National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

Intrusion, Incorporated
SecureNet Pro™ Intrusion Detection System
Version 4.1 SP 1

Report Number: CCEVS-VR-02-0032

23 December 2002

National Institute of Standards and Technology

Information Technology Laboratory

100 Bureau Drive

Gaithersburg, MD 20899

National Security Agency

Information Assurance Directorate

9800 Savage Road STE 6740

Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team

Maureen Cheheyl

Franklin Haskell

The MITRE Corporation

Bedford, Massachusetts

Alton W. Lewis

National Security Agency

Linthicum, Maryland

Common Criteria Testing Laboratory

COACT CAFE Lab

Columbia, Maryland

1. Executive Summary

This report documents the NIAP validators' assessment of the CCEVS evaluation of the Intrusion, Incorporated, SecureNet Pro™ Intrusion Detection System Version 4.1 Service Pack (SP) 1. It presents the evaluation results, their justifications, and the conformance result.

The evaluation was performed by the COACT Incorporated CAFE Laboratory and was completed on 20 December 2002. The information in this report is largely derived from the Evaluation Technical Report (ETR) written by COACT and submitted to the validators. The evaluation determined that the product conforms to the Common Criteria Version 2.1, Part 2 and Part 3, to meet the requirements of Evaluation Assurance Level (EAL) 2, resulting in a "pass" in accordance with CC Part 1 paragraph 175.

The TOE is the SecureNet Pro™ Intrusion Detection System Version 4.1 SP 1, which is a network monitoring and intrusion detection software-based application. The SecureNet Pro™ Intrusion Detection System is deployed as a two-tier architecture consisting of a single Sensor and a single Administrative Console. (The optional three-tier architecture, including a Provider Manager, was not evaluated, nor was the use of more than one Sensor or more than one Administrative Console.) The Sensor performs intrusion detection and analysis functions. The Administrative Console enables the Administrator to monitor, configure, and administer Sensors remotely, view Sensor monitoring sessions, replay archived sessions, and generate reports. Although the SecureNet Pro product ships with hardware and operating system for the Sensor, only the Sensor and Administrative Console software has been evaluated.

The validation team monitored the activities of the evaluation team, observed evaluation testing activities, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore the validation team concludes that COACT's findings are accurate, the conclusions justified, and the conformance results correct.

Disclaimers: The information contained in this Validation Report is not an endorsement of SecureNet Pro™ by any agency of the U.S. Government, and no warranty of SecureNet Pro™ is either expressed or implied.

2. Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level

(EAL) 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products negotiate a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List. The table below provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated
- The Security Target (ST), describing the security features, claims, and assurances of the product
- The conformance result of the evaluation
- The organizations and individuals participating in the evaluation

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	SecureNet Pro™ Intrusion Detection System Version 4.1 Service Pack (SP) 1
Protection Profile	None
Security Target	Intrusion, Inc. SecureNet Pro™ Intrusion Detection System Version 4.1 SP1 Security Target, F2-1202-004, dated December 20, 2002
Evaluation Technical Report	Intrusion, Inc. SecureNet Pro™ Evaluation Technical Report, F2-0902-001(1), October 30, 2002, with Addenda.
Conformance Result	Part 2 conformant and Part 3 EAL 2 conformant
CC Version	CC Version 2.1 and all applicable National and International Interpretations effective on 6 December 2001
CEM Version	CEM Version 1.0 and all applicable National and International Interpretations effective on 6 December 2001
Sponsor	Intrusion, Incorporated
Developer	Intrusion, Incorporated
Evaluators	COACT CAFE Lab: Eric J. Grimes, William R. Knight, Robert J. West, Jennifer A. Arthur, Thomas J. Fisher, Tonya D. Dawkins
Validators	Maureen Cheheyl (The MITRE Corporation) Franklin Haskell (The MITRE Corporation) Alton W. Lewis (NSA)

3. Security Policy

The Security Target does not state a security policy for SecureNet Pro.

The Security Objectives for the TOE state that

- The Administrative Console will manage the Sensor and its functions
- The Sensor will monitor the environment and detect intrusion attempts to the network or systems on the network by monitoring all data sent across the network
- The Sensor will respond to detected events by sending alerts of intrusion attempts or inappropriate activity occurring on the network or systems on the network to the Administrative Console.
- The Sensor will collect and store information about all events that are indicative of intrusion attempts or inappropriate activity occurring on the network or systems on the network that the Sensor is monitoring.

4. Assumptions and Clarification of Scope

Usage Assumptions

A.CONSOL The Administrative Console software application will be installed, configured and operated on a dedicated host that meets the system requirements specified to support the Administrative Console software application supplied as part of the SecureNet™ CC7345 delivery package.

A.INTER The Operating System that runs the Administrative Console environment provides the Administrator with an interface to the TOE through an X Windows GUI application.

A.UNAUTH Unauthorised access to the TOE is prevented by the security features of the Operating System, external to the TOE.

A.ATCKSIG The Administrator is responsible for obtaining the latest signature pack from the Intrusion, Inc. web site for use by the TOE.

A.CONFIG The Administrator will run the configuration executables at system initialisation to build the trusted Sensor and trusted Administrative Console configuration files. The Administrator will follow all administrative guidance procedures supplied in the SecureNet™ CC7345 delivery package to ensure proper configuration of these files.

A.INSTALL The Administrator will follow all administrative guidance procedures supplied in the SecureNet™ CC7345 delivery package to ensure proper installation of the Administrative Console software application.

A.IPADD The Administrator will configure all IP addresses to be monitored by the Sensor.

A.NOEVIL The Administrator is not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

Environmental Assumptions

A.OPSYS The Sensor is run on the Pilot 2.3 SP2 Operating System [which is a vendor-supplied version of Red Hat Linux6.2].

A.SENSOR The SecureNet™ CC7345 delivery package is provisioned and includes all hardware and software necessary to run the Sensor software application. The Sensor software application is delivered to the customer in a pre-installed and operational state.

A.SUPPORT The Pilot 2.3 SP2 Operating System will provide necessary support for the Sensor. The Red Hat Linux 6.2 Operating System will provide necessary support for the Administrative Console.

A.CC7345 The SecureNet™ CC7345 delivery package will be purchased from Intrusion, Inc. and delivered to the customer with all specified hardware and software necessary to ensure the TOE's compliance with the requirements outlined in this ST.

A.DEPLOY The Administrative Console requires a dedicated host for execution and is deployed on a secure LAN that has no direct links to untrusted LANs.

A.LOCATE The Administrative Console and the Sensor are located in a physically secure area.

Clarification of Scope

The TOE is designed solely to detect and respond (in a limited fashion) to attacks against the network the sensor is monitoring and the systems attached to that network. It relies to a large extent upon the environment and underlying operating system to supply almost all the protections one would consider necessary in a network environment.

As one would expect at EAL2, little effort was expended to search for and test for obvious vulnerabilities. The evaluators did examine a denial of service attack, though. The product resisted the attack the evaluators created, but no further attacks were created to probe the limits. Since the evaluation did not include multiple sensors, no guidance can be offered concerning, for example, configuration of Ethernet switches to divide the traffic in an attempt to defeat such attacks.

5. Architectural Information

The SecureNet Pro™ product consists of hardware and a CD containing the SNP software, operating system software, and documentation. The TOE consists wholly of software. Its components are deployed on separate pieces of (unevaluated) hardware with (unevaluated) operating systems as a sensor and a console that communicate with each other. The evaluated configuration includes a single Sensor and a single Administrative Console.

Sensor Subsystem

The Sensor performs intrusion detection and analysis functions. It detects the attacks described in its database and communicates this information to the console when requested.

It is the SNPd program that does all of the real work. It uses a NIC running in promiscuous mode to receive all the packets being broadcast on that Ethernet segment. It decodes and analyzes each packet, comparing the contents against its database of attack signatures. When an attack is detected, the Sensor records information about the attack and sends alerts to the Console.

The SNPt program also receives notifications from SNPd, reformats them into SNMP traps, and transmits the traps to agents designated to receive them.

Console Subsystem

The Administrative Console enables the administrator to monitor, configure, and administer the sensor remotely; to view sensor monitoring sessions; to replay archived sessions; and to generate reports.

The SNPc program runs on console systems using the X display. It receives alerts from the sensor and transmits instructions to it to change its operating parameters, including what to alert on and how much data to store.

The SNPreport program generates reports from the sensor data using filters and formatting.

Configuration

The evaluated configuration includes a single Sensor and a single Administrative Console, communicating over a private LAN distinct from the one being monitored.

The Administrative Console is deployed on a dedicated host connected to a secure LAN with no direct links to untrusted LANs. The minimum platform requirements for the Administrative Console software application are as follows: X86-based hardware platform, Red Hat 6.2 Operating System running Linux kernel 2.2.19-17, Pentium III 500 MHz CPU, 256 MB RAM, 8 GB disk space, 100-Mbps NIC, with an X Windows System and application software.

The Sensor, running on the SecureNet™ CC7345 hardware platform delivered with the SNP product, is connected to the same secure LAN from one connection and to the monitored network from another connection. The secure LAN is used only for communications between the Sensor and the Administrative Console.

The evaluated configuration is pictured in Section 8 below.

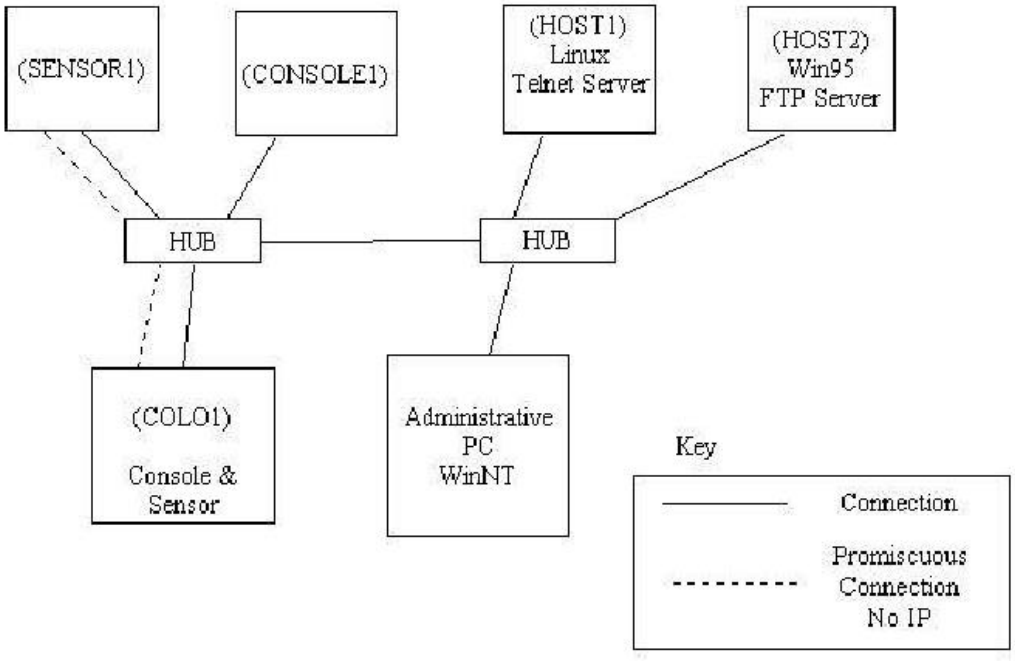
6. Documentation

The SecureNet Pro product is delivered with two CDs that contain the following files:

- *READmeFIRST.txt* describes the contents of the CD- ROM.
- *Readme_SNP41_Gig_SP1.txt* provides information about the SecureNet Pro™ Sensor updates.
- *SecureNet Pro™ QSG.pdf* is the SecureNet Pro™ Quick Start in Adobe Portable Document Format (PDF).
- *SecureNet Pro™ 4.1 SP1 User_Guide.pdf* is the PDF version of the SecureNet Pro™ 4.1 SP1 Software User Guide, Rev. A.
- *SecureNet 5745&Gig2 Quick Start.pdf* is the PDF version of the SecureNet 5745 Quick Start and SecureNet Pro™ Quick Start guides.
- *PDS Pilot API Guide.pdf* is the PDF version of the Pilot API Reference Guide.
- *Software_Licence_Agreement* contains the Intrusion Software License Agreement.
- *License.txt* contains the Adobe Acrobat Reader End User License Agreement.

7. IT Product Testing

The evaluators ran the vendor's suite of tests and then created and ran a test of their own. They also looked for obvious vulnerabilities. The following test configuration was used.



This configuration is adequate to generate the various kinds of traffic the product could be expected to handle, though not the volume. Note that, while it contains two sensors and two consoles, those are not tested simultaneously.

8. Evaluated Configuration

The TOE is deployed on (unevaluated) hardware and operating system as Sensors and Consoles that communicate with each other.

Sensor

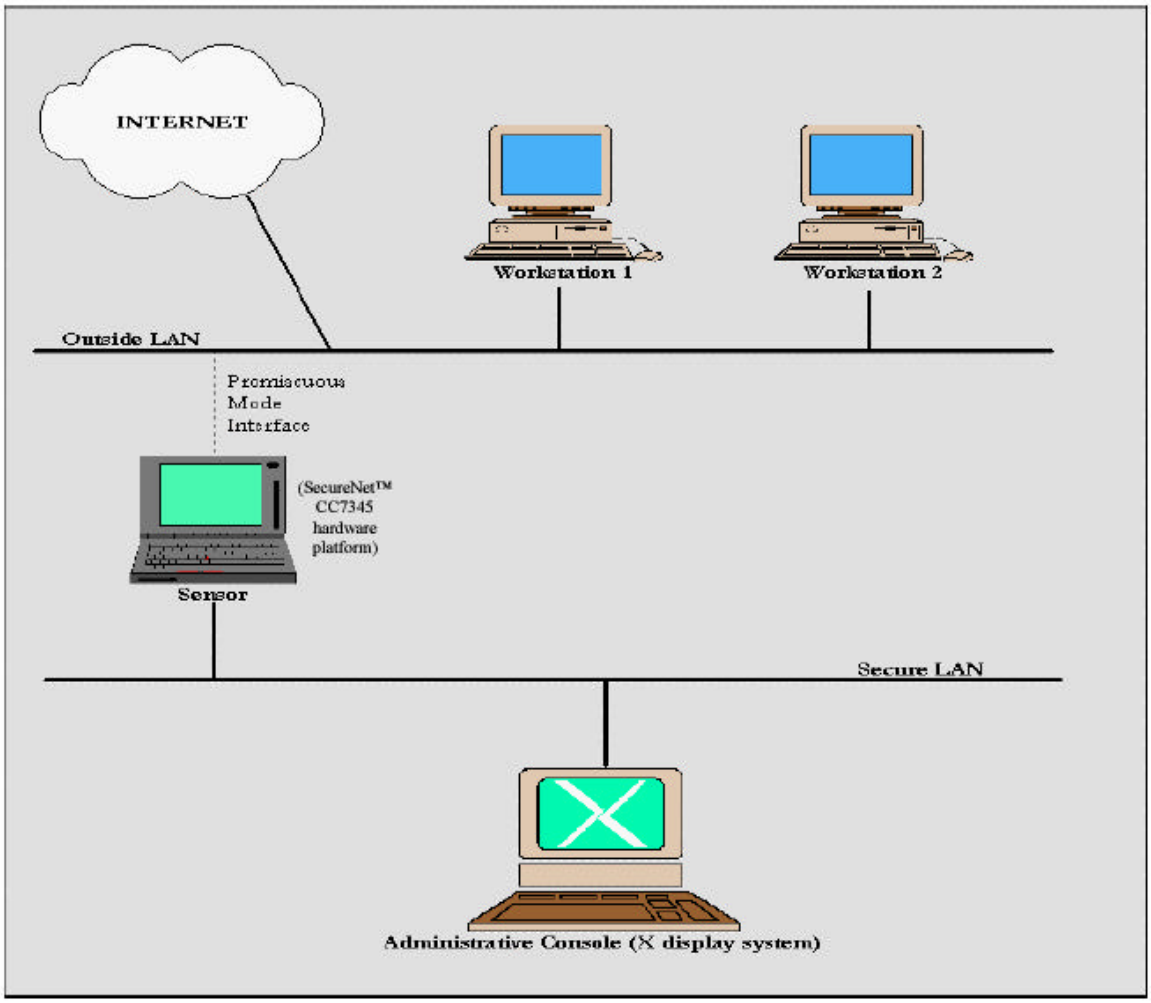
The Sensor is the SecureNet™ CC7345 hardware platform built by Intrusion, Inc., with a vendor-supplied version of Red Hat Linux6.2 Operating System (known by the vendor as the Pilot 2.3 SP2 Operating System) and the SecureNet Pro Sensor software installed.

Console

The Console is a hardware platform conforming to the specifications set forth in the SecureNet Pro™ Intrusion Detection System Version 4.1 SP1 Security Target with the SecureNet Pro Administrative Console software installed. The minimum platform requirements for the Administrative Console are as follows: X86-based hardware platform, Red Hat 6.2 Operating System running Linux kernel 2.2.19-17, Pentium III 500 MHz CPU, 256 MB RAM, 8 GB disk space, 100-Mbps NIC, with an X Windows System and application software.

Evaluated Configuration

The figure below represents the evaluated configuration as described in the SecureNet Pro™ Intrusion Detection System Version 4.1 SP1 Security Target.



9. Results of the Evaluation

The evaluation was conducted based upon the Common Criteria (CC), Version 2.1, dated August 1999 [1,2,3]; the Common Evaluation Methodology (CEM), Version 1.0, dated August 1999 [5]; and all applicable National and International Interpretations in effect on 6 December 2001. The evaluation confirmed the product as being Part 2 conformant and Part 3 EAL 2 compliant. The details of the evaluation are recorded in the Evaluation Technical Report, which is controlled by the COACT CAFE Laboratory.

The validation team followed the procedures outlined in the Common Criteria Evaluation Scheme [CCEVS] publication number 3 for Technical Oversight and Validation Procedures. The validation team has observed that the evaluation and all of its activities were in accordance with the Common Criteria, the Common Evaluation Methodology, and the CCEVS. The validation team therefore concludes that the evaluation and its results of pass are complete.

The evaluation provides for Assurance at the EAL 2 level with assurance components as shown in the table below:

Assurance class	Assurance components
Class ACM: Configuration management	ACM_CAP.2 Configuration items
Class ADO: Delivery and operation	ADO_DEL.1 Delivery procedures
	ADO_IGS.1 Installation, generation, and start-up procedures
Class ADV: Development	ADV_FSP.1 Informal functional specification
	ADV_HLD.1 Descriptive high-level design
	ADV_RCR.1 Informal correspondence demonstration
Class AGD: Guidance documents	AGD_ADM.1 Administrator guidance
	AGD_USR.1 User guidance
Class ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
Class AVA: Vulnerability assessment	AVA_SOF.1 Strength of TOE security function evaluation
	AVA_VLA.1 Developer vulnerability analysis

Evaluation of the Intrusion Inc. SecureNet Pro 4.1 Security Target (ST) (ASE)

The evaluation team applied each EAL 2 ASE CEM work unit. Evaluation team action during the course of the ST evaluation ensured that the ST contained a description of the environment in terms of threats, assumptions and policies; a statement of security requirements claimed to be met by the Intrusion Inc. SecureNet Pro product that are consistent with the Common Criteria; and product security function descriptions that support the requirements.

Evaluation of the Configuration Management capabilities (ACM)

The evaluation team applied each EAL 2 ACM CEM work unit. The ACM evaluation ensures that the integrity of the TOE is adequately preserved; in particular, that configuration management provides confidence to the consumer that the TOE and documentation used for evaluation are the ones prepared for distribution. It also ensures that the TOE is accurately and uniquely identified such that the consumer is able to identify the evaluated TOE and discern one version from another. Configuration Management (CM) systems are put in place to ensure the integrity of the portions of the TOE that they control, by providing a method of tracking changes and by ensuring that all changes are authorized. The Evaluation Team identified and analyzed the CM process to ensure that its documented procedures were followed and the procedures were employed during the course of this evaluation. The evaluation team ensured that the following items were considered configuration items: TOE implementation, design documentation, test documentation, and user guidance.

Evaluation of the Delivery and Operation documents (ADO)

The evaluation team applied each EAL 2 ADO CEM work unit. The ADO evaluation ensured the adequacy of the procedures to securely deliver, install, configure, and operationally use the TOE; and ensured that the security protection offered by the TOE was not compromised during these events.

Evaluation of the Development (ADV)

The evaluation team applied each EAL 2 ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF implements/employs the security functions. The design documentation consists of a functional specification and a high-level design document. The evaluation team also ensured that the correspondence analysis between the design abstractions correctly demonstrated that the lower abstraction was a correct and complete representation of the higher abstraction.

Evaluation of the Guidance Documents (AGD)

The evaluation team applied each EAL 2 AGD CEM work unit. The evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE.

Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each EAL 2 ATE CEM work unit. The evaluation team ensured that the TOE performed as described in the functional specification and as stated in the TOE security functional requirements. The evaluation team performed a sample of the vendor test suite, and devised an independent set of team tests and penetration tests. The vendor tests, team tests, and penetration tests substantiated the security functional requirements in the ST.

Vulnerability Assessment Activity (AVA)

The evaluation team applied each EAL 2 AVA CEM work unit. The evaluation team ensured that the TOE does not contain obvious vulnerabilities that can be exploited in the evaluated configuration, based upon the developer strength of function analysis and the developer vulnerability analysis as well as the evaluation team's performance of penetration tests.

Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's performance of a subset of the vendor test suite, the independent tests, and the penetration test also demonstrates the accuracy (or veracity) of the claims in the ST.

10. Validator Comments and Recommendations

The security goals for the product, described in Section 3 above, are modest. As pointed out in Section 4, the TOE is designed solely to detect and respond (in a limited fashion) to attacks against the network the sensor is monitoring and the systems attached to that network. It relies to a large extent upon the environment and underlying operating system to supply the protections one would consider necessary in a network environment. Furthermore, the evaluated configuration is limited to a single sensor and a single administrative console. With an assurance level of EAL 2, testing and analysis is also minimal.

The validators believe that the product meets the claims of the Security Target, but users should be aware of the bounds of the evaluation when preparing to install and use the product.

11. Security Target

Intrusion, Inc. SecureNet Pro™ Intrusion Detection System Version 4.1 SP1 Security Target

December 20, 2002

Document No. F2-1202-004

12. Bibliography

Criteria, Methodology, and Program Scheme Documentation

1. *Common Criteria for Information Technology Security Evaluation, Part 1 Introduction and General Model,* Version 2.1, dated August 1999
2. *Common Criteria for Information Technology Security Evaluation, Part 2 Security Functional Requirements,* Version 2.1, dated August 1999
3. *Common Criteria for Information Technology Security Evaluation, Part 3 Security Assurance Requirements,* Version 2.1, dated August 1999
4. *Common Methodology for Information Technology Security Evaluation,* Part 1, Version 0.6, dated January 1997
5. *Common Methodology for Information Technology Security Evaluation,* Part 2, Version 1.0, dated August 1999
6. *Guide for the Production of PPs and STs,* Version 0.9, dated January 2000

Developer Documentation

7. *Intrusion, Inc. Procedure for Document Revision Control,* Rev. C, dated 06/01/01
8. *Intrusion, Inc. Procedure for Approval, Release, and Control of Product Documents,* Rev. D, dated 06/01/01
9. *Intrusion, Inc. SecureNet Pro™ Software User Guide,* Rev. A, dated July 2001
10. *Intrusion, Inc. SecureNet Pro™ Security Functions Reference,* Version 4.3, dated April 2002
11. *Intrusion, Inc. SecureNet Pro™ Testing and Vulnerability Analysis Reference,* Version 3.3, dated April 2002
12. *Intrusion, Inc. SecureNet CC™ Drawing Tree,* Revision C, dated 03/12/02
13. *Intrusion, Inc. SecureNet 5745 Quick Start* (Part of Delivery package, on CD or Hardcopy), revision A, dated February 2002
14. *Intrusion, Inc. SecureNet Pro™ Quick Start* (Part of Delivery package, on CD or Hardcopy), revision A, dated February 2002
15. *Intrusion, Inc. READmeFIRST.txt* (Part of Delivery package, on CD or Hardcopy), revision A, dated February 2002
16. *Intrusion, Inc. Readme_SNP41_Gig_SP1.txt* (Part of Delivery package, on CD or Hardcopy), revision A, dated February 2002
17. *Intrusion, Inc. SecureNet Pro™ 4.1 SP1 Documentation* (Part of Delivery package, on CD or Hardcopy), revision A, dated February 2002
18. *Intrusion, Inc. 750-1006-101_c.tif,* revision C, dated 08/09/02 (Part 1 of the Bill of Materials for the SNP product)
19. *Intrusion, Inc. 714-1024-102_a.bmp,* revision A, dated 08/09/02 (Part 2 of the Bill of Materials for the SNP product)
20. *Intrusion, Inc. Pilot API Reference Guide* (Part of Delivery package, on CD or Hardcopy), revision A, dated February 2002

13. Glossary

BOM	Bill of Materials
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Evaluation Testing Laboratory
CEM	Common Evaluation Methodology

CM	Configuration Management
EAL	Evaluation Assurance Level
IDS	Intrusion Detection System
IT	Information Technology
LAN	Local Area Network
NIAP	National Information Assurance Partnership
NIDS	Network Intrusion Detection System
NIST	National Institute of Science & Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
PDF	Portable Document Format
PP	Protection Profile
RAM	Random Access Memory
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirements
SNP	SecureNet Pro™
SOF	Strength of Function
SP	Service Pack
ST	Security Target
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy
WAN	Wide Area Network