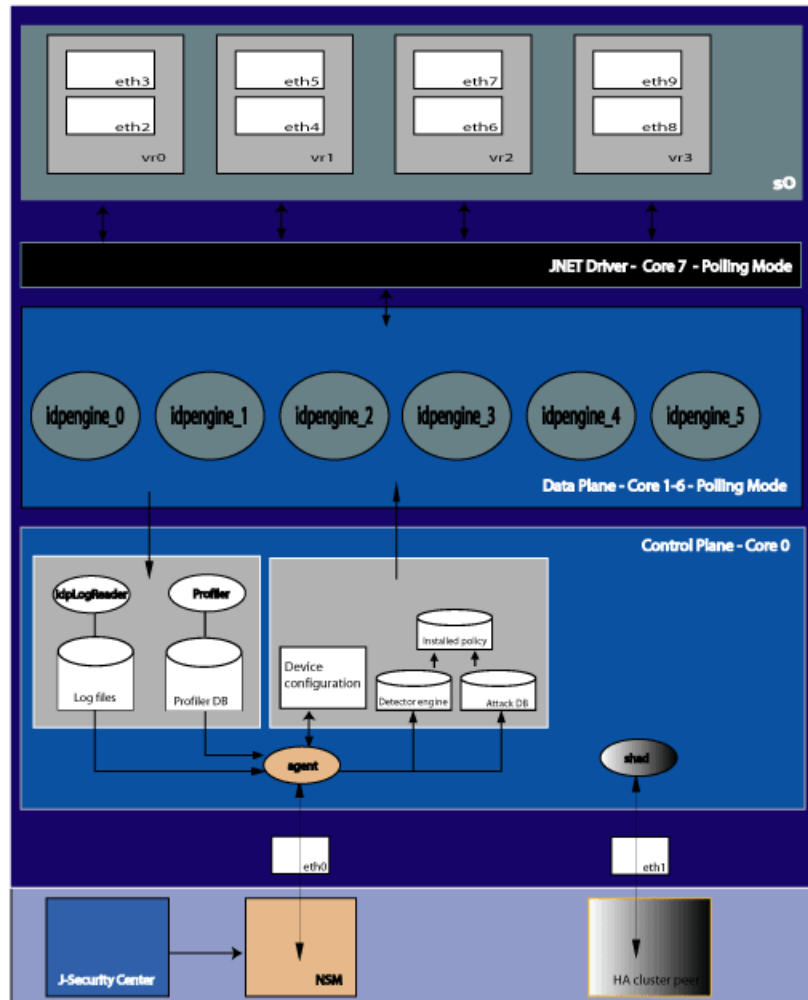


IDP Series Network Interfaces Overview

In Figure 1, eth0, eth1, eth2, eth3, and so forth are the IDP network interfaces.

Figure 1: IDP Network Interfaces



The following topics explain the features of these network interfaces:

- Management Interface (eth0) on page 2
- High Availability Interface (eth1) on page 2
- Traffic Interfaces on page 2
- Internal Bypass on page 3
- External Bypass on page 4
- Peer Port Modulation on page 5

Management Interface (eth0)

In Figure 1, eth0 is a dedicated management interface used for communication with Network and Security Manager (NSM). The agent process is a control plane process. It manages communication between the IDP appliance and NSM. The agent process handles the following functionality:

- Device configuration—You set part of the active configuration with the Appliance Configuration Manager (ACM), part with the CLI, and part with NSM. The agent process pushes changes you make from NSM to the IDP device.
- Security policy—You configure policies with NSM. You push a single policy to the IDP appliance to be installed and used by the IDP process engines. The installed policy is the policy used to determine which traffic the IDP process inspects, what to look for, and what actions to take.
- Detector engine—The IDP detector engine is a code base that contains the application signatures and protocol decoder definitions used by the IDP process engines in packet analysis. J-Security Center periodically updates the IDP detector engine. In Figure 1, note the process flow: first, you download updates from J-Security Center to NSM; then, you push updates from NSM to IDP appliances.
- Attack database—The attack database includes the attack objects used by the IDP rulebase to match attack signatures and protocol anomalies. J-Security Center updates predefined attack object definitions as often as necessary to provide zero-day coverage. As with detector engine updates, you download them from J-Security Center to NSM and then push them from NSM to the IDP appliance.
- Logging—The IDP process engines generate logs and packet captures related to security policy and application policy enforcement rules. The Profiler generates profiling and application volume logs. The agent process sends these logs to NSM so you can use NSM monitoring features to monitor security events and application usage.

High Availability Interface (eth1)

In Figure 1, eth1 is a dedicated high availability (HA) interface used for sync-state communication with a cluster peer in a high availability deployment. The shad process monitors the availability of the IDP node for HA purposes.



NOTE: High availability is not supported in the IDP 5.0 release.

Traffic Interfaces

In Figure 1, eth2, eth3, and so forth are the network interfaces you connect to the network devices that route traffic in your network.

The IDP Series implements the following abstract objects to manage network interfaces:

- Virtual circuit—A virtual circuit corresponds with the physical interface. For example, physical interface eth2 is a virtual circuit. You use the Appliance Configuration Manager (ACM) to configure speed and duplex, as well as optional interface alias settings for each interface.
- Virtual router—A virtual router contains a logical pair of virtual circuits. For example, virtual router vr0 contains eth2 and eth3. In transparent mode, traffic arrives in one interface and is forwarded through the other. You use ACM to configure the deployment mode (sniffer or transparent) and bypass options (internal, external, or off) for each virtual router. You can use the command-line interface to display information and status for each virtual router, including Address Resolution Protocol (ARP) and media access control (MAC) tables.
- Subscriber—A single subscriber named s0 contains all virtual routers. The subscriber maintains process and status of all traffic that flows through the device. You can use the command-line interface to view information and status maintained by subscriber s0. We test and support only configurations where the default subscriber is used.

Internal Bypass

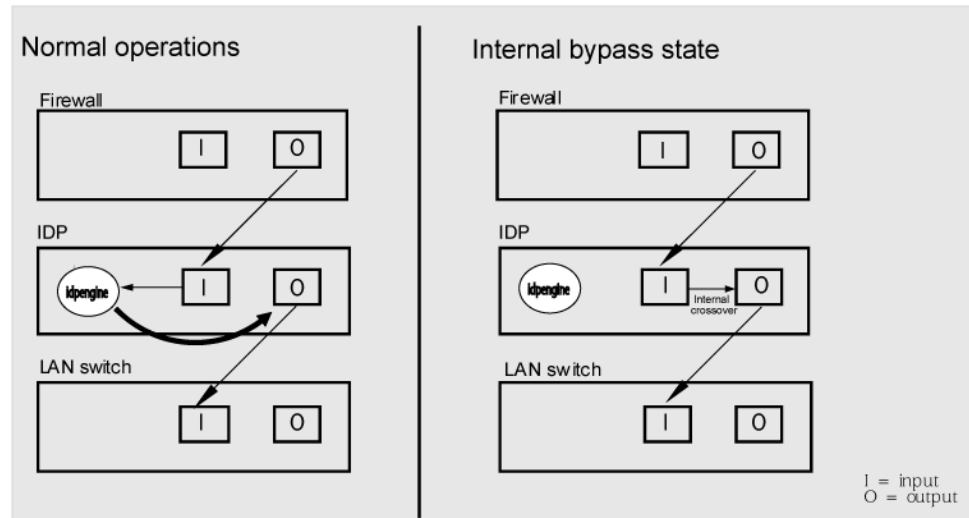
Physical interfaces are network interface cards (NICs). If your network security policy privileges availability over security, you can configure the interfaces to enter an internal bypass state in the event of failure or graceful shutdown. Internal bypass is also triggered when the JNET driver is in a state where it cannot receive packets.

In internal bypass, physical interfaces join mechanically to form a circuit that bypasses IDP processing. For example, if you configure internal bypass for vr0, and the IDP appliance encounters failure or is shut down, eth2 and eth3 join to form a circuit that avoids the IDP engine and forwards the traffic to the next network hop.

Internal bypass operates through a timing mechanism. When enabled, the timer on traffic interfaces counts down to a bypass trigger point. When the IDP appliance is turned on and available, it sends a reset signal to the traffic interface timer so that it does not reach the bypass trigger point. If the IDP operating system encounters failure, then it fails to send the reset signal, the timer counts down to the trigger point, and the traffic interfaces enter a bypass state. If the IDP appliance is shut down gracefully, the traffic interfaces immediately enter bypass.

Figure 2 shows the communications path when a virtual router is in internal bypass state.

Figure 2: Internal Bypass

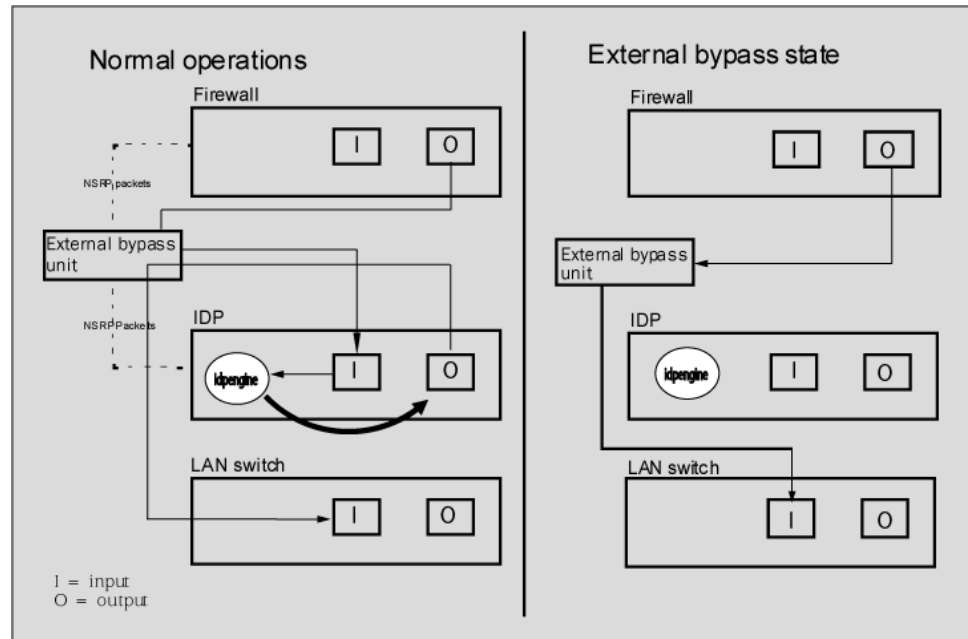


When the IDP operating system resumes healthy operations, it sends a reset signal to the traffic interfaces, and the interfaces resume normal operation.

External Bypass

External bypass operates according to the logic of a third-party external bypass unit. When the IDP appliance is turned on and available, it sends NetScreen Redundancy Protocol (NSRP) heartbeats to the external bypass unit. When the NSRP packets flow, the external bypass unit allows connections to proceed through the IDP appliance. If IDP encounters failure or is shut down, it cannot send the NSRP packets. IDP traffic interfaces enter a bypass state. When the external bypass unit detects this, it forwards packets around the IDP appliance, according to the rules you configure on the external bypass unit. See Figure 3.

Figure 3: Internal Bypass



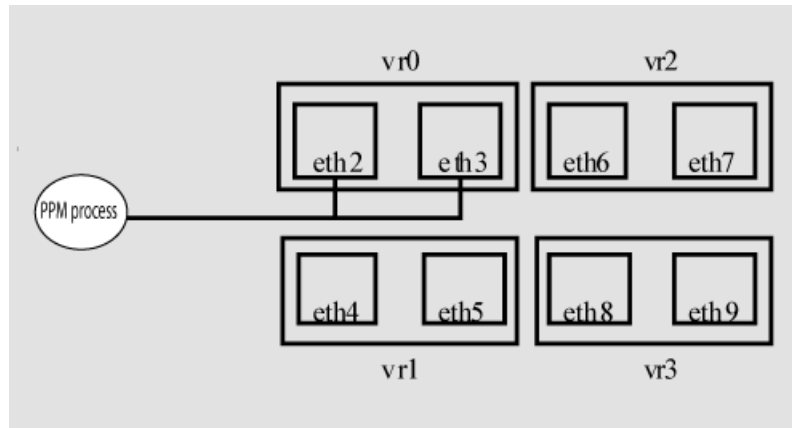
When the IDP appliance resumes healthy operations, it resumes sending NSRP packets. The external bypass unit detects this and allows connections to proceed through the virtual router.

Peer Port Modulation

The peer port modulation (PPM) feature supports deployments where routers monitor link state to make routing decisions. In these deployments, a router might be set to monitor link state on only one side of the IDP appliance. Suppose, for example, the router monitors only the IDP inbound interface. Suppose the inbound interface remains up but the outbound interface goes down. The router watching the inbound link would detect an available link and forward traffic to the IDP appliance. Traffic would be dropped at the point of failure—the outbound link. PPM propagates a link loss state for one traffic interface to all interfaces in the IDP virtual router.

When PPM is enabled, a PPM daemon monitors the health of IDP traffic interfaces belonging to the same virtual router. If a traffic interface loses link, the PPM process turns off any associated network interfaces in the same virtual router so that other network devices detect that the virtual router is down and route around it. For example, assume you have enabled PPM and configured IDP virtual routers as shown in Figure 4.

Figure 4: Peer Port Modulation



Suppose there is a network problem and eth3 goes down. The PPM daemon detects this and turns off the other interface in vr0: eth2. The interfaces in vr1, vr2, and vr3 are unaffected. After you fix the problem with eth3, the PPM daemon detects this, and turns on eth2.



NOTE: The PPM feature is independent of the bypass feature (NIC state setting). PPM is related to the *status of the link*, not the status of the IDP operating system. A link can be down even when the IDP operating system is healthy. Note, however, that PPM runs as a control plane process and operates only when the IDP appliance is turned on and the control plane is available. If the IDP operating system is unavailable, the PPM feature is also unavailable, regardless of the setting for the NIC state.

Related Topics The following related topics are included in the *IDP Concepts and Examples Guide*:

- IDP Series Operating System Overview
- Centralized Management with NSM Overview

The following related topics are included in the *IDP Administration Guide*:

- Configuring Virtual Routers (ACM Procedure)
- Tuning the JNET Driver Failure Count
- Configuring Interface Aliasing (ACM Procedure)

Published: 2010-03-15