WebSensing

# Security IP-Blocks

## Augment hardware designs with advanced network security features using WebSensing's reusable **Security IP-Blocks.**

The Web Sensing Security IP-blocks are a suite of reusable building blocks that can be used to augment new hardware designs with advanced network security features.

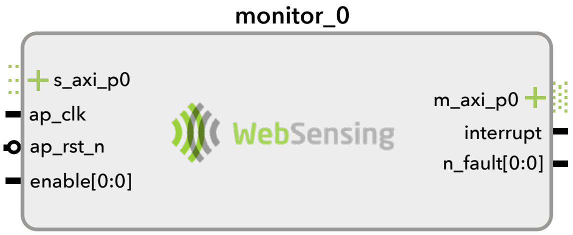
The IP-blocks are licensed through the standard Xilinx IP-block repository and accessible though the Vivado design tool suite. They can be used for any new hardware design employing Field Programmable Gate Array (FPGA) or System-on-Chip (SoC) devices, such as the Zynq-7000 and UltraScale MPSoC.

The suite includes a general Packet Inspection Engine (pie) capable of validating network traffic and protocols, with an associated Gigabit Ethernet PHY. When invalid traffic is detected, it can either be dropped from the network or some other action can be performed. The pie-block is customizable and can operate with manually crafted traffic parsers, grammars expressed in BNF using Bison, or both arbitrary binary grammars using Hammer combinators. A variant of the pie-block provides a general Data Diode capability.

The suite also includes line-speed AES-256 Encryption/Decryption blocks, certified under the NIST Cryptographic Algorithm Validation Program (CAVP), and SHA-256 Hashing capabilities.

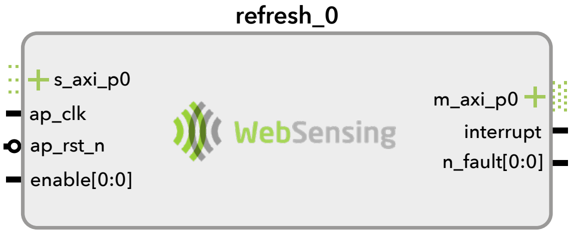
Web Sensing IP-blocks are highly customizable and can be adapted or configured to a wide variety of designer needs. For further information contact us through our web site at websensing.com.

| | |
|---|---|
| **PIE** | FPGA or SoC |
| **Gigabit Ethernet PHY** | FPGA or SoC |
| **AES-256** | FPGA or SoC |
| **SHA-256** | FPGA or SoC |
| **Network Diode** | FPGA or SoC |
| **Software Monitor** | SoC |
| **Software Refresh** | SoC |
| **Software Diversifier** | SoC |
| **Software Barrier** | SoC |



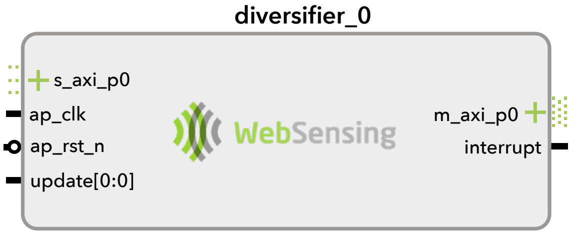
monitor

A *Software Monitor* block that continuously monitors the integrity of software to detect malicious, zero-day implants. This block can be hidden within an SoC on-chip FPGA hardware to monitor the Linux Kernel, device drivers, and/or applications running on the SoC processors.



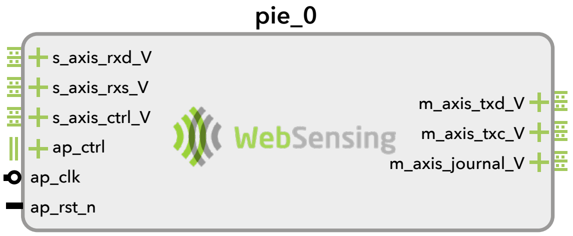
refresh

A *Software Refresh* block capable of restoring software to a "gold-standard" image thereby removing malicious implants.



diversifier

A *Software Diversifier* block capable of loading "diversified" software images thereby preventing re-infection. The images can be generated from source code using our compiler transformations.



pie

A *Software Barrier* block for isolating software memory regions and processes thereby providing cross-domain protections.