IPsec

NEXT

Video – IPsec Concepts

In the previous topic you learned about types of VPNs. It is important to understand how IPsec works with a VPN.

Click Play in the figure for a video about IPsec.

NEXT

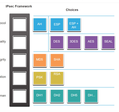
IPsec Technologies

IPsec is an IETF standard (RFC 4301) that defines how a VPN can be secured across IP networks. IPsec protects and authenticates IP packets between source and destination devices. IPsec provides these security functions:

Using the IPsec Framework, IPsec provides these security functions:

- **Confidentiality** - IPsec uses encryption algorithms to prevent unauthorized from reading the packet contents.
- **Integrity** - IPsec uses hashing algorithms to ensure that packets have not been altered between sender and receiver.
- **Origin authentication** - IPsec uses the Internet Key Exchange (IKE) protocol to authenticate users or end devices. Methods of authentication including using pre-shared keys (passwords), digital certificates, or RSA certificates.
- **Diffie-Hellman** - IPsec uses Diffie-Hellman to establish a shared key over the IP link.

IPsec is not bound to any specific cipher suite, encryption algorithm, or hash function. IPsec provides a framework that allows IPsec to easily integrate new security technologies without updating the existing IPsec standards. The currently selected technologies are singled to their specific security functions. The open-source strongSwan IPsec Framework implements the IPsec standards and is a free software suite that runs on Linux and other UNIX-like operating systems.



The security functions are listed in the table.

IPsec Function	Description
IPsec Protocol	The choices for IPsec Protocol include Authentication Header (AH) or Encapsulation Security Protocol (ESP). AH authenticates the user's source. ESP authenticates the user's source and encrypts the data. ESP is more secure than AH and currently recommended. Internet Key Exchange (IKE) is a hybrid protocol that provides utilities and services for Internet Security Association and Key Management Protocol (ISAKMP). These IKE (IKEV2), Advanced Encryption Standard (AES), Secure Hash Algorithm/Digital Signature Algorithm (SHA), for encryption is also an choice.
Confidentiality	Ensures that data arrives unchanged at the destination using a hash algorithm. Common hash algorithms are Message Digest 5 (MD5) and SHA.
Integrity	Ensures that data arrives unchanged at the destination using a hash algorithm. Common hash algorithms are Message Digest 5 (MD5) and SHA.
Authentication	Ensures data origin authentication using pre-shared keys (passwords), digital certificates, or RSA encrypted nonces (numbers used once). Pre-shared keys (passwords) are stored in plaintext. Digital certificates are signed certificates using the Rivest, Shamir, and Adleman (RSA) algorithm.
Diffie-Hellman	IPsec uses the DH algorithm to provide a public key exchange method for two peers to establish a shared secret key. The DH algorithm is a public key cryptography exchange that creating DH 1, 2, 5, and DH 14. DH 1 and DH 2 are considered weak and should not be used. DH 5 and DH 14 are considered strong.

The figure shows examples of the two different implementations. At DH is the hash building block of IPsec. When establishing a VPN link, the peers must share the same set of matching key exchange parameters, establish a shared key, authenticate each other, and negotiate the encryption parameters. Notice that AH doesn't use encryption.

IPsec Security Association Examples

NEXT

IPsec Protocol Encapsulation

Choosing the IPsec protocol encapsulation is the first building block of the framework. IPsec encapsulation packets using Authentication Header (AH) or Encapsulation Security Protocol (ESP). The choice of the ESP encapsulation which which authentic.

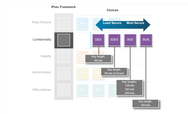
- AH is appropriate only when confidentiality is not required or permitted. It provides data authentication and integrity, but it does not provide data confidentiality.
- ESP is more secure than AH and is currently recommended.
- ESP provides both confidentiality and authentication. Its ciphers and hashes are more secure than those used in the other two protocols. Its authentication and integrity services are optional. ESP provides authentication and integrity services only if one of the authentication or integrity services is selected.
- ESP provides only confidentiality if no authentication or integrity services are selected.

NEXT

Confidentiality

Confidentiality is achieved by encrypting the data, as shown in the figure. The degree of confidentiality depends on the encryption algorithm and the length of the key used in the encryption algorithm. Cryptanalysis is the process of finding the key that is used to encrypt the data so that it can be read by an unintended recipient. The time it is possible all the possibilities in a function of the encrypted cipher of the obtaining decrypted. The time it takes to decrypt the data depends on the key length. For example, a 56-bit key can have approximately one and a number with a relatively supercomputer computer. A 128 bit key with the same machine can take roughly 2^72 or 72 quintillion years to decrypt.

The encryption algorithms highlighted in the figure are all symmetric key cryptosystems.



- DES uses a 56-bit key and should be avoided.
- 3DES is a cipher that for 56-bit DES. It uses three independent 56-bit encryption keys and 168 bit key, which provides significantly stronger encryption strength than DES. 3DES is considered to be a strong encryption algorithm.
- AES offers a stronger encryption than DES and is currently recommended. Advanced Encryption Standard (AES) uses a cryptographic key to convert data into a form that only someone with the proper key can read. Unlike DES, AES offers 128-, 192-, and 256-bit key options. AES cipher is strongest cipher continuously rather than encrypting blocks of data. 192-bit and 256-bit are considered to be very secure.

NEXT

Integrity

Data integrity means that the data that is received is exactly the same data that was sent. Potentially, data could be intercepted and modified. For example, in the figure, assume Alice's check for $100 is written to Bob. The check is then intercepted by Jack. Jack changes the check to read $1000 and then cashes the check. Bob is shocked to learning that the amount on the check is $1,000 and demands to cash it. Depending on the quality of the forgery or the artwork criteria, the attacker could be successful.

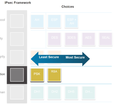
Note: Cisco now uses SHA-1 or legacy and recommends at least SHA-256 for integrity.

- Message Digest 5 (MD5) uses a 128-bit digest secret key. The sender-receiver message and 128-bit shared secret key are combined and run through the MD5 hash function. This creates a 128-bit message digest. The receiver then computes the message digest.
- The Secure Hash Algorithm (SHA) uses a 160-bit secret key. The sender-receiver message and the 160-bit shared secret key are combined and run through the SHA1 hash algorithm. The output is a 160-bit digest. The receiver then computes the message digest.

NEXT

Authentication

When contacting a particular long distance, you must know who is on the other end of the phone, which, in this, The same is true of IPsec peers. The device on the other end of the VPN tunnel must be authenticated before any communication is considered secure. The figure highlights the two peer authentication methods.



A pre-shared secret key (PSK) value is entered into each peer manually. The PSK is combined with other information to form the authentication key. PSKs are easy to configure manually, but do not scale well. Advanced Rivest Shamir Adleman keys are configured with the PSK or keys using peer with which it communicates.

Rivest, Shamir, and Adleman (RSA) encrypted nonces (numbers used once) are random numbers that are used in authentication. Nonces are exchanged in clear text. The nonces are used in derivation of keying material and authentication. RSA encrypted nonces provide a stronger form of authentication than pre-shared keys. The encryption keys are derived from the encrypted nonces, so the security of the key exchange is dependent on the strength of the encryption algorithm. The encryption keys are derived from the