

Intrusion Detection and Prevention Services and Device Configurations Supported in NSM

The Intrusion Detection and Prevention (IDP) device supports the following services in NSM:

- Inventory management service—NSM enables upgrading license and management of the IDP hardware details. Adding or deleting licenses or upgrading or downgrading software are not supported.
- Status monitoring service—Allows the IDP device’s status to be obtained, including name, domain, OS version, synchronization status, connection details, current alarms, CPU, memory, and swap.
- Logging service—Allows the IDP device’s logs to be obtained in a time-generated order. Logging configuration details that are set on the IDP device will apply to NSM.
- Packaging log files or debug files for remote analysis
- Managing interface settings such as setting IP addresses, settings IDP device host and network information, interoperability with NSM, Infranet Controllers, Secure Access devices, settings deployment mode, enabling layer 2 processing, and so on. For more information see the *ACM online Help*.

The following device configurations are not supported:

- Editing licensing information, although licenses can be viewed
- Rebooting the IDP device

On standalone IDP sensors and ISG security module settings inspects the following protocols using Table 1 .

Table 1: Intrusion Detection and Prevention: Supported Protocols

AIM	HTTP	Oracle	SMTP
CHARGEN	ICMP	POP3	SNMP/Trap
DHCP	IDENT	PortMapper	SQL Mon
DISCARD	IKE	RADIUS	SSH
DNS	IMAP	Rexec	SSL
ECHO	IRC	rlogin	Syslog
FINGER	LDAP	SunRPC	TELNET
FTP	LPR	Rsh	TFTP
GNUTELLA	MSN	RTSP	VNC
GOPHER	MSRPC	NBNAME	WHOIS

Table 1: Intrusion Detection and Prevention: Supported Protocols (continued)

GRE*	MS-SQL	NFS	Yahoo Messenger
H.225**	GTP	NNTOP	
	NTP	Rusers	
		SMB	

* GRE inspection are supported only for IP (protocol 0x0800) and PPP for CDMA A10 channel (protocol 0x8881). PPP is a Layer 2 protocol, which can carry any Layer 3 protocols. Within PPP, IDP inspects IP and Van Jacobson compressed TCP.

** Standalone IDP only.

Related Topics

- Adding Intrusion Detection and Prevention Clusters in NSM Overview
- Using Templates and Configuration Groups in NSM Overview
- NSM and Intrusion Detection and Prevention Device Management Overview

Published: 2009-08-20