

## IPSEC Remote Access Protocol Evaluation Criteria

### [1.](#) Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of [Section 10 of RFC2026](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts. Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/lid-abstracts.txt>.

To view the list Internet-Draft Shadow Directories, see <http://www.ietf.org/shadow.html>.

The distribution of this memo is unlimited.

### [2.](#) Copyright Notice

Copyright (C) The Internet Society (2000). All Rights Reserved.

### [3.](#) Abstract

This document describes criteria for evaluation of IPSEC Remote Access (IPSRA) protocols. In particular, this document focuses on criteria relevant to voluntary tunneling.

### [4.](#) Introduction

This document describes criteria for evaluation of IPSEC Remote Access (IPSRA) protocols. In particular, this document focuses on criteria relevant to voluntary tunneling.

---

INTERNET-DRAFT    IPSEC Remote Access Evaluation Criteria 21 November 2000

## [5.](#) Requirements language

In this document, the key words "MAY", "MUST", "MUST NOT", "optional", "recommended", "SHOULD", and "SHOULD NOT", are to be interpreted as described in [\[1\]](#).

Please note that the criteria specified in this document are to be used in evaluating protocol submissions. As such, the requirements language refers to capabilities of these protocols; the protocol documents will specify whether these features are required, recommended, or optional. For example, requiring that a protocol support confidentiality is NOT the same thing as requiring that all protocol traffic be encrypted.

A protocol submission is not compliant if it fails to satisfy one or more of the must or must not requirements for the capabilities that it implements. A protocol submission that satisfies all the must, must not, should and should not requirements for its capabilities is said to be "unconditionally compliant"; one that satisfies all the must and must not requirements but not all the should or should not requirements for its protocols is said to be "conditionally compliant."

## [6.](#) Overview

Requirements may be divided into several categories:

- Multi-protocol requirements
- Configuration requirements
- Overhead requirements
- PKI transition requirements
- Authentication requirements
- Accounting and auditing requirements
- Security requirements

### [6.1.](#) Multiprotocol requirements

With the widespread acceptance of IP, the usage of alternative protocols such as IPX, SNA, NetBEUI, and AppleTalk is declining rapidly. Thus while multi-protocol networks are still common today, this is not expected to be the case within five years. For those networks requiring multi-protocol support, alternatives are widely available, as described in [\[19\]](#) and [\[26\]](#). As a result, while an IPSEC remote access protocol MAY provide multi-protocol support, this is at best a minor objective, and protocol designers would be wise to optimize for IP.

Note that in order to provide for multi-protocol support, it is not necessary to encapsulate GRE or PPP within IPSEC. Rather, IPSEC can readily support multi-protocol tunneling via inclusion of the non-IP protocol number in the "Next Header" field of the AH or ESP header.

---

INTERNET-DRAFT    IPSEC Remote Access Evaluation Criteria    21 November 2000

Since multi-protocol use is declining rapidly, support for multi-protocol configuration such as what was provided in PPP, described in [16]-[18], is not a requirement for an IPSEC remote access protocol. Thus, it is feasible for an IPSEC remote access solution to focus solely on IP configuration mechanisms.

## [6.2.](#) Configuration requirements

The configuration requirements of a host with an IPSEC remote access interface are similar to those of a host needing to configure any other kind of interface. These include the need:

1. to obtain an IP address and other configuration parameters appropriate to the class of host
2. to reconfigure when required
3. to authenticate where required
4. to support address pool management
5. to support fail-over
6. to integrate with existing IP address management facilities such as DHCP
7. to maintain security and simplicity in the IKE implementation.

A configuration facility for IPSEC remote access MUST provide for both IP address assignment as well as configuration for a wide variety of parameters, such as those supported in DHCP [3]. Note that rich configuration facilities have already proved necessary in wide variety of cases outside of conventional LAN configuration. For example, in the case of PPP, IPCP, described in [4], was used to provide for IP address assignment. However, it was found that additional configuration parameters were necessary, so that non-standard extensions, described in [7] were developed. Rather than continuing down the road towards duplicating existing DHCP functionality, it was decided that it would be preferable to support DHCPINFORM capabilities, described in [3].

A configuration facility for IPSEC remote access SHOULD support the concept of a configuration lease, and MAY support the ability to force

reconfiguration of the client, in a manner such as that described in [14]. Configuration leases permit recovery of unused IP address space, and therefore result in more optimal use of addresses. The ability to force reconfiguration of the client can be useful in a number of circumstances, such as renumbering.

A configuration facility for IPSEC remote access MUST support the ability to authenticate the configuration conversation. As noted in [6], a number of security threats exist in IP address management, and so authentication may be desirable in order to mitigate these threats. Alternatively, it may be desirable to bind an IP address to a user or machine ID for the purposes of supporting policy-based networking. Note

that the need for authentication is particularly strong where forced reconfiguration is supported. Where DHCP authentication is implemented for these purposes, IPSEC remote access addressing SHOULD permit integration with DHCP authentication so as to permit universal coverage.

A configuration facility for IPSEC remote access SHOULD provide the ability to be able to obtain an IP address within the appropriate address pool. Today it is common to use distinct address pools for the purposes of service differentiation, and therefore the ability to obtain an address from the appropriate pool may be critical to the operation of the network. Methods for pool assignment include the user identity option as well as the user class option specified in [21].

A configuration facility for IPSEC remote access SHOULD NOT preclude the ability to provide for fail-over capabilities in terms of IP address management. With enterprise customers increasingly investing in IP address management systems with fail-over capabilities, creating additional pockets of addressing state creates the the need to provide those additional pockets with fail-over capabilities equivalent to those provided in DHCP fail-over, described in [8].

A configuration facility for IPSEC remote access MUST NOT compromise the simplicity or security of IKE, described in [12]. Since IKE is a key element of the Internet security architecture, it is critical to maintain inter-operability as well as the ability to predict and analyze the behavior of implementations.

### [6.3](#). Overhead requirements

Given the increasing popularity of IPSEC remote access, it is inevitable that this technology will be used in a wide variety of applications, including transport of voice and video. These applications typically involve transport of small payloads, and as a result the level of overhead introduced by an IPSEC remote access protocol is of concern.

It is possible that existing header compression schemes may be operating within an IPSEC remote access environment. These schemes are used to reduce the size of IP headers encapsulated within the IPSEC remote access headers. For example, the IP header compression scheme described in [23], or IPSEC minimal encapsulation, described in [22] may be in use. Where voice or video payloads are being carried within RTP, the IP/UDP/RTP compression scheme described in [24] may prove useful.

For the purpose of the comparisons that follow, the packet to be encapsulated by the IPSEC remote access protocol may be assumed to have been previously compressed by one of the above methods. For comparison purposes, overhead is calculated for a 700 octet packet as well as a 64 octet packet, In this calculation we assume an IP header of 20 octets,

a UDP header of 8 octets, an IPSEC header of 32 octets (corresponding to MD5 IPSEC AH) and (where applicable) an L2TP header of 8 octets. Overhead percentage is calculated as overhead/packet size.

As described below, for the case of the 64 octet packet, all known methods result in excessive overhead. Thus an IPSEC remote access protocol MAY provide additional mechanisms to reduce overhead in these scenarios.

#### [6.3.1.](#) IPSEC tunnel mode

In IPSEC tunnel mode, an IP header is used inside the IP and IPSEC headers. Thus, an IP packet would require an additional 52 octets of overhead for the addition of IP and IPSEC headers.

For a 64 octet packet, this results in overhead of 81.8%. For a 700 octet packet, overhead is 7.4%.

#### [6.3.2.](#) IPSEC/L2TP

L2TP, defined in [19], involves encapsulation of PPP within UDP and L2TP. Where IPSEC is used to provide security, 68 octets of overhead are

required.

For a 64 octet packet, this results in overhead of 106.3%. For a 700 octet packet, overhead is 9.7%.

#### [6.3.3.](#) IPSEC/L2TP with header compression

L2TP header compression, defined in [\[20\]](#), involves encapsulation of an L2TPHC header, which can be as small as a single octet, within IP. Thus where IPSEC is used to provide security, 53 octets of overhead are required.

For a 64 octet packet, this results in overhead of 82.8%. For a 700 octet packet, overhead is 7.6%.

#### [6.3.4.](#) IPSEC/L2TP with multiple PPP encapsulation

Using L2TP it is possible to include more than one PPP encapsulated frame within a single L2TP packet. This results in a reduction in overhead and attendant serialization time, at the expense of additional delay required to accumulate additional packets. Where the serialization time saved is greater than the additional delay, the tradeoff will be worthwhile. This is typically the case at bandwidths of less than 100 Kbps.

For the purposes of calculating overhead, let us assume that two 64 octet packets are bundled together. This results in overhead of 53.2%. For a 700 octet packet, overhead is 4.9%.

A summary of the overhead computed for each method is given below:

Protocol	Overhead w/ 64 octet packet	Overhead w/ 700 octet packet
----------	-----------------------------------	------------------------------------

IPSEC/L2TP	106.3%	9.7%
IPSEC/L2TP w/HC	82.8%	7.6%
IPSEC tunnel mode	81.8%	7.4%
IPSEC/L2TP w/ multiple PPP enc.	53.2%	4.9%

#### [6.5.](#) PKI transition requirements

An IPSEC remote access protocol MUST provide customers with the ability to deploy the solution securely without requiring that clients implement user certificates. An IPSEC remote access solution MUST support user authentication in the case where client and server machine certificates are present and SHOULD support user authentication in the case where only the server has a machine certificate, but the client does not have any certificate.

The transition to a PKI may be divided into several steps:

- a. Support for PKI on servers. This typically requires that machine certificates be deployed on the servers, along with appropriate certificate authorities and stores. It also requires that clients be capable of verifying the server's certificate against a current Certificate Revocation List (CRL). Since this will often require a client software upgrade, the work to transition to server certificates is comparable to the work required to deploy SSL/TLS-capable Web server and certificate-capable browsers.

Note that while some client software support for PKI must be



assumed, in this step, it is not necessary for the clients to obtain their own machine or user certificates. Thus it is possible for the clients to continue to authenticate using only legacy methods during this phase of the transition.

- b. Support for machine certificates on clients. This requires that machine certificates be deployed on clients. Completion of the previous step (a) often requires a client upgrade, which will typically also include support for client certificates. If the infrastructure for machine auto-enrollment has also been put in place as part of the server PKI rollout, then there may not be much additional work required to complete this step, above what was already required for the previous step. Note that if the client only supports a machine certificate, then this may imply the use of a non-PKI method for user authentication in addition to the machine certificate.
- c. Support for user certificates. This requires that user certificates be provided to users. Since storage of user certificates on the machine creates new vulnerabilities, smart-cards are typically be used to store the user certificates. Thus, a smart-card rollout may often be a prerequisite to deployment of user certificates. This in turn may require integration of smart-card provisioning with the existing identification system, such as the distribution of combined employee badge/smart-cards. Since this step may require considerable work above and beyond the tasks required to carry out transition steps a and b, support for legacy authentication methods will likely be required at least until this transition step is complete.

Thus, an IPSEC remote access solution **MUST** support transition step b, and **SHOULD** support transition step a.

#### [6.6.](#) Authentication requirements

An IPSEC remote access protocol **MUST** support user authentication and **MUST** offer compatibility with legacy authentication methods commonly in use today. This includes PPP authentication methods, described in [\[40\]](#). Note that since RADIUS, defined in [\[15\]](#), merely serves to encapsulate an authentication method, it does not itself constitute an authentication method.

Since support for a variety of authentication methods is already available within existing IETF standard frameworks such as such as GSS\_API [\[31\]](#), an IPSEC remote access protocol **SHOULD** support the GSS\_API authentication framework and **MAY** support other frameworks such as SASL

[30] or EAP [29].

Support for existing frameworks is important since creating new frameworks increases the complexity of developing new authentication methods and while also complicating their deployment. Rather than fragmenting the market while increasing the cost of development, a more useful approach is to unify the authentication frameworks, making it possible for developers to create authentication modules that will be usable in a variety of applications.

Work toward support of GSS\_API within other frameworks is already underway. For example, SASL, described in [30], already supports negotiation of GSS\_API as a method, as noted in [38]. Similarly, work on permitting GSS\_API to be used for initial authentication [41], has enabled GSS\_API support within EAP.

#### [6.7.](#) Accounting and auditing requirements

An IPSEC remote access protocol SHOULD support accounting and auditing. In order to support accounting, it is necessary to be able to accurately determine the duration of the IPSEC remote access session. Without a standardized IPSEC keep-alive this can prove difficult to achieve since security associations may remain in place after a client disconnect or crash.

#### [6.8.](#) Security requirements

##### [6.8.1.](#) Identity protection

An IPSEC remote access protocol MUST provide for identity protection. Since IKE Aggressive Mode exposes the user identity, an IPSEC remote access protocol MUST NOT rely on aggressive mode. For example, an IPSEC remote access solution MUST protect against man in the middle attacks without requiring the use of Aggressive Mode.

Note that main mode with signature authentication is secure against passive attacks but not active attacks.

##### [6.8.2.](#) Denial of service attacks

Denial of service attacks can be characterized based on the capabilities of the attacker:

1. Attackers that can send and receive IP-address spoofed messages corresponding to one real party in the attack.

2. Attackers that can only send IP-address spoofed messages corresponding to one real party in the attack (but not receive).

---

INTERNET-DRAFT    IPSEC Remote Access Evaluation Criteria 21 November 2000

3. Attackers that can gain physical access to the device being attacked.

An IPSEC remote access protocol MUST provide protection against attacks in categories 1 and 2. Attackers in category 3 are able to deny service without having to attack on the wire protocols, so that there is little that can be done to deter them within an IPSEC remote access protocol.

#### [6.8.3.](#) Man-in-the-middle attacks

Use of pre-shared keys in main mode is vulnerable to man-in-the-middle attacks when used for IPSEC remote access. This occurs since in main mode it is necessary for SKEYID\_e to be used prior to the receipt of the identification payload. Therefore the selection of the pre-shared key may only be based on information contained in the IP header. However, in remote access situations, dynamic IP address assignment is the rule, so that it is typically not possible to identify the required pre-shared key based on the IP address.

Thus when pre-shared keys are used in IPSEC remote access, the same pre-shared key is shared by a group of users and is no longer able to function as an effective shared secret. In this situation, neither the client nor the server identifies itself during IKE phase 1; it is only known that both parties are a member of the group with knowledge of the pre-shared key. This permits anyone with access to the group pre-shared key to act as a man-in-the-middle.

Note that this vulnerability does not occur in aggressive mode since the identity payload is sent earlier in the exchange. However, when aggressive mode is used the user identity is exposed and this may be undesirable.

## [7.](#) References

- [1] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [2] Atkinson, R., Kent, S., "Security Architecture for the Internet

Protocol", [RFC 2401](#), November 1998.

- [3] Droms, R., "Dynamic Host Configuration Protocol", [RFC 2131](#), March 1997.
- [4] McGregor, G., "The PPP Internet Protocol Control Protocol (IPCP)", [RFC 1332](#), May 1992.

Aboba

Informational

[Page 10]

---

INTERNET-DRAFT    IPSEC Remote Access Evaluation Criteria 21 November 2000

- [5] Alexander, S., Droms, R., "DHCP Options and BOOTP Vendor Extensions", [RFC 2132](#), March 1997.
- [6] Droms, R., Arbaugh, W., "Authentication for DHCP Messages", Internet draft (work in progress), [draft-ietf-dhc-authentication-11.txt](#), June 1999.
- [7] Cobb, S., "PPP Internet Protocol Control Protocol Extensions for Name Server Addresses", [RFC 1877](#), December 1995.
- [8] Droms, R., Kinnear, K., Stapp, M., Volz, B., Gonczi, S., Rabil, G., Dooley, M., Kapur, A., "DHCP Failover Protocol", Internet draft (work in progress), [draft-ietf-dhc-failover-04.txt](#), June 1999.
- [9] Kent, S., Atkinson, R., "IP Authentication Header", [RFC 2402](#), November 1998.
- [10] Kent, S., Atkinson, R., "IP Encapsulating Security Payload (ESP)", [RFC 2406](#), November 1998.
- [11] Piper, D., "The Internet IP Security Domain of Interpretation of ISAKMP", [RFC 2407](#), November 1998.
- [12] Harkins, D., Carrel, D., "The Internet Key Exchange (IKE)", [RFC 2409](#), November 1998.
- [13] Pereira, R., Anand, S., Patel, B., "The ISAKMP Configuration Method", Internet draft (work in progress), [draft-ietf-ipsec-isakmp-mode-cfg-05.txt](#), August 1999.
- [14] De Schrijver, P., T'Joens, Y., "Dynamic host configuration : DHCP reconfigure extension", Internet draft (work in progress), [draft-](#)

[schrijvp-dhcpv4-reconfigure-00.txt](#), June 1999.

- [15] Rigney, C., Rubens, A., Simpson, W., Willens, S., "Remote Authentication Dial In User Service (RADIUS)", RFC 2138, April, 1997.
- [16] Simpson, W., Editor, "The Point-to-Point Protocol (PPP)", STD 51, [RFC 1661](#), July 1994.
- [17] Sklower, K., Lloyd, B., McGregor, G., Carr, D., and T. Coradetti, "The PPP Multilink Protocol (MP)", [RFC 1990](#), August 1996.
- [18] Simpson, W., Editor, "PPP LCP Extensions", [RFC 1570](#), January 1994.
- [19] Townsley, W.M., Valencia, A., Rubens, A., Pall, G.S., Zorn, G., and Palter, B., "Layer Two Tunneling Protocol L2TP", [RFC 2661](#), August

Aboba

Informational

[Page 11]

---

INTERNET-DRAFT IPSEC Remote Access Evaluation Criteria 21 November 2000

1999.

- [20] Valencia, A. J., "L2TP Header Compression ('`L2TPHC'')", Internet draft (work in progress), [draft-ietf-l2tpext-l2tphc-03.txt](#), October 1999.
- [21] Stump, G., Droms, R., Gu, Y., Vyaghrapuri, R., Demirtjis, A., Beser, B., Privat, J., "The User Class Option for DHCP", Internet draft (work in progress), [draft-ietf-dhc-userclass-04.txt](#), October 1999.
- [22] Perkins, C., "Minimal Encapsulation Within IP", [RFC 2004](#), October 1996.
- [23] Degermark, M., Nordgren, B., Pink, S., "IP Header Compression", [RFC 2507](#), February 1999.
- [24] Casner, S. and V. Jacobson, "Compressing IP/UDP/RTP Headers for Low-Speed Serial Links", [RFC 2508](#), February 1999.
- [25] Engan, M., Casner, S. and C. Bormann, "IP Header Compression for PPP", [RFC 2509](#), February 1999.
- [26] Hamzeh, K., Pall, G., Verthein, W., Taarud, J., Little, W., Zorn, G., "Point-to-Point Tunneling Protocol (PPTP)", [RFC 2637](#), July

1999.

- [27] Rigney, C., "RADIUS Accounting", [RFC 2139](#), April 1997.
- [28] Rigney, C., Willens, S., Calhoun, P., "RADIUS Extensions", [draft-ietf-radius-ext-04.txt](#), Internet Draft (work in progress), May 1999.
- [29] Blunk, L., Vollbrecht, J., "PPP Extensible Authentication Protocol (EAP)", [RFC 2284](#), March 1998.
- [30] Myers, J., "Simple Authentication and Security Layer (SASL)", FC 2222, October 1997.
- [31] Linn, J., "Generic Security Service Application Program Interface, Version 2", [RFC 2078](#), January 1997.
- [33] Kohl, J., Neuman, C., "The Kerberos Network Authentication Service (V5)", [RFC 1510](#), September 1993.
- [34] Neuman, B. C., Ts'o, T., "Kerberos: An Authentication Service for Computer Networks", IEEE Communications, 32(9):33-38, September 1994.

- [35] Tung, B., Neuman, B. C., Hur, M., Medvinsky, A., Medvinsky, S., Wray, J., Trostle, J., "Public Key Cryptography for Initial Authentication in Kerberos", Internet draft (work in progress), [draft-ietf-cat-kerberos-pk-init-08.txt](#), May 1999.
- [36] Baize, E., Pinkas, D., "The Simple and Protected GSS-API Negotiation Mechanism", [RFC 2478](#), December 1998.
- [37] Linn, J., "The Kerberos Version 5 GSS-API Mechanism", [RFC 1964](#), June 1996.
- [38] Myers, J., "SASL GSSAPI mechanisms", Internet draft (work in progress), [draft-ietf-cat-sasl-gssapi-00.txt](#), March 1999.
- [39] Piper, D., "A GSS-API Authentication Mode for IKE", Internet draft (work in progress), [draft-ietf-ipsec-isakmp-gss-auth-02.txt](#), December 1998.

- [40] Lloyd, B., Simpson, W., "PPP Authentication Protocols", [RFC 1334](#), October 1992.
- [41] Swift, M., Trostle, J., "Initial Authentication and Pass Through Authentication Using Kerberos V5 and the GSS-API (IAKERB)", Internet draft (work in progress), [draft-ietf-cat-iakerb-04.txt](#), October 1999.
- [42] Pereira, R., Beaulieu, S., "Extended Authentication within ISAKMP/Oakley", Internet-draft (work in progress), [draft-ietf-ipsec-isakmp-xauth-05.txt](#), September, 1999.

## [8.](#) Security Considerations

This document, being a requirements document, does not have any security concerns. The security requirements on protocols to be evaluated using this document are described throughout the document.

## [9.](#) IANA Considerations

This draft does not create any new number spaces for IANA administration.

## [10.](#) Acknowledgments

Thanks to Scott Kelly of Redcreek Communications and Ari Huttunen of Data Fellows for useful discussions of this problem space.

## [11.](#) Authors' Addresses

Bernard Aboba  
Microsoft Corporation  
One Microsoft Way  
Redmond, WA 98052

Phone: +1 (425) 936-6605  
EMail: [bernarda@microsoft.com](mailto:bernarda@microsoft.com)

## [12.](#) Full Copyright Statement

Copyright (C) The Internet Society (2000). All Rights Reserved.  
This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English. The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns. This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE."

### 13. Expiration Date

This memo is filed as <[draft-aboba-ipsra-req-02.txt](#)>, and expires August 1, 2001.