

# Network IPS Corporate Certification Testing Criteria

Version 1.0



26 June 2006

## TABLE OF CONTENTS

<b>INTRODUCTION.....</b>	<b>1</b>
WHY DEPLOY NETWORK INTRUSION PREVENTION SYSTEMS? .....	1
REGARDING THE CRITERIA REQUIREMENTS.....	1
WHAT A NETWORK INTRUSION PREVENTION SYSTEM MINIMALLY PROVIDES .....	1
WEBSITE OF CERTIFIED NETWORK IPS DEVICES .....	2
<b>BASELINE REQUIREMENTS.....</b>	<b>3</b>
FUNCTIONAL REQUIREMENTS.....	3
<i>Administrative Functions</i> .....	3
<i>Administration</i> .....	3
<i>Identification &amp; Authentication</i> .....	4
<i>Traffic Flow</i> .....	4
<i>Logging</i> .....	4
<i>Reporting</i> .....	6
ASSURANCE REQUIREMENTS .....	6
<i>Functional Testing</i> .....	6
<i>Security Testing</i> .....	7
<i>Documentation</i> .....	8
<b>GLOSSARY .....</b>	<b>9</b>
ABOUT THE GLOSSARY TERMS .....	9
DEFINED TERMS .....	9

## INTRODUCTION

### WHY DEPLOY NETWORK INTRUSION PREVENTION SYSTEMS?

Corporate businesses and enterprises need to secure and monitor their networks. These organizations are faced with protecting themselves at several, often dissimilar, points in their networks against a myriad of threats. They need a means to not only block malicious attackers entering through perimeter Internet and WAN connections but also to prevent the exploitation of network resources by valid users who either unwittingly or purposefully introduce compromised equipment or exploits into the core of an organization's network.

Properly designed and configured Network Intrusion Prevention Systems help satisfy these needs. While continuing to pass legitimate network traffic, Network Intrusion Prevention Systems are capable of successfully and repeatedly repelling network-borne attacks aimed at network services, servers, and clients. They protect against threats including buffer overflows, worms targeting vulnerabilities in network services, and rate-based denials-of-service. Having been designed to introduce minimal latency, they are suitable for deployments both near perimeter Internet and WAN connections as well as at the core of an organization's network. While providing security to the network, a Network IPS can additionally alert on, log, and report attack attempts.

For all these reasons, the Network IPS is a necessary component in an organization's arsenal of layered network security defenses.

### REGARDING THE CRITERIA REQUIREMENTS

The *Network IPS Corporate Certification Testing Criteria* consists of a baseline set of functional and assurance requirements that are applicable to organizations including small-to-medium sized businesses, corporations, and enterprises. To attain and retain ICSA Labs Network IPS Certification, Candidate Network IPS products and services must completely satisfy the entire set of baseline requirements herein.

Conventions:

*Italics* - All italicized terms and expressions appearing in this document are defined in the glossary at the end of this document. Italicized terms and expressions begin with a capital letter. The only other usages of italics occur in individual requirement titles and in identifying documents.

Notes - Several requirements are followed by one or more notes. Strictly speaking, notes are not requirements. Instead, notes attempt to clarify some portion of the preceding requirement.

Phraseology:

Throughout the criteria phrases such as "provide a means" and "include the capability" are used. When they occur, they are meant to alert the reader that the capability in question need not be implemented by default, at all times, or be the only configurable option ultimately available to end users.

### WHAT A NETWORK INTRUSION PREVENTION SYSTEM MINIMALLY PROVIDES

This document presents in criteria language the baseline set of requirements that a corporate Network Intrusion Prevention System (IPS) must minimally include. The following paragraphs describe at a high level the functionality provided by a corporate Network IPS that meets the baseline set of criteria requirements.

A corporate Network IPS includes at least one *Segment*. An information flow control *Policy* that determines the level of vulnerability protection is applied to the *Mission Interfaces* comprising each segment being tested. Without being evaded and according to the applied *Policy*, it repeatedly blocks attacks targeting an evolving set of remotely exploitable, server-side vulnerabilities that are relevant to end users. Also it mitigates the effects of traditional denial-of-service attacks. While providing these protections the Network IPS introduces a tolerable amount of latency.

Additionally a corporate Network IPS logs and reports on numerous security, operational, and system events, providing appropriate data for each. It requires administrator identification and authentication prior to permitting secure, remote administration. Its mission interfaces must be transparent thereby not affecting existing network topologies. Also, the Network IPS engine is itself tamperproof. Finally, it includes guidance for administrators documenting how to properly configure and use it.

### WEBSITE OF CERTIFIED NETWORK IPS DEVICES

The Network Intrusion Prevention portion of the ICSA Labs website includes a page that lists the developers and products or services that are currently **ICSA Labs Network IPS Certified**. Any optional requirements beyond this baseline set of criteria requirements against which the SUT was successfully tested are shown on the website. The presentation of the certified products and services is intended to assist end users in determining which Network IPS may be particularly suited for their needs and environment. Also of particular value are the certification testing reports that are also available on the website. There is no charge for any of this information.

## BASELINE REQUIREMENTS

### FUNCTIONAL REQUIREMENTS

#### Administrative Functions

##### AF1 – *Enable Transparent Mode*

Unless it is already in *Transparent Mode*, the *SUT* must include a means to place its *Mission Interfaces* into *Transparent Mode*.

NOTE1 to AF1 – This does not preclude the *SUT* from providing modes other than *Transparent Mode* for its *Mission Interfaces*.

NOTE2 to AF1 – There is no requirement that the *Mission Interfaces* be separate from the *Remote Administration* interface. However, if there is a separate *Remote Administration* interface, there is no requirement that it also be in *Transparent Mode*.

##### AF2 – *Transparent Mode Administrative Capabilities*

While in *Transparent Mode*, the *SUT* must provide a means to:

1. Access the *SUT* through the *Remote Administration* interface;
2. Configure and apply various *Policies*;
3. Configure and change or acquire the date and time;
4. Enable and disable logging of the events defined in LO1.1;
5. Display all required log data in the *Log(s)* that was specified in LO2 for the events defined in LO1;
6. Generate and display all required report data for the events defined in RE1 and RE2;
7. Configure and change all *Authentication Configuration Data*;
8. Configure and change *Remote Administration* settings;
9. Enable and disable the network acquisition and automatic enforcement of protection updates.

NOTE1 to AF2 – By prefixing the listed requirements with “provide a means to” the requirement implies that these capabilities have to be present. However, there is no requirement that these capabilities be implemented by default, at all times, or be the only capabilities available.

NOTE2 to AF2 – With regards to AF2.9, there may be multiple types and bundling of *SUT* updates. The requirement refers to only those *SUT* updates that ultimately provide vulnerability protection for network services, servers, clients, and the *Engine* itself.

#### Administration

##### AD1 – *Remote Administration*

The capability must exist for a *User* to perform encrypted *Remote Administration* of the *Engine* through at least a single *Engine* interface.

NOTE1 to AD1 – This requirement is not implicitly or explicitly requiring a dedicated administration interface on the *Engine*, as *Remote Administration* could be performed using a *Mission Interface*.

## Identification & Authentication

### IA1 – Identify & Authenticate Prior to Administrative Function Access

The *SUT* must include the capability to require and enforce *User* identification followed by authentication with a password having the characteristics specified in IA2 or a multi-factor *Authentication Mechanism* prior to permitting access to the *Administrative Functions* and other non-required *SUT* functions.

### IA2 – Strength of Password (CONDITIONAL)

The *SUT* must include the capability to set *User* passwords to a mix of eight or more letters, numbers, and special characters.

NOTE1 to IA2 – This requirement is CONDITIONAL as the *SUT* may provide a multi-factor rather than a password authentication mechanism to meet IA1. Thus IA2 does not apply when the *SUT* provides a multi-factor authentication mechanism, a password is not one of the necessary factors, and the *SUT* can be tested without a password factor in the event that there is one.

## Traffic Flow

### TF1 – Passing IP Traffic

While in *Transparent Mode*, the *SUT* must pass all *Clean* IP traffic up to 80% of the *Rated Throughput* through its *Mission Interfaces* according to the *Policy* being enforced.

## Logging

### LO1 – Required Log Events

The *SUT* must include the capability to capture the required log data in LO2 for the following security, operational, and system events:

1. Security Events
  - a. All attempts to pass attacks through the *Engine* that target any *Vulnerability Set* elements when the *Policy* for the *Vulnerability Set* element related to the attack is tuned to:
    - i. Detect and prevent;
    - ii. Detect and permit.
2. Operational Events
  - a. When a *User* powers down the *Engine*, in the event that such functionality exists; (CONDITIONAL)
  - b. When a change is made to the *Policy* being enforced;
  - c. When a change is made to the *Authentication Configuration Data* of a *User*;
  - d. When a *User* attempts to authenticate to a *Remote Administration* interface.
3. System Events
  - a. After any startup sequence is complete when the *Engine* powers on;
  - b. When the link status of a *Mission Interface* changes.

NOTE1 to LO1 – Requirement LO1.2.a is CONDITIONAL in that there may not be a software or command line interface to power down the *Engine*. If not, then this requirement would not be applicable. There is no requirement to log when the *Engine* is powered down using either a physical switch on the *SUT* or any other physical means.

## LO2 – *Required Log Data*

The *SUT* must include the capability to accurately capture in a *Log* for each required log event in LO1 the following log data elements:

1. For all events:
  - a. The date and time that the event occurred;
    - i The date must consist of the four-digit year, the month, and the numerical day in the month;
    - ii The time must consist of the hour, the minute, and the second;
  - b. A description indicating why the *SUT* logged the event.
2. For “Security” events in LO1.1:
  - a. An indication of the action taken by the *SUT*;
  - b. The protocol;
  - c. For IP, the source and destination IP addresses;
  - d. For TCP and UDP, the source and destination ports;
  - e. A unique identifier representing the *Engine* that detected the event.
3. For “Operational” event LO1.2.d:
  - a. An indication of the username that attempted to authenticate;
  - b. An indication of success or failure to authenticate;
4. For “System” event LO1.3.b:
  - a. The physical *SUT* interface link status.

NOTE1 to LO2 – Log data for the events in LO1 may be logged in different *Logs* and may in fact require different interfaces to review those *Logs*.

## LO3 – *Aggregating Logging of Multiple Related Packets*

Upon detecting multiple packets corresponding to a single LO1.1-related event, the *SUT* must include the capability to aggregate the log data capture for that event into a single entry in the *Log*.

NOTE1 to LO3 – This requirement implies in part that a single attack cannot appear in the *Log* as more than a single attack.

## LO4 – *Log Data Presentation*

All required log data corresponding to all required log events defined in LO1 must be available for review upon demand and presented in a human readable format while preserving the relative sequence of events.

## LO5 – *Linking Multiple Logs for a Single Event (CONDITIONAL)*

A clear, accurate correlation between any log data for a single event retrieved from multiple *Logs* must exist linking the data for the event together.

NOTE1 to LO5 – This requirement is CONDITIONAL. It is only relevant for those *SUTs* that record all the required log data for one or more required log events but that do not display that data wholly together.

## Reporting

### RE1 – *Most Common Policy Violations*

The *SUT* must include the capability to report the ten most common *Policy* violations over the preceding:

1. Hour;
2. Day;
3. Seven days;
4. Thirty days;
5. Ninety days.

### RE2 – *Most Common Sources of Policy Violations*

From its perspective, the *SUT* must include the capability to report on the ten most common sources of *Policy* violations over the preceding:

1. Hour;
2. Day;
3. Seven days;
4. Thirty days;
5. Ninety days.

## ASSURANCE REQUIREMENTS

### Functional Testing

#### FT1 – *Administrative Functions Work Properly*

The *SUT* must demonstrate through testing that the *Administrative Functions* defined in AF1 and AF2 operate properly.

#### FT2 – *Average One-Way Latency*

While testing under the following conditions:

1. While in *Transparent Mode*;
2. While enforcing a *Policy* that meets ST4, ST5, ST6, and ST7;
3. With *Background Traffic* flowing through the *SUT* and filling the *SUT* bandwidth between 0% and 80% of the *Rated Throughput*;
4. With attack traffic targeting *Vulnerability Set* elements comprising between 0% and 2% of the *Rated Throughput*.

the average one-way latency introduced into traffic flows by the *SUT* must be less than or equal to the value in Table 1 that corresponds to the media speed of a *Mission Interface* unless the *SUT's Rated Throughput* is less than the media speed of a *Mission Interface*, in which case the average one-way latency it introduces into traffic flows must be less than or equal to the value in Table 2 that corresponds to the *Rated Throughput* of the *SUT*.

	Mission Interface Media Speeds			
	10 Mbps	100 Mbps	1 Gbps	10 Gbps
Max Ave One-Way Latency	1.5 ms	1.5 ms	500 $\mu$ s	100 $\mu$ s

Table 1

	Rated Throughput (RT) – in bps		
	$\leq$ 325 Mbps	325 Mbps < RT < 5 Gbps	$\geq$ 5 Gbps
Max Ave One-Way Latency	1.5 ms	$1 \times 10^6 / (2 * RT)$ seconds	100 $\mu$ s

Table 2

NOTE1 to FT2 – The *SUT* developer provides ICSA Labs with the *Rated Throughput* for the *SUT* in bps (e.g., 500Mbps) prior to testing.

## Security Testing

### ST1 – *SUT Not Addressable*

While in *Transparent Mode*, it must be demonstrated through testing that the *Mission Interfaces* ignore non-administrative communication attempts.

### ST2 – *No Unauthorized Access to Administrative Functions*

While in *Transparent Mode*, it must be demonstrated through testing that unauthorized access to or control of any *Administrative Function* does not occur.

### ST3 – *Engine Not Vulnerable*

While in *Transparent Mode*, it must be demonstrated through testing that the *Engine* itself is not vulnerable via its *Mission Interfaces* to the evolving set of vulnerabilities known in the Internet community that can be remotely tested.

### ST4 – *Coverage of Attacks against Server-Side Vulnerabilities*

The *SUT* must demonstrate through testing that it is capable of preventing all attacks aimed at server-side *Vulnerability Set* elements from passing through after arriving on *SUT Mission Interfaces*, regardless of their origin and destination, under the following conditions:

1. While in *Transparent Mode*;
2. While exercising the *Administrative Functions*;
3. With *Background Traffic* flowing through the *SUT* and filling the *SUT* bandwidth between 0% and 80% of the *Rated Throughput*;
4. With attack traffic targeting *Vulnerability Set* elements comprising between 0% and 2% of the *Rated Throughput*;
5. With and without the use of evasion techniques known in the Internet community.

NOTE1 to ST4 – This Vulnerability Set contains remotely exploitable vulnerabilities. There are no client side vulnerabilities in the set. An unannounced, representative sample of attacks targeting Vulnerability Set elements are tested to successfully demonstrate success in meeting this requirement.

### ST5 – Coverage of Trivial Denial of Service (DoS) Attacks

The *SUT* must demonstrate through testing that it has the capability to appropriately *Mitigate* all *Trivial DoS Attacks* arriving on a *SUT Mission Interface*, regardless of their origin, under the following conditions:

1. While in *Transparent Mode*;
2. While exercising the *Administrative Functions*;
3. With *Background Traffic* flowing through the *SUT* and filling the *SUT* bandwidth between 0% and 80% of the *Rated Throughput*;
4. With *Trivial DoS Attack* traffic comprising between 0% and 10% of the *Rated Throughput*;
5. With attack traffic targeting *Vulnerability Set* elements comprising between 0% and 2% of the *Rated Throughput*.

NOTE1 to ST5 – Distributed DoS (DDoS) attacks fall outside the scope of this requirement and the Baseline criteria. An unannounced, representative sample of *Trivial DoS Attacks* is tested to successfully demonstrate success in meeting this requirement.

NOTE2 to ST5 – The logging of the Security Events defined in LO1 will be disabled if possible during testing unless opposed by the *SUT* vendor.

### ST6 – Repeated Protection

While in *Transparent Mode*, the *SUT* must demonstrate through testing that at all times after successfully preventing attacks targeting *Vulnerability Set* members and mitigating all *Trivial DoS Attacks* that it continues to successfully prevent and mitigate, respectively, such attacks in accordance with the *Policy*.

### ST7 – No False Positives after Tuning

While in *Transparent Mode* and following appropriate tuning of the *Policy*, the *SUT* must demonstrate through testing that it does not detect in *Clean* traffic an attack of any kind.

NOTE1 to ST7 – By permitting *Policy* tuning to avoid false positives, ST7 does not make it permissible for the *SUT* to fall short on any requirement in this document including those related to vulnerability coverage and repeatability (ST4, ST5, and ST6).

## Documentation

### DO1 – Set Up Instructions

Sufficient, accurate *Guidance* must be provided for a *User* to set up the *SUT*.

### DO2 – Administrative Functions Usage Instructions

Sufficient, accurate *Guidance* must be provided for a *User* to perform the *Administrative Functions* in AF1 and AF2.

## GLOSSARY

### ABOUT THE GLOSSARY TERMS

This glossary is intended to ensure that readers understand what ICSA Labs means by various terms as they appear in criteria requirements. Defined here in the glossary are terms found throughout the baseline requirements, the optional requirements, and the glossary itself. When appearing in the requirements or in the glossary these terms are italicized. Glossary definitions expand upon those that might be found in a dictionary and override definitions that may exist in literature outside of this criteria document.

### DEFINED TERMS

*Administrative Functions* – These are the set of required *SUT* operations that an administrative *User* can perform only after successfully identifying and authenticating to the *SUT*.

*Authentication Configuration Data* – Depending on the *Authentication Mechanism(s)* available on the *SUT*, there may be varying types of *Authentication Configuration Data*. When the *Authentication Mechanism* is a password, then the *Authentication Configuration Data* is the password itself as well as the *Authentication Mechanism* in use (i.e., passwords). For multi-factor *Authentication Mechanisms*, any data that must be entered by an administrative *user* into the *SUT* for synchronization between it and the hardware or software token is part of the *Authentication Configuration Data*. Also included is the type of multi-factor *Authentication Mechanism* in use (e.g., SecureID tokens).

*Authentication Mechanism* – This is the specific type or method of authentication. It is either single or multi-factor. The predominant single-factor *Authentication Mechanism* is the password. An example of a multi-factor *Authentication Mechanism* is a SecureID token.

*Background Traffic* – This predominantly *Clean* traffic is comprised of a distributed mix of IP traffic comprised of protocols that are commonly found at Internet connections, WAN connections, and at the core of varying kinds and sizes of networks including but not limited to those at financial, insurance, multimedia, and international technology organizations as well as universities. The frames vary in size and represent what one would actually see in the locations and types of networks mentioned above.

*Clean* – Properly formed and known to be both free of attacks and not part of an ongoing DoS attack stream.

*Engine* – The component of a *SUT* that detects and ultimately enforces the applied *Policy* controlling the flow of traffic to and through the *SUT*.

*Guidance* – This is information that the end-user customer often receives or that managed service provider employees refer to that aids them in the use of the *SUT*. This information can be presented in several formats such as printed (book, binder, loose-leaf paper, etc.) or electronic (a .pdf file on a DVD/CDROM, an .html file on a web site, etc.).

*Log* – When it appears as a noun, it refers to a non-volatile physical storage space on some component of the *SUT* including a dedicated separate logging server. Data sent to and received by a *User* via e-mail is considered an alert and does not constitute a *Log*.

*Mission Interface* – This is an interface where filtering decisions are made to drop or pass network traffic through the *Engine* based on the current set of applied *Policies* applied to a *Segment*.

*Mitigate* – To mitigate a *Trivial DoS Attack* the following occur: The average throughput for all traffic not related to the *Trivial DoS Attack* is no less than 70% of the average throughput prior to the start of the *Trivial DoS Attack*. For those *Trivial DoS Attacks* that are not rate-based the attack itself is either neutered or blocked. For those *Trivial DoS Attacks* that are rate-based, 80% of the *Trivial DoS Attack* traffic is blocked.

*Policy* – This is the current set of vulnerability protections applied to and enforced by a *Segment*. The *Policy* also determines what and whether to log and alert on.

*Rated Throughput* – Provided to ICSA Labs by the *SUT* developer prior to testing, this is the amount of bandwidth that ICSA Labs will consume during testing with *Background Traffic* and attack traffic using the necessary number

of *Segments*. The value provided to ICSA Labs by the developer may or may not correspond to any technical marketing material. Following successful certification testing this value will be published in the resulting certification testing report and in the matrix of certified products on the ICSA Labs web site.

*Remote Administration* – This is the remote execution of *Administrative Functions* by a *User*. The modifier, “remote”, indicates that the administration is not being performed locally on or through a direct, non-networked connection to the *SUT* and indicates that a separate station is connected in some way to one of the *SUT*’s network interfaces.

*Segment* – This is a pair of physical or logical *Mission Interfaces* on the *SUT*.

*SUT* – This is the Subject Under Test. The *SUT* may be a product or a service. It is the total package submitted to ICSA Labs for testing against the requirements in this criteria document. The package submitted may consist of some or all of the following components but is not limited to: Network IPS *Engine* hardware; *Engine* application software; *Engine* firmware; underlying *Engine* operating system software and utilities; *Remote Administration* station hardware; *Remote Administration* station software; installation, configuration and/or administration documentation; device for multi-factor *Authentication Mechanism*; any 3<sup>rd</sup> party logging tool or utility; etcetera.

*Transparent Mode* – This is a state in which one cannot address or receive responses from any of the *Mission Interfaces* that are in use on the *SUT*.

*Trivial DoS Attacks* – This is a Denial of Service (DoS) where a published DoS attack tool exists, or the DoS attack can be readily performed without the use of such a tool. *Trivial DoS Attacks* are resource consumption and/or rate-based attacks. A DoS attack that requires one or a series of enabling conditions or events (e.g., a Distributed DoS attack) is not considered a *Trivial DoS Attack*.

*User* – This is any individual be it administrative or otherwise that may be set up with an account enabling them to perform actions on the *SUT* that may include some or all of the *Administrative Functions*. If the *SUT* is a service rather than a product, then the *User* is most likely an operator employed by the developer in a SOC or similar environment.

*Vulnerability Set* – This is an evolving set of remotely exploitable, low-to-high severity vulnerabilities that are relevant to organizations ranging from carriers to enterprises to small-to-medium businesses.

Copyright © 2005-2006 Cybertrust, Inc. All Rights Reserved. No part of this report may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopy, recording, or any information or storage retrieval system, without the express permission in writing from ICSA Labs. ICSA Labs is a division of Cybertrust, Inc. and is a registered mark of Cybertrust, Inc.