**IPSec**

In [computing](https://en.wikipedia.org/wiki/Computing), **Internet Protocol Security** (**IPsec**) is a network [protocol suite](https://en.wikipedia.org/wiki/Protocol_suite) that [authenticates](https://en.wikipedia.org/wiki/Authentication) and [encrypts](https://en.wikipedia.org/wiki/Encryption) the [packets](https://en.wikipedia.org/wiki/Packet_(information_technology)) of data sent over a network. IPsec includes protocols for establishing [mutual authentication](https://en.wikipedia.org/wiki/Mutual_authentication) between agents at the beginning of the session and negotiation of [cryptographic keys](https://en.wikipedia.org/wiki/Key_(cryptography)) to use during the session. IPsec can protect data flows between a pair of hosts (*host-to-host*), between a pair of security gateways (*network-to-network*), or between a security gateway and a host (*network-to-host*).[[1]](https://en.wikipedia.org/wiki/IPsec#cite_note-rfc2406-1) Internet Protocol security (IPsec) uses cryptographic security services to protect communications over Internet Protocol (IP) networks. IPsec supports network-level peer authentication, data-origin authentication, data integrity, data confidentiality (encryption), and replay protection.

IPsec provides two choices of security service: Authentication Header (AH), which essentially allows authentication of the sender of data, and Encapsulating Security Payload (ESP), which supports both [authentication](https://searchsecurity.techtarget.com/definition/authentication) of the sender and encryption of data as well. The specific information associated with each of these services is inserted into the packet in a header that follows the IP packet header. Separate key protocols can be selected, such as the ISAKMP/Oakley protocol.

Modes of operation

*The IPsec protocols AH and ESP can be implemented in a host-to-host* ***transport*** *mode, as well as in a* ***network tunneling mode****.*

### Transport mode

In transport mode, only the payload of the IP packet is usually [encrypted](https://en.wikipedia.org/wiki/Encrypted) or authenticated. The routing is intact, since the IP header is neither modified nor encrypted; however, when the [authentication header](https://en.wikipedia.org/wiki/Authentication_Header) is used, the IP addresses cannot be modified by [network address translation](https://en.wikipedia.org/wiki/Network_address_translation), as this always invalidates the [hash value](https://en.wikipedia.org/wiki/Hash_value). The [transport](https://en.wikipedia.org/wiki/Transport_layer) and [application](https://en.wikipedia.org/wiki/Application_layer) layers are always secured by a hash, so they cannot be modified in any way, for example by [translating](https://en.wikipedia.org/wiki/Port_address_translation) the [port](https://en.wikipedia.org/wiki/TCP_and_UDP_port) numbers.

A means to encapsulate IPsec messages for [NAT traversal](https://en.wikipedia.org/wiki/NAT_traversal) has been defined by [RFC](https://en.wikipedia.org/wiki/Request_for_Comments) documents describing the [NAT-T](https://en.wikipedia.org/wiki/NAT-T) mechanism.

### Tunnel mode

In tunnel mode, the entire IP packet is encrypted and authenticated. It is then encapsulated into a new IP packet with a new IP header. Tunnel mode is used to create [virtual private networks](https://en.wikipedia.org/wiki/Virtual_private_network) for network-to-network communications (e.g. between routers to link sites), host-to-network communications (e.g. remote user access) and host-to-host communications (e.g. private chat).[[25]](https://en.wikipedia.org/wiki/IPsec#cite_note-25)

Tunnel mode supports NAT traversal.

# Secure Electronic Transaction

**Secure Electronic Transaction** (**SET**) was a [communications protocol](https://en.wikipedia.org/wiki/Communications_protocol) standard for securing [credit card](https://en.wikipedia.org/wiki/Credit_card) transactions over insecure [networks](https://en.wikipedia.org/wiki/Computer_network), specifically, the [Internet](https://en.wikipedia.org/wiki/Internet). SET was not itself a [payment system](https://en.wikipedia.org/wiki/Payment_system), but rather a set of security protocols and formats that enabled users to employ the existing credit card payment infrastructure on an open network in a secure fashion. However, it failed to gain attraction in the market. VISA now promotes the [3-D Secure](https://en.wikipedia.org/wiki/3-D_Secure) scheme.

## Participants

A SET system includes the following participants:

* Cardholder
* Merchant
* Issuer
* Acquirer
* Payment gateway
* Certification authority

### How it Works

Both cardholders and merchants must register with CA (certificate authority) first, before they can buy or sell on the Internet. Once registration is done, cardholder and merchant can start to do transactions, which involve 9 basic steps in this protocol, which is simplified.

1. Customer browses website and decides on what to purchase
2. Customer sends order and payment information, which includes 2 parts in one message:
   1. a. Purchase Order – this part is for merchant
   2. b. Card Information – this part is for merchant’s bank only.
3. Merchant forwards card information (part b) to their bank
4. Merchant’s bank checks with Issuer for payment authorization
5. Issuer send authorization to Merchant’s bank
6. Merchant’s bank send authorization to merchant
7. Merchant completes the order and sends confirmation to the customer
8. Merchant captures the transaction from their bank
9. Issuer prints credit card bill (invoice) to customer

## Dual signature

As described in (Stallings 2000):

An important innovation introduced in SET is the *dual signature*. The purpose of the dual signature is to link two messages that are intended for two different recipients. In this case, the customer wants to send the order information (OI) to the merchant and the payment information (PI) to the bank. The merchant does not need to know the customer's credit-card number, and the bank does not need to know the details of the customer's order. The customer is afforded extra protection in terms of privacy by keeping these two items separate. However, the two items must be linked in a way that can be used to resolve disputes if necessary. The link is needed so that the customer can prove that this payment is intended for this order and not for some other goods or service.

The message digest (MD) of the OI and the PI are independently calculated by the customer. The dual signature is the encrypted MD (with the customer's secret key) of the concatenated MD's of PI and OI. The dual signature is sent to both the merchant and the bank. protocol arranges for the merchant to see the MD of the PI without seeing the PI itself, and the bank sees the MD of the OI but not the OI itself. The dual signature can be verified using the MD of the OI or PI. It doesn't require the OI or PI itself. Its MD does not reveal the content of the OI or PI, and thus privacy is preserved.

# Stateful firewall

In computing, a **stateful firewall** is a [network firewall](https://en.wikipedia.org/wiki/Firewall_(networking)) that tracks the operating state and characteristics of network connections traversing it. The firewall is configured to distinguish legitimate packets for different types of connections. Only packets matching a known active connection are allowed to pass the firewall.

Stateful packet inspection (SPI), also referred to as dynamic packet filtering, is a security feature often included in business networks.

**Stateful inspection**, also known as [dynamic packet filtering](https://searchnetworking.techtarget.com/definition/dynamic-packet-filter), is a firewall technology that monitors the state of active connections and uses this information to determine which network packets to allow through the firewall.

#### Stateful vs. Stateless Firewalls

A firewall can be described as being either Stateful or Stateless.

**STATELESS Firewalls**

Stateless firewalls watch network traffic and restrict or block packets based on source and destination addresses or other static values. **They’re not ‘aware’ of traffic patterns or data flows.** A stateless firewall uses simple rule-sets that do not account for the possibility that a packet might be received by the firewall ‘pretending’ to be something you asked for.

A stateless firewall filter, also known as an access control list (ACL), does not statefully inspect traffic. Instead, it evaluates packet contents statically and does not keep track of the state of network connections.

*Purpose of Stateless Firewall Filters*

The basic purpose of a stateless firewall filter is to enhance security through the use of packet filtering. Packet filtering enables you to inspect the components of incoming or outgoing packets and then perform the actions you specify on packets that match the criteria you specify. The typical use of a stateless firewall filter is to protect the Routing Engine processes and resources from malicious or untrusted packets.

**STATEFUL Firewall**

Stateful firewalls can watch traffic streams from end to end. They are aware of communication paths and can implement various IP Security (IPsec) functions such as tunnels and encryption. In technical terms, this means that stateful firewalls can tell what stage a TCP connection is in (open, open sent, synchronized, synchronization acknowledge or established). It can tell if the MTU has changed and whether packets have fragmented. etc.

Neither is really superior and there are good arguments for both types of firewalls. Stateless firewalls are typically faster and perform better under heavier traffic loads. Stateful firewalls are better at identifying unauthorized and forged communications.

# SYN Attack

## Definition - What does *SYN Attack* mean?

A SYN attack is a type of denial-of-service (DoS) attack in which an attacker utilizes the communication protocol of the Internet, TCP/IP, to bombard a target system with SYN requests in an attempt to overwhelm connection queues and force a system to become unresponsive to legitimate requests.

A SYN attack is also known as a TCP SYN attack or a SYN flood.

## Techopedia explains *SYN Attack*

The easiest way to describe how a SYN attack works is to think about your local grocer with the ticket system to serve customers at the meat counter. Any new customer is expected to pull a new, numbered ticket from the dispenser so the grocer can service the line-up of customers in an orderly fashion.

Normally, this system works well. The grocer notes what ticket number is to be serviced next, calls out that number, the customer answers and the transaction is begun.

However, imagine if a large number of customers took tickets and the grocer patiently started calling out numbers only to have no customers respond. He would probably wait a minute or two and call another number. Eventually the whole system would break down with no transactions occurring because the grocer is too busy trying to figure out who to service.

This is the same process as a SYN attack. An attacker would send an initial request (a SYN) asking for acknowledgment from the receiving server (an ACK). The receiving server would place this in a queue with identifying information, using a small amount of memory and resources to do so. The server would expect a quick return from its acknowledgment but the attacker would not do so - or simply not respond. The server would wait for a pre-defined timeout period to discard the connection request.

In the meantime, if a large number of these requests had been hitting the server, it would eventually become overwhelmed and unresponsive.

What is important to understand about SYN attacks is the attacker does not have to use a very powerful system or large bandwidths to accomplish an attack. In fact, a typical home PC with a dial-up connection can generate sufficient activity to bring down whole websites. Couple this with the idea of distributed attacks, where malware infects a large number of computers, and it is possible to see how easy it is to cause large problems.

As a result, there is a large body of "best practices" on how to prevent this including appliances specifically designed to identify and strip out packets in a SYN flooding attack.