Network Integrity Systems
1937 Tate Blvd SE
Hickory, NC 28602
Phone: 828.322.2181
Fax: 828.322.5294

info@networkintegritysystems.com
www.networkintegritysystems.com

We Bring Security To Light™

Application Note:
Interceptor Version 2.3 Software Security Features

Network Integrity Systems is proud to announce the release of a major software upgrade to the Interceptor. The following is a description of the greatly enhanced security features offered with this revision.

Multiple Accounts and Local Authentication Database

Interceptor login access requires authentication against a local authentication database which stores encrypted passwords using a one-way hash for each login account. The hashing algorithm for the storage of the passwords uses an SHA512 digest.

The local authentication database allows for the definition of multiple accounts for login to the Interceptor. Each account defined in the Interceptor is assigned privileges relative to a role definition for Network (System Administration) and Monitoring functions. Network and Monitoring roles are assigned separately and are defined as per None, Operator, Admin, representing elevated levels of privilege.

Administration functions for the Interceptor Local Authentication Database allow the following user configuration operations on each account by an appropriately privileged user:

Define the user's real name on account creation
Change login user name
Change login password
Change Role assignment
Disable (lockout) or re-enable an account
Force a password change on next login

Password Policies

System wide password policies for all user accounts are configurable to provide the following capabilities:

Disable (lock out) an account after 3 consecutive failed logins.
Enable password expiration (also known as password aging).
Definition of the password expiration period.
Require the use of strong passwords. A strong password is defined as a password which is at least 10 characters long and contains at least 2 of: lower case letter, upper case letter, special character.
Prohibition of old passwords (also known as password history).
Configurable number of old passwords to remember.

Network Integrity Systems
1937 Tate Blvd SE
Hickory, NC 28602
Phone: 828.322.2181
Fax: 828.322.5294

info@networkintegritysystems.com
www.networkintegritysystems.com

We Bring Security To Light™

Pre-Login Banner Message

Pre-Login banner messages can be configured to display an appropriate message pertaining to unauthorized access or an acceptance of terms before logging in to an Interceptor. The configuration of whether the message is displayed and the content of the message are configurable.

Idle Session Timeout

To forcibly disconnect idle sessions, an idle session timeout can be configured. To accommodate specific idle timeout policies the idle session timeout period is configurable in minutes for durations from 1 minute to 24 hours.

Secure Shell (SSH) Protocol

To address privacy of network communications for login to the Interceptor, the Secure Shell protocol is supported as a replacement to the Telnet protocol. The SSH protocol is defined by two versions, of which the Interceptor only supports the more secure version 2.

When using an SSH enabled terminal emulation program the privacy via encryption that SSH protocol uses ensures that information likes passwords cannot be obtained by eavesdropping on a network connection.

SSH sessions are authenticated against the local authentication database of the Interceptor.

Network Access Control

The interceptor deploys network session and connection management methods to protect against simple denial-of-service or network intrusion attacks. TCP/IP connections (SSH or Telnet) are limited to 3 connections per minute. A maximum of 5 concurrent TCP/IP connections is allowed for inbound connections.

To constrain network access to authorized clients, network filtering by IP address or Ethernet MAC address is allowed. IP address filtering allows definition of addresses by single IP address, an address range specifying a start and end address, or an address range by specifying an IP address with subnet mask.

Network connections are immediately disconnected upon login authentication failure.

SNMPv3 Agent

The Interceptor uses licensed software components which embed the leading-edge SNMP agent EMANATE®/Lite from SNMP Research International, Incorporated. EMANATE®/Lite provides full support for the SNMPv3 protocol including the SNMPv3 privacy protocols of DES, 3DES, and AES.

Network Integrity Systems
1937 Tate Blvd SE
Hickory, NC 28602
Phone: 828.322.2181
Fax: 828.322.5294

info@networkintegritysystems.com
www.networkintegritysystems.com

To support SNMPv3 the SNMPv3 USM user database is administered and stored separately from the Interceptor local login authentication database. This measure ensures the local login authentication database cannot be manipulated via the SNMPv3 protocol.

Logging and Audit Trail

The Interceptor maintains log files in human readable format of all significant events. Interceptor operations distinguish between Network (System Administration) and Monitoring roles. Separate log files are maintained to keep the logging data for one role from being viewed by users who do not have the requisite role assigned to them. For example, a Monitoring operator cannot view the Network logs containing authentication result data. Further, to maintain the integrity of the logging audit trail, the contents of log files cannot be modified (i.e. deleted) by any level of user privilege.

To support redundant log collection, log data can be forwarded using the SYSLOG protocol to a remote syslog target. Log forwarding using SYSLOG protocol is configurable for each of the Network and Monitoring logs with each log type supporting: enablement, Remote Syslog Target specification, and Syslog Facility. The facility specification supports all 24 facilities as noted in RFC 3164.

Network logging details include: Login authentication events (e.g. successful login, bad password, account lockout), administrative changes to network configuration (including the local account database), blocked accesses by IP or MAC address filtering, and SNMP security violations.

Monitoring logging details include: Intrusion alarms and administrative changes to monitoring configuration.

NTP Client

Maintaining accurate time for event correlation is important. To ensure that the Interceptor is logging or reporting events with accurate timestamps, the configuration of time synchronization using the NTP protocol is fully supported.

Secure configuration from the factory

The Interceptor ships from the factory with defaults that represent a secure configuration. This secure configuration is represented as:

Single network administrator account with a well-known username and password. The password on this account that must be changed on first login and if desired the admin username can be changed and/or deleted and replaced with another.
Secure Password Policies including: strong passwords required, password expiration enabled, password history enabled with a history list of last 10 passwords.
SNMP agent is disabled.
Telnet access is disabled (SSH must be used for access from the network).

Network Integrity Systems
1937 Tate Blvd SE
Hickory, NC 28602
Phone: 828.322.2181
Fax: 828.322.5294

info@networkintegritysystems.com
www.networkintegritysystems.com

If such a secure configuration is undesired, the configuration can be adjusted to be less restrictive.

Factory Reset

The resetting of Interceptor configuration to a clean factory default is supported from the RS-232 serial console only. Should this capability be undesired, this feature may be disabled by an appropriately privileged administrator.

Certifications

Security software features for the Interceptor were developed in accordance with ISO 9001:2000 quality procedures.

The software development for v2.3 was performed using a rigorous cycle of requirements definition, design, design review, and implementation, design verification, and requirements validation. Implemented software is verified and validated against engineering and marketing requirements definitions. For the v2.3 software release, 144 design level requirements were met using a validation suite of 1274 tests.

Among others, SNMP Research uses the InterWorking Labs suite of tools for testing their products (EMANATE®/Lite) which are based on:

SNMPv2c (RFC-1902 through RFC-1908, and RFC 1901)
SNMPv3 (RFC-3410 to RFC-3418 and 3584)

Trademark Acknowledgements