IPSec Security Associations and the Security Association Database (SAD); Security Policies Security Policy Database (SPD); Selectors; the Security Parameter Index (SPI)

Woah, there sure is a lot of "security" stuff in that topic title. Those items are all closely related, and important to understand before w looking at the core IPSec protocols themselves. These constructs are used to guide the operation of IPSec in a general way and alsc exchanges between devices. They control how IPSec works and ensure that each datagram coming into or leaving an IPSec-capabl properly treated.

Where to start… where to start. ☺ Let's begin by considering the problem of how to apply security in a device that may be handling r exchanges of datagrams with others. There is overhead involved in providing security, so we do not want to do it for every message or out. Some types of messages may need more security, others less. Also, exchanges with certain devices may require different pro others.

Security Policies, Security Associations and Associated Databases

To manage all of this complexity, IPSec is equipped with a flexible, powerful way of specifying how different types of datagrams shou To understand how this works, we must first define two important logical concepts:

- **Security Policies:** A *security policy* is a rule that is programmed into the IPSec implementation that tells it how to process diffe datagrams received by the device. For example, security policies are used to decide if a particular packet needs to be processe not; those that do not bypass AH and ESP entirely. If security is required, the security policy provides general guidelines for hov provided, and if necessary, links to more specific detail.

  Security policies for a device are stored in the device's *Security Policy Database (SPD)*.

- **Security Associations:** A *Security Association (SA)* is a set of security information that describes a particular kind of secure c between one device and another. You can consider it a "contract", if you will, that specifies the particular security mechanisms f for secure communications between the two.

  A device's security associations are contained in its *Security Association Database (SAD)*.

It's often hard to distinguish the SPD and the SAD, since they are similar in concept. The main difference between them is that secur are general while security associations are more specific. To determine what to do with a particular datagram, a device first checks th security policies in the SPD may reference a particular security association in the SAD. If so, the device will look up that security ass use it for processing the datagram.

support!

Donate $2 Donate $5 Donate $10 Donate $20 Donate $30 Donate: $

Home - Table Of Contents - Contact Us

The TCP/IP Guide (http://www.TCPIPGuide.com)
Version 3.0 - Version Date: September 20, 2005