

Network Working Group
Internet-Draft
Intended status: Experimental
Expires: July 24, 2008

Y. Sheffer
Y. Nir
Check Point
January 21, 2008

Secure Beacon: Securely Detecting a Trusted Network
draft-sheffer-ipsec-secure-beacon-03

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with [Section 6 of BCP 79](#).

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>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on July 24, 2008.

Copyright Notice

Copyright (C) The IETF Trust (2008).

Abstract

Remote access clients, in particular IPsec-based ones, are heavily deployed in enterprise environments. In many enterprises the security policy allows remote-access clients to switch to unprotected operation when entering the trusted network. This document specifies a method that lets a client detect this situation in a secure manner, with the help of a security gateway. We propose a minor extension to IKEv2 to achieve this goal.

Internet-Draft

IPsec Secure Beacon

January 2008

Table of Contents

1.	Requirements Notation	3
2.	Introduction	3
2.1.	Goals	3
2.2.	Client Mobility	4
2.3.	Alternative Solutions	4
3.	Protocol Details	4
3.1.	Extending IKE for Secure Network Detection	4
3.1.1.	The IKE_SA_INIT Exchange	5
3.1.2.	The IKE_AUTH Exchange	5
3.2.	IKE Notify Payloads	6
3.2.1.	SECURE_NETWORK_DETECT	6
3.2.2.	SECURE_NETWORK_DETECTED	6
3.3.	Detecting Movement	6
3.4.	The Gateway's Decision	7
3.5.	Client Security Policy	7
4.	Interoperation with MOBIKE	7
5.	IANA Considerations	8
6.	Security Considerations	8
7.	Change Log	9
7.1.	-03	9
7.2.	-02	9
7.3.	-01	10
7.4.	-00	10
8.	Acknowledgements	10
9.	References	10
9.1.	Normative References	10
9.2.	Informative References	10
	Authors' Addresses	11
	Intellectual Property and Copyright Statements	12

Internet-Draft

IPsec Secure Beacon

January 2008

1. Requirements Notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [[RFC2119](#)].

2. Introduction

The IKE and IPsec protocols are often used for remote-access clients. IKE version 2 [[RFC4306](#)] provides enhanced support for remote-access clients through the use of EAP. In many cases, IPsec clients need to be "turned off" when the client roams into the internal, or "trusted" network of an enterprise. This operation is very sensitive, since an adversary may use this mechanism to force the client to send unprotected packets into the network. This document defines an extension to IKEv2 where the client contacts a trusted gateway, the gateway detects that the client is located in a trusted network, and delivers an indication to the client in a secure manner. An important property of this protocol is that the exchange may terminate early, if the client and the server agree that IPsec is not required; otherwise the protocol will "fall through" into a standard IKEv2 exchange, generating IKE and Child security associations.

Unfortunately at the time of writing, there is no IETF work group chartered with IPsec. We encourage discussion of this draft on the IPsec mailing list, <https://www1.ietf.org/mailman/listinfo/ipsec>.

2.1. Goals

The proposed protocol should fulfill the following goals.

- o Security, in particular the protocol should not adversely affect the security of IKE.
- o Robustness: the protocol should fall back into a full IKE exchange if any error is detected.
- o Performance: minimize the number of exchanges and the CPU effort

expanded, whether the client is in the trusted or untrusted network.

- o Usability: the user should not be required to perform any action unless this is required for security. We avoid sending the client's identity, because this normally requires input from the user.
- o Simplicity: the protocol should deal with the case of "simple" networks, meaning networks where the internal network is wholly trusted. It does not need to cover more complex topologies.
- o Extensibility: however, the base protocol can be extended, e.g. to handle more complex networks.

[2.2.](#) Client Mobility

Client mobility in IKEv2 is defined using the MOBIKE protocol extension, [[RFC4555](#)]. [Section 4](#) below specifies how the Secure Beacon solution coexists with MOBIKE.

[2.3.](#) Alternative Solutions

There are several alternatives for providing the functionality discussed here.

- o Several proposals related to Mobile IP, such as [[I-D.ietf-mip4-vpn-problem-solution](#)], rely on secure connectivity to the Home Agent, which is assumed to be in the trusted network. This solution obviously can only be applied in a Mobile IP setting.
- o Some proprietary solutions rely on secure connectivity to other "internal" hosts, for example the Windows Domain Controller.
- o Another solution we have considered is to open a dedicated, short-lived TLS connection into the security gateway. This would enable the client to authenticate the gateway. However an IPsec gateway should not be assumed to implement TLS.
- o Lastly, we considered a new protocol, possibly derived from IKE. A separate protocol offers modularity as its main benefit. However we have chosen to reuse IKE itself, where the exchange can be completed as a full IKE exchange. This results in fewer exchanges, and possibly in a simpler implementation.

[3.](#) Protocol Details

The following sections describe the protocol, first at the exchange level and then at the payload level. Following that, we discuss two central issues: how the client detects that it has moved, so that this protocol can be run, and how the gateway can make the decision whether the client is in the trusted or untrusted network.

[3.1.](#) Extending IKE for Secure Network Detection

To summarize, we add an IKE notification to message #1 of the protocol, and another to message #2. However, the protocol is only terminated after the initiator has authenticated the responder, i.e. after message #4. It is important to note that the initiator's identity may not be authenticated if the protocol is terminated early.

[3.1.1.](#) The IKE_SA_INIT Exchange

The IKE_SA_INIT exchange is modified as follows:

Initiator		Responder
-----		-----
HDR, SAi1, KEi, Ni, N1	-->	
	<--	HDR, SAR1, KEr, Nr, N2, [CERTREQ]

All payloads, with the exception of the notifications, have their usual semantics. The first notification, N1, is of type SECURE_NETWORK_DETECT. It denotes to the responder that it SHOULD respond with a second notification (N2), which is of type SECURE_NETWORK_DETECTED. Both notifications are defined in [Section 3.2](#). Note that both notifications are sent in the clear.

Following the first exchange, there are three options:

- o If there is no response after the normal retransmission period, the client SHOULD assume it is on an untrusted network, and is experiencing connectivity problems. For example, the IKE port may be blocked.
- o Otherwise, a response was received. If N2 is not received, or if

it is received but explicitly specifies that the initiator is in an untrusted network, the protocol continues according to standard IKE rules. This would be the case if the responder does not understand the SECURE_NETWORK_DETECT notification.

- o If N2 indicates that the initiator is in a trusted network, the protocol continues as detailed in [Section 3.1.2](#) below.

[3.1.2](#). The IKE_AUTH Exchange

The initiator now responds with a truncated IKE_AUTH exchange:

```
HDR, SK {[IDi, CERT,] [CERTREQ,] [IDr,] [AUTH]} -->
```

The initiator sends the AUTH payload only if it can be authenticated in message #2, i.e. if it uses a shared secret or certificate, rather than EAP. Even if the initiator normally authenticates using one of these methods, it MAY omit both IDi and AUTH, in order to avoid user interaction. If AUTH is included, then the responder MUST authenticate the initiator.

The responder replies with:

```
<-- HDR, SK {IDr, [CERT,] AUTH}
```

The initiator MUST now validate the identity of the responder as defined in [\[RFC4306\]](#), and following that, MUST terminate the

protocol. Obviously in this case, no Child SA is created and therefore no IPsec-protected traffic will be sent. Moreover, no long-term IKE SA is created, and both parties SHOULD delete their IKE SAs. The initiator SHOULD send an Informational exchange containing a Delete payload for the IKE SA. The responder should regard a persistent IKE SA where a secure network has been detected as anomalous and audit their existence. The responder MUST NOT allow any Create Child SA exchanges based on such an IKE SA.

See also [Section 3.5](#) regarding implications on the client's security policy.

It is RECOMMENDED that the client display a message to the user at this point, announcing that it has moved into unprotected mode.

[3.2.](#) IKE Notify Payloads

We define two new notify payload types, SECURE_NETWORK_DETECT and SECURE_NETWORK_DETECTED.

[3.2.1.](#) SECURE_NETWORK_DETECT

This notification type has the value [TBD-BY-IANA1]. It contains no data.

[3.2.2.](#) SECURE_NETWORK_DETECTED

This notification type has the value [TBD-BY-IANA2].

This notify payload includes a single 1-octet data item. It has the value 0 if the responder believes that the initiator is coming from an untrusted network, or if the responder cannot determine where the initiator is coming from. It has the value 1 if the responder believes that the initiator is coming from a trusted network.

Implementations MAY include additional data in this notify payload, however this usage SHOULD be signaled with a Vendor ID payload. Such additional data MUST be ignored by the receiver if not understood.

[3.3.](#) Detecting Movement

Mobility detection is outside the scope of this document. The procedures involved are best described in [[RFC4436](#)] for IPv4. The DNA procedures SHOULD be followed, so that the client can employ the mechanism defined here whenever it suspects that it has moved into a new network, particularly from a trusted to an untrusted network.

[3.4.](#) The Gateway's Decision

The gateway MUST be configured to make a correct decision regarding the client's location. Typically, the gateway would only detect clients connecting through the trusted network if their IKE packets arrive from a trusted physical network interface. Determining which network or network type is considered trusted is left to local policy.

It is RECOMMENDED that the gateway indicate an untrusted network, if it detects that the client is behind a NAT. See [Section 6](#) for rationale.

[3.5.](#) Client Security Policy

If the client sends the SECURE_NETWORK_DETECT notification and does not receive an indication of a trusted network, it SHOULD NOT change its existing SPD and SPD Cache.

If the client receives the SECURE_NETWORK_DETECTED notification indicating a trusted network, it should alter its behavior as follows.

The client SHOULD create BYPASS entries in the SPD Cache for all PROTECT entries in the SPD which are associated with the peer gateway. An entry is said to be associated with a peer gateway if it is a transport mode entry and the remote address is the peer gateway address, or if it is a tunnel mode entry, and the remote tunnel address is the peer gateway address.

The above SPD Cache entries MUST be reset (flushed) whenever the client detects that it has moved from one network attachment to another. See [Section 3.3](#).

IKEv2 allows the client to populate the SPD Cache dynamically based on the INTERNAL_IPv*_SUBNET attributes in the configuration payload (see [section 6.3](#) in IKEv2 Clarifications [[RFC4718](#)]). However, since the client does not reach this state, depending on its static SPD configuration, such a client might effectively create a BYPASS entry for the entire IP address space.

[4.](#) Interoperation with MOBIKE

The client MAY include the SECURE_NETWORK_DETECT notification in any Informational exchange that contains an UPDATE_SA_ADDRESSES notification.

By this time, the client has already determined that the gateway

supports both MOBIKE and the Secure Beacon extension. The gateway MUST respond with a SECURE_NETWORK_DETECTED notification in the response to this Informational exchange.

If the gateway's response specifies that the client is in a trusted network:

- o The gateway MUST NOT attempt a return routability check, if such a check would have normally been required.
- o Both client and gateway MUST tear down the existing IKE SA, and terminate the IKE protocol. The client SHOULD send an Informational exchange containing a Delete payload for the IKE SA.
- o It is RECOMMENDED that the client display a message to the user at this point, announcing that it has moved into unprotected mode.
- o The next time the client detects that it has moved, it SHOULD re-initiate an IKE exchange.

5. IANA Considerations

This document does not create any new namespaces to be maintained by IANA, but it requires new values in namespaces that have been defined in the IKEv2 base specification.

This document defines several new IKEv2 notifications whose values are to be allocated from the "IKEv2 Notify Message Types" namespace.

Notify Messages - Error Types	Value
-----	-----
None	
Notify Messages - Status Types	Value
-----	-----
SECURE_NETWORK_DETECT	TBD-BY-IANA1 (16396..40959)
SECURE_NETWORK_DETECTED	TBD-BY-IANA2 (16396..40959)

6. Security Considerations

The proposed solution needs to be analyzed carefully, since it may cause a host to switch from protected to unprotected communication. Following are the threats that we have identified.

1. The notifications are sent in the clear. A passive attacker will learn whether the responder is receiving traffic over a trusted or untrusted interface. This is information that the attacker is probably able to obtain otherwise.

2. An active attacker may be able to change either or both notifications. The first notification N1 does not carry any data, so it can at worst be deleted. In this case the protocol will revert to normal IKE.
3. An active attacker's change to the N2 notification (or deletion of N2) will be detected since IKE message #2 is authenticated and integrity-protected. Therefore this attack is only equivalent to a DoS attack on IKE. Moreover, the protocol is "fail safe" since any detected failures or attacks will at worst result in the client using a secure channel where one is not required by policy.
4. This protocol can be defeated by an active attacker who can inject packets into the trusted network and relay the responses to such packets back into the untrusted network. Such an attacker will be able to cheat the client into believing that it is on the trusted network. We believe we do not have to address this threat.
5. This protocol MUST NOT be used if the network can change the path between the client and the security gateway without the client's awareness, causing its security properties to change. That is, if the network can route traffic sometimes over a trusted path and sometimes over an untrusted one, without notifying the endpoint. Such a situation might be possible in incorrectly configured Mobile IP deployments, e.g. where the same Home Agent is shared between a trusted Wi-Fi access network and an untrusted one, and where the IPsec layer is not informed of the connectivity changes.
6. There are rare cases when a client is collocated with a NAT. One such case is a client implemented within a software virtual machine. In such cases the client is likely to remain unaware when moving from a trusted to an untrusted network. Therefore we recommend ([Section 3.4](#)) to always indicate an untrusted network to clients behind NAT.

[7.](#) Change Log

[[Note to RFC Editor: please remove this section before publication.]]

[7.1.](#) -03

Intended status changed to Experimental.

[7.2.](#) -02

Minor editorial changes.

Internet-Draft

IPsec Secure Beacon

January 2008

[7.3.](#) -01

Added a section on the client's security policy, per [\[RFC4301\]](#).
Added discussion of the interaction with MOBIKE. Added treatment of client behind NAT.

[7.4.](#) -00

Initial version.

[8.](#) Acknowledgements

We would like to thank Ariel Shaged for his many useful comments.
Thanks to Steve Kent for helping to clarify security policy issues.

[9.](#) References

[9.1.](#) Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", [RFC 4301](#), December 2005.
- [RFC4306] Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", [RFC 4306](#), December 2005.
- [RFC4436] Aboba, B., Carlson, J., and S. Cheshire, "Detecting Network Attachment in IPv4 (DNav4)", [RFC 4436](#), March 2006.
- [RFC4555] Eronen, P., "IKEv2 Mobility and Multihoming Protocol (MOBIKE)", [RFC 4555](#), June 2006.

[9.2.](#) Informative References

[I-D.ietf-mip4-vpn-problem-solution]

Vaarala, S. and E. Klovning, "Mobile IPv4 Traversal Across IPsec-based VPN Gateways",
[draft-ietf-mip4-vpn-problem-solution-04](#) (work in progress), December 2007.

[RFC4718] Eronen, P. and P. Hoffman, "IKEv2 Clarifications and Implementation Guidelines", [RFC 4718](#), October 2006.

Sheffer & Nir

Expires July 24, 2008

[Page 10]

Internet-Draft

IPsec Secure Beacon

January 2008

Authors' Addresses

Yaron Sheffer
Check Point Software Technologies Ltd.
5 Hasolelim st.
Tel Aviv 67897
Israel

Email: yaronf@checkpoint.com

Yoav Nir
Check Point Software Technologies Ltd.
5 Hasolelim st.
Tel Aviv 67897
Israel

Email: ynir@checkpoint.com

Full Copyright Statement

Copyright (C) The IETF Trust (2008).

This document is subject to the rights, licenses and restrictions contained in [BCP 78](#), and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM 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.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information

on the procedures with respect to rights in RFC documents can be found in [BCP 78](#) and [BCP 79](#).

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).