Interoperability Issues for VPN IPsec Solutions

Iulian Danalachi, Mihai-Lucian Petrescu

Military Technical Academy
George Cosbuc Blvd., no. 81-83, Sector 5,
Bucharest, zip code 050141
ROMANIA
iulian.danalachi@gmail.com, mihai.petrescu@gmail.com

Abstract: An issue of testing that should be taken into consideration is the compatibility and interoperability of the IPsec components when implementing an IPsec solution. This article will guide us trough some key point introductive notions involved in the interoperability problem, we'll see a short overview of some of these problems and afterwards we will discuss about some of the testing solutions of IPsec interoperability that we should take into consideration.

Key-Words: IPsec, private networks, interoperability, testing, protocols

1. Introduction

IPsec is a collection of protocols that assist in protecting communications over IP networks [1]. In other words Internet Protocol Security ensures the security of a virtual private network over the internet. IPsec is one of the most used protocol for ensuring the authentication , confidentiality , and the integrity of the IP packets. IPsec protocols work together in various combinations to provide protection for communications. IPsec protocol work with a variety of standard cryptographic and process negotiation schemes, as for many security systems they include digital signatures and certificates, public keys infrastructure and authorizations. IPsec work by encapsulating the original packet in another IP packet, and then it creates a new header with the information needed by the other endpoint. IPsec is commonly used also for its interoperability, it can work with most systems and standards even in the same time with other VPN protocols. For example, IPsec can negotiate and authenticate encryption while a L2TP virtual private network receives a packet, creates a tunnel and send the encapsulated packet to the other endpoint.

This is a post conference paper. Parts of this paper have been published in the Proceedings of the 3rd International Conference on Security for Information Technology and Communications, SECITC 2010 Conference (printed version).

1.1 Involved protocols

IPsec uses an algorithm named Internet Key Exchange (IKE) for exchanging keys between the endpoints. IKE permits for the endpoints to negotiate keys in a secure manner using the ISAKMP protocols for creating Security Associations and OAKLEY which uses the Diffie-Hellman algorithm for exchanging the keys between endpoints. IKE can be used in conjunction with Kerberos, digital certificates X.509v3 or pre-shared keys.
Authentication Header AH provides integrity protection for all packet headers and data [2], with the exception of a few IP header fields that routinely change in transit. Ah can be attached to each datagram and contains a hash signature HMAC-MD5 or HMAC-SHA1.
Encapsulated Security Payload ESP encrypts the content of a packet in two ways : transport – it protects only the content not the header and tunnel- the entire packet is encrypted. ESP also uses HMAC MD5 and SHA1 functions for authentication and DES-CBC for the encryption.
Some of the benefits in using IPsec are that IPsec provides security directly on

ISSN 2067 – 4074

the IP network layer and secure everything that is put on top of the IP network layer. The protocol has also been an Internet standard for quite some time and has been proven to be a secure and trusted method of securing data. Another benefit is the IPsec support the use of multiple tunnels or nested tunnels, if a user must pass through two or more secure gateways the tunnels can be double encrypted.
Like any other VPN solution IPsec has some limitations, one of which is the interoperability issue, different IPsec implementations do not always meet the standard and communicate without problems with each other.

2. Interoperability issues

Although this problem is not new and there were some improvements in the industry it is well known that IPsec implementation will always have to face some challenges of interoperating between various implementations and vendors. One of these reasons is that many vendors offer IPclients and Gateways, the implementations of IPsec differ from product to product and this differences can lead to interoperability issues [2]. Even though the vendors say that their product is IPsec compliant which means that their product meet the current IETF IPsec standards, they may implement the standards in a different manner [2] which can cause problems that are subtle and hard to diagnose. Another reason is that many vendors offer additional functionalities to their products such as encryption algorithms, that are not a part of the IPsec standards from various reasons such as ease of use.
The problems of interoperability in IPsec VPNs can consist in some of these issues:

- Different authentication methods, encryption algorithms or compression algorithms are supported by the endpoints
- Certain digital certificate fields or data can be encoded or interpreted differently by the endpoints, or they could handle certificate extensions in a conflicting way
- The endpoint have different default parameters such as Diffie- Helman group 2 versus group 1
- The endpoints perform security associations rekeying in different ways because of the different interpretations and implementation of standards, different rekeying behavior can result in lost of traffic. Another issue regarding rekeying if time-related, by the means of where to start deleting the old security association and where to start using the new one. Some implementations of IPsec deletes all IPsec SAs after the IKE SA with which they were negotiated expires and other allow them to continue until they expire [2].
- In some cases regarding IKE negotiations some endpoints sends a notification message that it wants to start an IKE negotiation with an endpoint from whom it has no current security associations because the starting endpoint might be rebooted or it lost the previously negotiated SAs and if the other peer don't have this feature implemented there will be an interoperability issue
- Endpoints may be configured with different lifetime values for IKE or IPsec security associations [2]
- In some cases the IPsec implementation will delete a security association if no traffic is sent through it, even if the negotiated time did not expire. By using the dead peer detection and endpoint knows that its peer is able to communicate and receive accordantly the IPsec protected traffic that it sends. It is used to ensure that an unused SA is kept alive, this preventing the deletion of the inactive SAs.
- Usually the IPsec gateways implementations interoperate with others vendors implementations, but in some cases the clients can interoperate only with the vendors gateway implementations [2]

3. Testing solutions for IPsec interoperability

Interoperability is more difficult to achieve when higher level functions are required such as encryption key exchange and digital certificate validation checks. To gain an understanding of the broader questions of interoperability, there are a few good sources of information, one of which is the VPN Consortium.
The consortium is a trade association for VPN vendors that deal with interoperability issues. Members participate regularly in interoperability "bake-offs" to see how specific features of their VPN equipments work with equipment from other vendors [3].

The consortium tests VPN products for interoperability and compliance; in fact both logos commonly can be found on VPN equipments. A interoperability logo on a piece of VPN equipment means the vendor has demonstrated that that product interoperates with other products in the group's testing program. A compliance logo means that the product conforms to specific parts of the IPSec standard.
These are some test done by the VPN Consortium to assure VPN users that their IPsec Systems are interoperable with other IPsec systems [3] :

- Basic Interoperability - for an IPsec system to be interoperable with other IPsec system, it has to interoperate with at least three quarters of the other systems that are in the test. Interoperability is defined as creating a working IKE tunnel between the systems that normal IP traffic can flow through. The tunnel requires TripleDES for encryption, SHA-1 for hash, 1024-bit key exchange, and a preshared secret for authentication. As the term "Basic" implies, every IPsec implementation shipped today should have these features and should be able to interoperate with other IPsec systems [3].
- AES Interoperability -this test is almost identical to the Basic Interoperability Test, except that the encryption used in the systems is 128-bit AES. It is commonly believed that in the future AES will become the most popular algorithm for encryption.
- IKEv2 Basic Interoperability- this test assures VPN users that IPsec system that uses IKEv2 as gateways are generally interoperable with other IKEv2 systems. To pass, a system has to interoperate with all of the other systems that are in the test. Interoperability is achieved when we have created a working IKEv2 tunnel between the systems that normal IP traffic can flow through. The tunnel requires AES for encryption, SHA-1 for the hash and PRF, 1024-bit key exchange, and a preshared secret for authentication. As the term "Basic" implies, every IKEv2 implementation shipped today should have these features and should be able to interoperate with other IKEv2 systems.
- IPv6 Interoperability -The IPv6 Interoperability test is identical to the AES Interoperability Test, except that the systems use fixed IPv6 addresses for both the internal and external networks [3].
- Certificate Interoperability -The test assures VPN users that IPsec systems are generally interoperable with other IPsec systems when using PKIX certificates for authentication. The test is identical to the AES Interoperability Test, except that the systems use PKIX certificates for authentication [3].

Another source of information regarding interoperability is the ICSA Labs Web Site. In 1998 they established IPsec Product Certification Testing Program and the IPsec Products Developers Consortium which had as a primary focus the interoperability issues. The ICSA web site provides us a list of tested and certified products and the set of criteria's that a product has to meet to be certified [4].

ISSN 2067 – 4074

A few years back the National Institute of Standards and Technology provided us with a web platform which offered real time IPsec interoperability testing. The Nist IP Security Web Based Interoperability Tester called IPsec-Wit provides the ability to test IPsec implementations with the reference IPsec implementation at NIST. The testers could chose to negotiate a SA with the NIST implementation using the IKE or they could establish a security association with the NIST implementation [5]. From the user-related point of view this solution is accessible from remote locations, it is available at any time, it requires no modification to the tester's IPsec implementation, it allows tester to resume testing later and it is a configurable, easy to use and well documented solution. The current capabilities of the IPsec WIT are as fallows : the keys can be negotiated manually or through IKE negotiation, it uses configurable ports for IKE negotiation, peer authentication is made through pre-shared secrets, it uses MD5 or SHA or ISAKMP hash, and for encryption DES or 3DES, Diffie–Hellman exchange – First Oakley Group, the IPsec AH algorithms consist in using HMAC-MD5 or HMAC-SHA1 and the algorithms for IPsec ESP are for encryption DES, 3DES, IDEA, RC5, Blowfish or ESP-Null as for the authentication HMAC-MD5 or HMAC-SHA1, it uses variable key length for RC5 and Blowfish [5].
It is also well known that IPsec vendors themselves perform interoperability testing and make the results public through their web site. Most vendors also offer configuration guidelines so that their product can be configure to operate with the other common products, in this way facilitating the interoperability.

4 Conclusion

Interoperability issues do in fact exist and some of these issues can be solved or at least identified when designing the solution and especially when implementing and testing the prototype for an IPsec infrastructure. After deploying the solution we could also do some more testing using some online tools and of course we will always have to keep in mind the vendors specifications, notes, guidelines when were dealing with interoperability issues.

References

[1] RFC 2401, *Security Arhitecture for the Internet Protocol*, http://www.ietf.org/rfc/rfc2401.txt

[2] NIST, *Guide to IPsec VPNs*, Special Publication 800-77, 2005

[3] VPN Consortium Web site http://www.vpnc.org

[4] ICSA Lab Web site http://www.icsalab.com/ipsec

[5] NIST IP Security Web Based Interoperability Tester http://ipsec-wit.antd.nist.gov

[6] Jon C. Snader, *VPNs Illustrated – Tunnels, VPNs and IPsec*, Addison-Wesley Professional, 2005