Product Overview

Enterprises and service providers alike are seeking to generate higher revenues in new and existing markets, while reducing costs. The Encryption Services PIC integrates IPsec encryption services onto Juniper Networks M Series Multiservice Edge Routers or Juniper Networks T Series Core Routers, allowing customers to securely transport traffic across untrusted third-party access networks, as well as public infrastructures. These integrated encryption capabilities, combined with the richness of MPLS, enable the deployment of new, value-added services while minimizing maintenance costs and overall operational expenditures.

Product Description

Juniper Networks® Encryption Services (ES) PIC integrates directly into M Series Multiservice Edge Routers and T Series Core Routers and provides IPsec encryption at rates exceeding 800 Mbps of throughput at full Data Encryption Standard (3DES)/Secure Hash Algorithm (SHA)-1 strength. The performance is complemented by a rich set of IPsec features whose packet processing tasks are easily handled by the ES PIC’s onboard processor, without affecting router forwarding performance. This scalability, combined with a rich feature set, enables you to offer a number of different services directly from the edge router, removing the need to deploy additional service creation devices. These services include secure access to MPLS VPNs, site-to-site managed IPsec VPNs, premium security of IPsec over MPLS VPNs, encrypted transit traffic across untrusted third-party wholesale networks, secure backhaul, and many other applications.

Architecture and Key Components

The ES PIC packs the processing power to enable M Series and T Series routers to terminate thousands of IPsec tunnels originating from various locations and provides encryption for any customer-facing or core interface on the router.

Encrypted Access Links

Encrypted access links are particularly useful for customers whose access links are provisioned by a third-party provider. The encrypted tunnel originates at the customer site, extends through the untrusted third-party network, and is terminated on the trusted provider’s access aggregation router. Traffic is forwarded in the clear across the provider’s private IP network, and then IPsec-encrypted when it leaves the provider backbone for the target subscriber site.

IPsec into Layer 3 2547 MPLS VPNs

You can use the ES PIC to terminate IPsec tunnels from customer sites and map all traffic into an RFC 2547bis VPN. This enables remote sites to securely access the corporate VPN, even when tunneling across third-party access networks or the Internet. The provider edge (PE) router terminates the IPsec tunnel from the remote site on the ES PIC, and then maps the IP traffic into an MPLS 2547 VPN, extending the reach of the provider VPN.

Premium Security: Encrypted Traffic Within 2547 VPNs

Some users have extremely high security requirements and require IPsec encryption of traffic within a Layer 3 2547 VPN. In this case, the ES PIC receives inbound traffic in the clear (or IPsec-encrypted), encrypts it, and then maps it into a 2547 VPN.
Encrypted Backhaul Traffic and Wholesale Transit Traffic

The ES PIC can be used for encrypting backhaul traffic for transport across third-party wholesale networks. Traffic is decrypted by the provider’s router, which terminates the tunnel. In this case, the originating ES PIC is deployed in a router that receives aggregated traffic from the provider’s customer access links. Alternatively, you can set up encrypted tunnels across networks as part of an IPsec VPN service or to offer a “carrier-of-carrier” IPsec virtual private network service.

Secure Analysis

To enhance the operational efficiency, you can gather traffic analysis data at the routers and forward it to collection points or network operation centers (NOCs). Traffic statistics are collected on access links to measure the volume of subscriber traffic, to develop subscriber traffic profiles, or to implement usage-based billing for premium services. IPsec plays an essential role in supporting these applications by enabling the secure transport of sensitive traffic analysis data. In these applications, the encrypted tunnel originates at an IPsec-capable device, extends across the network, and terminates at the collection point in the NOC.

Features and Benefits

Router Integration

The ES PIC integrates directly into the edge router, enabling IPsec termination directly in the edge router without additional equipment. Additionally, this allows for tight integration with other edge router services, such as MPLS VPNs.

Modular Scalability

Each ES PIC supports up to 1,024 static or 512 dynamic IPsec tunnels. A single ES PIC provides IPsec support for all interfaces in the same chassis without restriction. Multiple ES PICs can be accommodated in a single chassis, allowing deployments to scale gracefully when high-density implementations are needed.

Data Origin Integrity

The ES PIC provides data integrity, data origin authentication, anti-replay service, and confidentiality. The ES PIC supports tunnel mode with a choice of Authentication Header (AH), Encapsulating Security Payload (ESP), or AH and ESP combined to provide configuration flexibility. Each protocol provides data origin authentication and anti-replay service to prevent man-in-the-middle attacks.

Routed IPsec Tunnels

The ES PIC supports dynamic routing protocols directly over IPsec tunnels. When a new host behind the IPsec endpoint is added to the IPsec VPN, it will automatically be reachable by other hosts through the routes learned via the routing protocol running over the IPsec tunnel (using it as link). This dramatically reduces operational costs, as there is now no requirement to change configuration (access-list) each time a new host is added to the VPN. The ES PIC also supports dynamic routing protocols over IPsec over generic routing encapsulation (GRE) tunnels.

Security Association Management

Secure keys are automatically generated and exchanged in accordance with Internet Key Exchange (IKE), part of the IPsec framework. In addition to pre-shared keys, X.509 digital certificates are supported for automated operations and reduced operational costs. PKI online enrollment is supported by providing new certificates online as certificates expire, further reducing the costs of managing a large number of endpoints.

High Availability

The ES PIC has been designed with carrier class deployments in mind and can be configured for automatic stateful failover to a standby ES PIC. When the primary ES PIC experiences a failure, the backup becomes active, inherits all tunnels and security associations (SAs), and acts as the new next hop for IPsec traffic—no tunnel renegotiation is required. In addition, the ES PIC supports a back-up tunnel configuration that uses dead peer detection (DPD) to detect an endpoint failure and switch to a new tunnel.

Multicast over IPsec Tunnels

The ES PIC supports streaming and content delivery over secure connections, opening the way for a range of value-added services. As more and more content is distributed via multicast, this provides a new premium security multicast service opportunity.

Monitoring and Statistics

The ES PIC collects and analyzes an array of performance statistics to enable network visibility, improve planning, and ensure the integrity of security associations. These include statistical reporting for input and output bytes per tunnel, as well as for authentication failures, anti-replay failures, and other errors per PIC.

IPsec Integration with MPLS

The ES PIC works in conjunction with MPLS for the creation of new services. The ES PIC supports the termination of IPsec into the VPN routing and forwarding table (VRF) of an MPLS VPN. This allows customers to use IPsec to tunnel into an MPLS VPN over a public infrastructure or an untrusted third-party access network. The ES PIC also supports IPsec over an MPLS VPN as a way of providing premium level security for customers who have highly sensitive data. Finally, customers who desire to secure MPLS label addressing can be offered MPLS over GRE over IPsec.

Many of the world’s largest service providers have already deployed Juniper Networks routers as a dedicated access and VPN solution on the strength of the portfolio’s exceptional scale and stability. The ES PIC coupled with the interface density supported by M Series and T Series routers enables you to support thousands of IPsec tunnels terminating into a single PE router.
Features and Benefits

<table>
<thead>
<tr>
<th>Feature</th>
<th>Feature Description</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routed IPsec tunnels</td>
<td>Run routing protocols directly over IPsec tunnels</td>
<td>Routes to new endpoints for the VPN are automatically learned by all other endpoints, reducing operational costs.</td>
</tr>
<tr>
<td>Static and dynamic SA support</td>
<td>• Configurable SA lifetime&lt;br&gt;• Anti-replay, counter and log support for anti-replay</td>
<td>Enhances interoperability and increases configuration flexibility.</td>
</tr>
<tr>
<td>Multicast over IPsec tunnels</td>
<td>Secure multicast IPsec tunnel connections</td>
<td>Enables streaming and content delivery services over secured connections.</td>
</tr>
<tr>
<td>High availability IPsec solutions</td>
<td>• ES PIC automatic stateful failover&lt;br&gt;• IPsec tunnel automatic failover with DPD</td>
<td>• Immediate failover of all IPsec tunnels to a backup ES PIC with no tunnel renegotiation required.&lt;br&gt;• Failure of remote endpoint can quickly be detected and traffic switched to a backup tunnel to avoid loss of data.</td>
</tr>
</tbody>
</table>

Specifications

System Requirements/Platforms Supported

ES PIC is supported on all M Series routers and T320 Core Routers.

- ES PIC on M7i and M10i routers requires Junos® operating system 6.0 or later.
- ES PIC on M40e routers requires Junos OS 5.2 or later.
- ES PIC on M320 routers requires Junos OS 6.2 or later.
- ES PIC on T320 routers requires Junos OS 6.0 or later.

Authentication Hash Algorithms (RFC 2403, 2404)

- MD5
- SHA-1, SHA-1-HMAC96

Encryption Algorithms (RFC 2405, 2410)

- Null
- DES (56 bit)
- 3DES (168 bit)

Security Associations

- Pre-shared Keys
- X.509 Digital Certificates
- PKI auto enrollment

IKE Exchange Modes

- Main/Aggressive mode supported for IKE SA setup
- Quick Mode supported for IPsec SA setup

LEDs

- Green: PIC is operating normally
- Off: PIC is not enabled

Agency Approvals

Safety

- CAN/CSA-C22.2 No. 60950-00/UL 60950—Third Edition, Safety of Information Technology Equipment
- EN 60950, Safety of Information Technology Equipment

EMC

- AS/NZS 3548 Class A (Australia / New Zealand)
- EN 55022 Class A Emissions (Europe)
- FCC Part 15 Class A (USA)
- VCCI Class A (Japan)

Immunity

- EN 61000-4-2 ESD
- EN 61000-4-3 Radiated Immunity
- EN 61000-4-4 EFT
- EN 61000-4-5 Surge
- EN 61000-4-6 Low Frequency Common Immunity

NEBS

- Designed to meet these standards
- GR-63-CORE: NEBS, Physical Protection
- GR-1089-CORE: EMC and Electrical Safety for Network Telecommunications Equipment
- SR-3580 NEBS Criteria Levels (Level 3 Compliance)

ETSI

- ETS-300386-2 Telecommunication Network Equipment Electromagnetic Compatibility Requirements

Juniper Networks Services and Support

Juniper Networks is the leader in performance-enabling services that are designed to accelerate, extend, and optimize your high-performance network. Our services allow you to maximize operational efficiency while reducing costs and minimizing risk, achieving a faster time to value for your network. Juniper Networks ensures operational excellence by optimizing the network to maintain required levels of performance, reliability, and availability. For more details, please visit [www.juniper.net/us/en/products-services](http://www.juniper.net/us/en/products-services).
## Ordering Information

<table>
<thead>
<tr>
<th>Model Number</th>
<th>Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PE-ES-800</td>
<td>IPsec Processing Services PIC, 800 Mbps</td>
<td>M7i, M10i</td>
</tr>
<tr>
<td>PB-ES-800</td>
<td>IPsec Processing Services PIC, 800 Mbps</td>
<td>M40e, M320, T320, T640</td>
</tr>
</tbody>
</table>

## About Juniper Networks

Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks delivers the software, silicon and systems that transform the experience and economics of networking. The company serves customers and partners worldwide. Additional information can be found at [www.juniper.net](http://www.juniper.net).