
   192.5.41.41      5.0.0.0    16 64   0      0.00000 0.000000  0.00000
```

There are several ways to configure NTP on the gateway, including the use of NTP version 4. This audit task passes.

Audit Step 6 FAIL Finding 1

Unnecessary services

CES#show services management

Management Protocol	Public	Private
HTTP	NONE	TRUE
HTTPS	FALSE	TRUE
SNMP	NONE	FALSE
FTP	NONE	FALSE
TELNET	NONE	TRUE
Identification	NONE	FALSE
CRL Retrieval	FALSE	FALSE
CMP	FALSE	FALSE
Radius Accounting	FALSE	TRUE

© SANS Institute 2004 As part of GIAC practical repository Author retains full rights

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Certification Modes

FIPS DISABLED

There are three possible scenarios: None, False and True. None means that it cannot be enabled. The clear text management services are not available via the public interface. The other available services are not enabled via the public interface. On the private interface, the management services that are available are telnet, http and https. Radius accounting is not a management service and it is not available as a daemon. It is only enabled in order to send data to a RADIUS accounting server internally.

Notice that there is a FIPS certification mode available. This VPN gateway has been certified to comply with FIPS 140-1 Level 2 (http://csrc.nist.gov/cryptval/140-1sp/140sp179.pdf (January 14, 2004)). This certification, from the management perspective, means disabling ftp, telnet and http. Http can be disabled without a problem since https is available. The only alternative to the telnet service for CLI access from the internal network is to connect to the VPN gateway via a serial console, or use a trusted internal host as a 'jumpstation'.

This audit task fails.

Audit Task 7 PASS

TunnelGuard Policy Enforcement

This task is quite involved, as it requires preparation on the VPN gateway of a TunnelGuard policy, launching a client VPN session to connect to the gateway, successfully pass the requirements of the TunnelGuard policy, then execute a command in the client that will break the settings being enforced by the TunnelGuard agent, according to the policy that the gateway delivered.

Step 1: Build a TunnelGuard ruleset. Exact steps are outlined in a Nortel document, titled " A TunnelGuard Companion", document number TT030502, available from http://www.nortelnetworks.com.
The image below shows the Software Requirement Set (SRS) BI & NAV.
This definition monitors only two binaries:

NAV Norton Antivirus, version 7.61
BI BlackIce, version 7.0

© SANS Institute 2004 As part of GIAC practical repository Author retains full rights

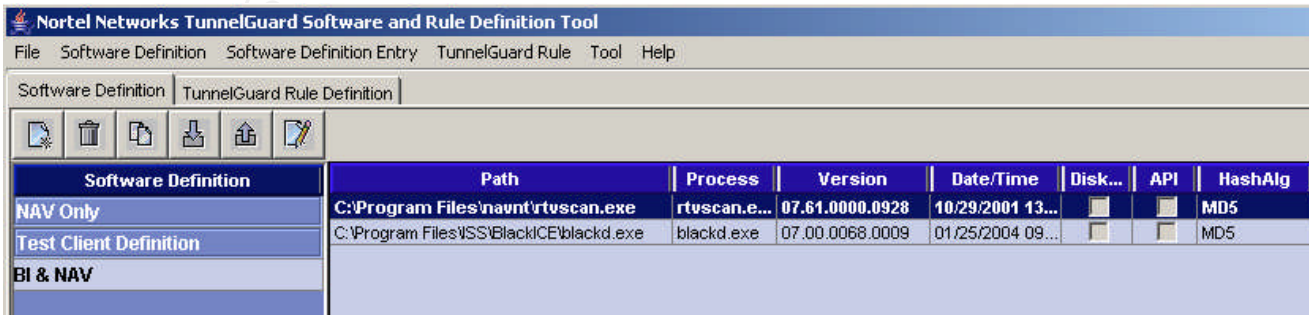
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

All aspects of the binary are monitored, including its MD5 hash. This MD5 hash is created at the time the administrator creates the SRS.
The file listing below is the SRS exported in xml format.


```
<?xml version="1.0" encoding="UTF-8"?>
<srs SRSName="BI &amp; NAV" SRSOS="WIN_ALL" SRSComment="">
<srsEntry EntryPath="C:\Program Files\navnt\rtvscan.exe"
EntryMaxVersion="07.61.0000.0928" EntryMinVersion="07.61.0000.0928"
EntryProcessName="rtvscan.exe" EntryHashType="MD5"
EntryHashValue="E653817964F17595C666B376E360B54D"
EntryOnDiskOnly="False" EntryAPICall="False" EntryIgnorePath="False"
EntryMaxDateTime="2001/10/29 13:38:50" EntryMinDateTime="2001/10/29
13:38:50"/>
<srsEntry EntryPath="C:\Program Files\ISS\BlackICE\blackd.exe"
EntryMaxVersion="07.00.0068.0009" EntryMinVersion="07.00.0068.0009"
EntryProcessName="blackd.exe" EntryHashType="MD5"
EntryHashValue="AD7CE31F74121F3940484885B03D7EF4"
EntryOnDiskOnly="False" EntryAPICall="False" EntryIgnorePath="False"
EntryMaxDateTime="2004/01/25 09:33:58" EntryMinDateTime="2004/01/25
09:33:58"/>
</srs>
```


If any of the binaries is not loaded in memory when the tunnel is initially created OR if either one of the binaries is unloaded after the tunnel as been set up, the tunnel will be torn down.

SRS DEFINITION



© SANS Institute 2004 As part of GIAC practical repository Author retains full rights

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

TUNNELGUARD DEFINITION

Step 2: Apply the TunnelGuard ruleset

Contivity allows for the creation of multiple user groups. Each group can be configured to enforce a single TunnelGuard ruleset. Each ruleset can be composed of several SRS definitions.

TunnelGuard Policy/ Ruleset, as applied to Test group

TunnelGuard	Enabled
TunnelGuard: Restricted Filter	deny all
TunnelGuard: Policy	BI & NAV
TunnelGuard: Periodic Check Interval (mins)	15
TunnelGuard: Agent Query Timeout Interval (sec)	2
TunnelGuard: Initial Policy Failure Action	Teardown Tunnel

Step 3: Use a client with the TunnelGuard Agent loaded to connect to the VPN gateway. Unload one of the TunnelGuard policy elements and review the results.

The results of the connection/unload/disconnection, as shown in the client TunnelGuard log.

```
2004-01-28 17:04:47,303  INFO [] - Properties:
2004-01-28 17:04:47,313  INFO [] -    dumpProperties          = true
2004-01-28 17:04:47,323  INFO [] -    dumpSessionList          = true
2004-01-28 17:04:47,323  INFO [] -    logAgedSessionDelete      = true
2004-01-28 17:04:47,323  INFO [] -    logCheckResultAlways      = true
2004-01-28 17:04:47,323  INFO [] -    logIntraIntervalCheckResult= false
2004-01-28 17:04:47,323  INFO [] -    logNetworkIoBytes         = false
```


© SANS Institute 2004 As part of GIAC practical repository Author retains full rights

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

2004-01-28 17:04:47,323 INFO [] - logSessionHistoryIntervals = 0
2004-01-28 17:04:47,323 INFO [] - logSRSBundleUpdate = true
2004-01-28 17:04:47,323 INFO [] - logTunnelUpDown = true
2004-01-28 17:04:47,323 INFO [] - numChecksPerInterval = 4
2004-01-28 17:04:47,323 INFO [] - rollLogFileOnStartup = true
2004-01-28 17:04:47,333 INFO [] - ErrorInfoNumber = 10
2004-01-28 17:04:47,333 INFO [] - End Properties.
2004-01-28 17:05:00,261 INFO [] - Agent started at Wed Jan 25 17:04:59 MST 2004 listening on port 8121
2004-01-29 13:54:33,744 INFO [] - TunnelStatus is up
2004-01-29 13:54:33,764 INFO [] - already listening on port 8282
2004-01-29 13:54:33,854 INFO [10.13.145.1] - Sessions:
2004-01-29 13:54:33,854 INFO [10.13.145.1] - Session:
2004-01-29 13:54:33,854 INFO [10.13.145.1] - session address : 10.13.145.1
2004-01-29 13:54:33,854 INFO [10.13.145.1] - creation time : Thu Jan 29 13:54:33 MST 2004
2004-01-29 13:54:33,864 INFO [10.13.145.1] - pending delete : false
2004-01-29 13:54:33,864 INFO [10.13.145.1] - client username : none
2004-01-29 13:54:33,864 INFO [10.13.145.1] - client IP addr : none
2004-01-29 13:54:33,864 INFO [10.13.145.1] - server IP addr : none
2004-01-29 13:54:33,864 INFO [10.13.145.1] - End list of sessions.
2004-01-29 13:54:36,017 INFO [10.6.225.63] - SRS bundle saved for this session
2004-01-29 13:54:37,669 INFO [10.6.225.63] - checkStatus response = STATUS_FAIL
2004-01-29 13:54:37,669 INFO [10.6.225.63] - checkStatus reason =
SRS - BI & NAV

SRSEntry - C:\Program Files\Network ICE\BlackICE\blackd.exe
C:\Program Files\Network ICE\BlackICE\blackd.exe not found in snapshot for process blackd.exe
SRSEntry - C:\Program Files\NavNT\rtvscan.exe

2004-01-29 13:58:37,980 INFO [] - Current time reported from the CES is: Thu Jan 29 13:58:53 MST 2004
2004-01-29 13:58:37,980 INFO [] - Session list entry removed for 10.13.145.1
2004-01-29 13:58:37,980 INFO [] - Sessions:
2004-01-29 13:58:37,980 INFO [] - End list of sessions.
2004-01-29 13:58:38,010 INFO [] - TunnelStatus is down

From the eventlog in the VPN gateway side, we have confirmation that the client session went down because it failed to meet the requirements.

The VPN gateway is in Central Standard Time. The TunnelGuard policy is being checked every 15 minutes.

© SANS Institute 2004 As part of GIAC practical repository Author retains full rights

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

CES#show logging events key-word trlab02

…….

01/29/2004 12:20:03 0 Security [11] Session: IPSEC[trlab02] attempting login
01/29/2004 12:20:03 0 Security [11] Session: IPSEC[trlab02] logged into group /Base/Test
01/29/2004 12:20:03 0 Security [01] Session: IPSEC[trlab02]:71 attempting auth entication using RADIUS
01/29/2004 12:20:03 0 Security [11] RADIUS: "trlab02" access OK by server "10.0.1.1".
01/29/2004 12:20:03 0 Security [11] Session: IPSEC[trlab02]:71 authenticated using RADIUS
01/29/2004 12:20:03 0 Security [01] Session: IPSEC[trlab02]:71 trlab02 has no active accounts
01/29/2004 12:20:03 0 Security [11] Session: IPSEC[trlab02]:71 bound to group /Base/Test
01/29/2004 12:20:03 0 Security [01] Session: IPSEC[trlab02]:71 Incoming client version (V04_65), minimum version (V04_65) push action (Filter Traffic), action not needed
01/29/2004 12:20:03 0 Security [01] Session: IPSEC[trlab02]:71 Building group filter permit all
01/29/2004 12:20:03 0 Security [01] Session: IPSEC[trlab02]:71 Building tunnel guard restricted filter deny all
01/29/2004 12:20:03 0 Security [01] Session: IPSEC[trlab02]:71 Applying tunnel guard restricted filter
01/29/2004 12:20:03 0 Security [11] Session: IPSEC[trlab02]:71 authorized
01/29/2004 12:20:03 0 Security [12] Session: IPSEC[trlab02]:71 physical addresses: remote 10.1.190.92 local 10.10.50.1
01/29/2004 12:20:03 0 Security [12] Session: IPSEC[trlab02]:71 assigned IP add ress 10.6.225.63, mask 0.0.0.0
01/29/2004 12:20:03 0 Security [12] Session: IPSEC[trlab02]:71 physical addresses: remote 10.1.190.92 local 10.10.50.1
01/29/2004 12:20:04 0 Security [12] Session: IPSEC[trlab02]:71 physical addresses: remote 10.1.190.92 local 10.10.50.1
01/29/2004 12:20:48 0 Security [01] Session: IPSEC[trlab02]:71 Restricted filter no longer required. Restoring initial filter permit all
01/29/2004 12:36:40 0 TUNNELGUARDd [00] Periodic check required for Tunnelguard user [trlab02] from IP[10.6.225.63].
01/29/2004 12:51:40 0 TUNNELGUARDd [00] Periodic check required for Tunnelguard user [trlab02] from IP[10.6.225.63].
01/29/2004 12:52:22 0 TUNNELGUARDd [00] Agent 10.6.225.63: Removed user trlab02 from user list
01/29/2004 12:52:22 0 TUNNELGUARDd [00] Resources for user trlab02 freed.

© SANS Institute 2004 As part of GIAC practical repository Author retains full rights

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The agent/server communications over the VPN tunnel allowed the server to check the status of the policy at the set interval. During this check, it was found that the client did not meet the policy. Immediate action was taken to tear down the tunnel. This audit task passes.

Audit Task 8 PASS

Test External Client DHCP Service

On the VPN gateway, in enabled mode, issue the command:

CES#show ip dhcp proxy-server

```
DHCP Proxy Server Configuration
                DHCP server:    Primary    10.13.145.79
                                Secondary  0.0.0.0
                                Tertiary   0.0.0.0
            DHCP Cache size:    5
     Immediate Address Release:    Enabled
       DHCP Blackout Interval:    300
    Override Blackout Interval
when no addresses are available:    Enabled
```

This command shows that an external DHCP server is used to assign IP addresses to clients. An alternative is to use local IP pools, allocated per group. This audit task passes.

Audit Task 9 PASS

Configuration of SNMP Traps

On the VPN gateway, console, in enable mode, issue the following commands:

CES#show snmp-traps trap-host

Host Name or IP Address	Community Name	Enabled	Status
10.13.145.79	vpn1	TRUE	Operational
10.0.60.249	vpn1	TRUE	Operational

© SANS Institute 2004 As part of GIAC practical repository Author retains full rights

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Entry from host 10.0.60.249:

18:11:38 01/19/04 0 10.13.145.1 130315548 1.3.6.1.4.1.2505.1.4 6 101 1.3.6.1.4.1.2505.1.7 Integer 1 1.3.6.1.4.1.2505.1.4.1 String Failed Login Attempt: Username=get / http/1.0: Date/Time=01/19/2004 18:11:24 1.3.6.1.4.1.2505.1.8 String 1.3.6.1.4.1.2505.1.9 String 01/19/2004 1.3.6.1.4.1.2505.1.10 String 18:11:24 1.3.6.1.4.1.2505.1.11 TimeTick 130315548

CES#show snmp-traps trap-groups hardware

Contivity SNMP Hardware Traps

Name	Enabled	Interval	Send One
LAN on Slot 1 Interface 1	Yes	00:03:00	Yes
LAN on System Board	Yes	00:03:00	Yes
Memory Usage	Yes	00:03:00	Yes
Hard Disk 0	Yes	00:03:00	Yes
Intrusion	Yes	00:03:00	Yes
Normal Temperature	Yes	00:03:00	Yes
Voltage 12 V Plus	Yes	00:03:00	No
Voltage 2.5 VA	No	00:03:00	No
Voltage 3.3 V Plus	No	00:03:00	No
Voltage 5 V Plus	No	00:03:00	No
Chassis Fan	No	00:03:00	No
CPU One Fan	No	00:03:00	No
Heart Beat	Yes	00:03:00	Yes

CES#show snmp-traps trap-groups service

Contivity SNMP Service Traps

Name	Enabled	Interval	Send One
VRRP	No	00:03:00	No
FIPS	Yes	00:03:00	Yes
Anti-Spoofing	Yes	00:03:00	Yes
Multicast Relay	No	00:03:00	No
RIP	No	00:03:00	No
IPSec Failover Service	No	00:03:00	No
Tunnelguard	Yes	00:03:00	No
NAT	No	00:03:00	No
Routing Policy Server	No	00:03:00	No
Firewall	Yes	00:03:00	Yes
Client Routes Marshaler	No	00:03:00	No
Temporary Licenses	No	00:03:00	No
Buffer Usage	Yes	00:03:00	Yes

© SANS Institute 2004 As part of GIAC practical repository Author retains full rights

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

CES#show snmp-traps trap-groups server

Contivity SNMP Server Traps

Name	Enabled	Interval	Send One
IP Address Pool	Yes	00:03:00	Yes
CMP	No	00:03:00	Yes
Load Balancing Service	No	00:03:00	Yes
OSPF	No	00:03:00	No
Global Backup Interface Services	No	00:03:00	No
DHCP Server	Yes	00:03:00	Yes
DhcpRelay	Yes	00:03:00	Yes
Certificates Validity	No	00:03:00	Yes
Auto Backup Servers	Yes	00:03:00	Yes
Internal LDAP Server	Yes	00:03:00	Yes
RADIUS Authentication Servers	Yes	00:03:00	Yes
RADIUS Accounting Server	Yes	00:03:00	Yes
Network Time Protocol	Yes	00:03:00	Yes
External LDAP Servers	No	00:03:00	Yes
CLIP	No	00:03:00	No
SNMP Servers	No	00:03:00	Yes
LDAP Proxy Servers	No	00:03:00	No
DNS Servers	Yes	00:03:00	Yes

CES#show snmp-traps trap-groups ietf

Contivity SNMP Standard IETF Traps

Name	Enabled
SNMP Authentication	Yes
VRRP	No
OSPF	No
DSU/CSU	No

Link Up/Down

Name	Enabled
Physical Interfaces	Yes
BranchOffice Nailed-Up Tunnel	No
BranchOffice OnDemand Tunnel	No

© SANS Institute 2004 As part of GIAC practical repository Author retains full rights

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

CES#show snmp-traps trap-group attack

```
Contivity SNMP Attack Traps
  Name                          Enabled
  ------------------------------  -------
  Failed Login                    Yes
  Firewall                        Yes
  Security Intrusion              Yes
```

The test results show that extensive SNMP traps are available. These traps should be configured in accordance with the corporate policies. This audit task passes.

Audit Task 10 PASS

External User Authentication Service

On the VPN gateway, console, in enable mode, issue the following commands:

CES#show radius-server group "/Base/Test" all

```
  Group Level Radius Attributes:
    Remove suffix from User ID : FALSE
    Domain Delimiter : @
    Error Code Pass Thru : TRUE
    Response Timeout Interval : 3
    Maximum Transmit Attempts : 3
  Group Radius Server Configuration:
    Primary Radius Server:
      RadiusServer : Enabled
      Hostname or IP address : 10.13.145.80
      Interface : Private
      Status : Configured
      Port : 1645
    Alternate1 Radius Server:
      RadiusServer : Enabled
      Hostname or IP address : 10.0.0.71
      Interface : Private
      Status : Configured
      Port : 1645
    Alternate2 Radius Server:
      RadiusServer : Enabled
      Hostname or IP address : 10.0.0.72
```


© SANS Institute 2004 As part of GIAC practical repository Author retains full rights

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Interface : Private
Status : Configured
Port : 1645

The results of this test show that 3 RADIUS servers are configured for authentication of users that belong to the Test group. There are other options for authentication like LDAP, but this group is configured to only use RADIUS. When the command is issued, a test request is sent to the RADIUS servers. The status of Configured is ascertained in real time. This audit task passes.

Audit Task 11 FAIL Finding 2

SANS Top 20- OpenSSL implementation is vulnerable

This test was conducted using Lightning, a front end to the nessus scanner. A policy specific to Web servers was used, including Denial of Service (DOS) plugins. The results were checked for false positives and false negatives. The data below are the confirmed results.

The plugin # 11875 determined that it is possible the web server is vulnerable.

10.13.145.1 443/tcp 4.0.0.25 OpenSSL overflow via invalid certificate passing
Nessus ID: 11875
The remote host seem to be running a version of OpenSSL which is older than 0.9.6k or 0.9.7c. There is a heap corruption bug in this version which might be exploited by an attacker to gain a shell on this host.
Solution : If you are running OpenSSL, Upgrade to version 0.9.6k or 0.9.7c or newer
Risk factor : High

Additional review of the documentation from Nortel confirmed that the version of OpenSSL that shipped in server software 04_80.124 was earlier than 0.9.6k. (BUGID Q00763927). Nortel does not address the impact of the vulnerability, but it is likely it will only lead to a Denial of Service.

http://www142.nortelnetworks.com/bvdoc/contivity/tt/TT030502.pdf (January 14, 2004)

This audit test fails.

© SANS Institute 2004 As part of GIAC practical repository Author retains full rights

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Measurement of Residual Risk

Prior to conducting the audit, documentation provided by the vendor was reviewed to gain insight into the functionality available and the configuration options that could be used to setup the system in a reliable, secure way. After the initial data collection, an interview with the future administrators of the system was done in order to understand their risk posture. The initial risk assessment was done taking into account the service this system will provide and the means available for managing and monitoring the system.

The Audit checklist was designed to cover a range of operational controls that could be taken into account to minimize risks to the system.

There are various audit tasks that failed. Those tasks will be reviewed to understand what steps, if any, are available to further reduce the risks to the system.

As Audit Task 11 (OpenSSL) demonstrates, it is possible to have a configuration that is secure until a new vulnerability is discovered. Although the threat relating to new vulnerabilities is often times difficult to assess, the impact related to the vulnerability is such that immediate action should be taken. Administrators should remain informed about the vulnerabilities that may affect their systems, based in the configuration being used at the time.

Is the System Auditable?

This system can perform a variety of functions. This audit focused on three key aspects: Management Plane, supporting services needed for providing IPSec tunnel termination and TunnelGuard services. As such, the research conducted into the testing procedures and the control objectives was very specific. The system provides clear and concise ways for management and audit. The system, and the key aspects under review, is clearly auditable.

Certain areas related to management, such as administrative-level user accounts, were not audited. This area in particular is of outmost importance, yet no effective controls were found. This concern will be communicated as part of the Risk Assessment.

It is important to put this audit in perspective. Different corporations will have different policies and standards. Some could accept the use of unencrypted management channels, while others have clear policies regarding the use of encrypted management channels. This audit could be used to evaluate quickly and efficiently the options made available by the vendor and how to adapt them to the operational framework of a given installation.

© SANS Institute 2004 As part of GIAC practical repository Author retains full rights

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Assignment 4 - Risk Assessment

Summary

Certain risks were identified before the audit. The audit checklist was developed to ascertain what configuration options were available and could be implemented as mitigating controls to those risks. The vulnerabilities that were specific to the system and that were High or Critical were the target of the audit. Eleven specific items were tested, only 3 items failed. Of those two only one could be easily fixed. The only item that could not be fixed by a configuration change is Audit Task 11, OpenSSL. To stay current with the vulnerabilities related to OpenSSL or the system's operating system, the administrators must take to register with the vendor and receive updates related to the equipment being used as they become available.

Background

The audit produced a rich amount of information. Although most of the Audit Tasks were successful, two of them were not.

Finding 1 (reference: Audit Tasks 2 and 6). The control objective was to only use HTTPS for management of the system. The other tow services found available are HTTP and Telnet. HTTP can be disabled with no loss of access. In regards to telnet, that is the only straightforward method to gain access to the CLI (Command Line Interface), as SSH is not available. There are various options available to continue using only encrypted services for management of the system.

> Option 1: connect the serial console of the VPN gateway to a terminal server or to another computer, then access the terminal server or computer over an SSH session prior to gaining access to the gateway's console. This setup would maintain the end-to-end management over an encrypted session. It will also mean that a system should be physically placed near the gateway to configure the serial connection between the two devices.
>
> Option 2: A variation of Option 1.Instead of using a serial connection, configure a computer with SSH on the same VLAN as the private IP interface of the VPN gateway, ensuring that only these two devices are in that VLAN. This configuration would not maintain the end-to-end encryption. However, the VPN gateway can take advantage of internal firewall rules to limit the use of telnet to the computer that is used as the 'jumpstation'. In addition, this computer could also be used as a backup and syslog server, avoiding the transfer of unencrypted confidential data

© SANS Institute 2004 As part of GIAC practical repository Author retains full rights

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

over the network beyond the local VLAN. More secure methods of transferring the data can be implemented at that time.

Finding 2 (reference: Audit Task 11). The server operating system for the Contivity VPN gateway is based on VxWorks. The only way to upgrade the operating system is by moving to a new release, sometimes called 'sustaining release'. This release of software by Nortel will attempt to address the needs of the users and also to remediate bugs and issues that may have been found since the earlier releases. Before conducting any upgrade to a newer version of monolithic code as the one for the VPN gateway, proper testing is required to ensure that no features that previously worked would be affected by the new release.

The latest production release that addresses the OpenSSL vulnerability is 04_85.120, as documented in http://www142.nortelnetworks.com/bvdoc/contivity/doc_pdf/315000E02.pdf (page 33) (January 14, 2004)

This release also addresses other important issues, like the ability to now specify a minimum TunnelGuard agent version and the move of TunnelGuard log entries from the Event log to the System log. The System log can be forwarded via syslog, while the Event log is only kept locally.

To address the findings of the audit, some configuration changes were made. An upgrade to version 04_85.120 is being tested at this time. Firewall controls were put in place to limit the IP addresses of machines that could connect to the HTTPS service as a mitigating control.

Audit Task 6 PASS

Unnecessary services

The telnet and http services were shutdown down by issuing the following commands:

CES(config)#no telnet enable
CES(config)#no http enable
CES(config)#exit

These settings were verified following the same procedure as in Task 6.

© SANS Institute 2004 As part of GIAC practical repository Author retains full rights

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

CES#show services management

```
Management Protocol    Public    Private
----------------------------------------
HTTP                   NONE      FALSE
HTTPS                  FALSE      TRUE
SNMP                   NONE      FALSE
FTP                    NONE      FALSE
TELNET                 NONE      FALSE
Identification         NONE      FALSE
CRL Retrieval          FALSE      FALSE
CMP                    FALSE      FALSE
Radius Accounting      FALSE      TRUE

Certification Modes
------------------------
FIPS          ENABLED
```

As the administrators choose between Option 1or 2 for CLI access, changes to the management services may be needed.

Audit Recommendations

This audit uncovered a variety of settings that could be implemented to provide the means for remotely detection malfunctions, configuration changes and other anomalies. Enabling all these settings would create a large amount of data that needs to be handled properly. The VPN gateway, as a critical component that provides secure remote access to employees, needs to be integrated within a management framework that is capable of dealing with the various alerts the system can generate. Especial care should be given to TunnelGuard alerts, as they could elicit malicious activity taking place in the user's machine, like a worm or virus that may have disabled one of the elements that a TunnelGuard policy is checking for.

Administrative access to the VPN gateway shall be restricted and a means for enforcing corporate policies for passwords, their construction and expiration should be devised. Currently the VPN gateway does not provide any means for password aging or complexity.

Secure, encrypted tunnel shall be used exclusively. Auto Backup, currently available only over ftp, shall be done with an emphasis on the security on the server were they reside and taking into account that data in transit can be intercepted. The placement of the backup and syslog servers, from a network perspective, should take into account the insecure mechanism used (ftp and syslog).

© SANS Institute 2004 As part of GIAC practical repository Author retains full rights

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Costs

Implementation of the audit checklist is within the level of work that an administrator should expect when configuring a device as critical as the VPN gateway. The need for an administration and monitoring framework is beyond the scope of this audit. The audit concentrated on finding the most comprehensive and efficient configuration to take advantage of such framework, as it becomes available.

References

- http://www142.nortelnetworks.com/bvdoc/contivity/doc_pdf/315000E02.pdf (pages 33 and 34) (January 14, 2004)
- http://www142.nortelnetworks.com/bvdoc/contivity/doc_html/317017A00/TunnelGuard_Guide.htm (January 14, 2004)
- http://csrc.nist.gov/cryptval/140-1sp/140sp179.pdf (January 14, 2004)
- http://www.nortelnetworks.com/promotions/2003b/apac/sync/collateral/contivty48features_pss5.pdf (January 14, 2004)
- http://www.sans.org/practical/GSNA/William_Karwisch_GSNA.pdf (January 14, 2004)
- http://www.microsoft.com/windowsserver2003/techinfo/overview/quarantine.mspx (January 14, 2004)
- http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns413/networking_solutions_package.html (Janaury 14, 2004)
- (http://www.ietf.org/IESG/LIAISON/itut-sg17-ls-x805-end2end-communications.pdf) (January 14,2004)
- http://www.sans.org/newsletters/cva/#process (January 14, 2004)
- http://www.sans.org/top20 (January 14, 2004) Version 4.0
- http://csrc.nist.gov/nissc/1997/proceedings/577slides.pdf (December 15, 2003)

© SANS Institute 2004 As part of GIAC practical repository Author retains full rights

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Last Updated: May 25th, 2013

Upcoming SANS IT Audit Training

Community SANS @ CANHEIT	Ottawa, ON	Jun 13, 2013 - Jun 14, 2013	Community SANS
SANSFIRE 2013	Washington, DC	Jun 14, 2013 - Jun 22, 2013	Live Event
Community SANS Chicago	Chicago, IL	Jul 08, 2013 - Jul 12, 2013	Community SANS
SANS vLive - SEC566: Implementing and Auditing the Twenty Critical Security Controls - In-Depth	SEC566 - 201307,	Jul 08, 2013 - Aug 07, 2013	vLive
SANS Rocky Mountain 2013	Denver, CO	Jul 14, 2013 - Jul 20, 2013	Live Event
Critical Security Controls Summit	Washington, DC	Aug 12, 2013 - Aug 18, 2013	Live Event
Community SANS Dallas	Dallas, TX	Aug 19, 2013 - Aug 22, 2013	Community SANS
SANS vLive - AUD507: Auditing Networks, Perimeters, and Systems	AUD507 - 201309,	Sep 02, 2013 - Oct 16, 2013	vLive
SANS CyberCon Fall 2013	Online, VA	Sep 09, 2013 - Sep 14, 2013	CyberCon
Network Security 2013	Las Vegas, NV	Sep 14, 2013 - Sep 23, 2013	Live Event
Community SANS Miami	Miami, FL	Sep 16, 2013 - Sep 19, 2013	Community SANS
Network Security 2013 - SEC566: Implementing and Auditing the Twenty Critical Security Controls - In-Depth	Las Vegas, NV	Sep 16, 2013 - Sep 20, 2013	vLive
Mentor Session - SEC 566	Troy, MI	Oct 01, 2013 - Dec 10, 2013	Mentor
Community SANS Washington @ GWU	Washington, DC	Oct 07, 2013 - Oct 10, 2013	Community SANS
SANS Baltimore 2013	Baltimore, MD	Oct 14, 2013 - Oct 19, 2013	Live Event
SOS SANS October Singapore 2013	Singapore, Singapore	Oct 21, 2013 - Nov 02, 2013	Live Event
SANS Chicago 2013	Chicago, IL	Oct 28, 2013 - Nov 02, 2013	Live Event
Community SANS New York	New York, NY	Nov 04, 2013 - Nov 07, 2013	Community SANS
SANS Sydney 2013	Sydney, Australia	Nov 11, 2013 - Nov 23, 2013	Live Event
SANS London 2013	London, United Kingdom	Nov 16, 2013 - Nov 25, 2013	Live Event
Community SANS Toronto	Toronto, ON	Nov 18, 2013 - Nov 21, 2013	Community SANS
SANS vLive - SEC566: Implementing and Auditing the Twenty Critical Security Controls - In-Depth	SEC566 - 201312,	Dec 02, 2013 - Jan 15, 2014	vLive
Community SANS Vancouver	Burnaby, BC	Dec 09, 2013 - Dec 12, 2013	Community SANS
North America ICS Security Summit & Training 2014	Lake Buena Vista, FL	Mar 11, 2014 - Mar 20, 2014	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced