IPSP Working Group
INTERNET DRAFT

S. Fluhrer
Cisco Systems
7 November 2001

Tunnel Endpoint Discovery
draft-fluhrer-ted-00.txt

Status of this Memo

Abstract

The ISAKMP, IKE and IPSec DOI RFCs [RFC2408, RFC2409, RFC2407] specify how an IPSec tunnel is negotiated with an encrypting security gateway (peer), however, they do not specify how the initiator knows who the encrypting peer is. This document specifies a method where the initiator can find the appropriate peer, and also negotiate a mutually acceptable set of proxies.

Overview and Rational

One of the difficulties with deploying ISAKMP/IPSec based networks is the problem of configuring each IPSec host or security gateway with the information required to associate what encrypted traffic should be forwarded to which peer. It is especially important that adding a new encrypting host or gateway should not require the reconfiguration of all existing peers. Tunnel Endpoint Discovery (TED) attempts to solve this problem by relying on routing to find the appropriate peer.

Here is an overview of the TED protocol: if an IPSec host or security gateway needs to know the appropriate peer for a particular flow, it

creates a "TED Probe", which is an ISAKMP packet with the source IP being the source IP of the flow, and the destination IP being the destination IP of the flow. The TED probe packet will follow exactly the same path as an unencrypted packet would. When that TED probe arrives at the encrypting peer, that peer recognizes it and absorbs it. The peer then sends a "TED response" to the original IPSec host or security gateway, which will inform it as to the peer's identity, and allow it to create an appropriate set of proxies. The original host can then either proceed with IKE Phase 1, or go immediately to IKE Phase 2 if it already happens to have an IKE SA with that particular peer.

TED Probe Format

A TED Probe is an IKE packet (UDP with destination port 500, and with an ISAKMP header), with the source and destination IP addresses in the IP header being the source IP and the destination IP of the flow being queried, whose exchange type is 240, message ID zero, a unique cookie as the initiator cookie, zeros as the responder cookie, and is unencrypted. The payloads in the probe MUST include an ID payload which is the IP address of the initiating IPSec host or security gateway (which MUST be the first ID payload within the probe).

Processing on Receiving a TED Probe

Upon receiving a TED probe, the responder SHOULD examine its SPD to determine whether the source and destination within the IP header would be IPSec protected, and if so, what would an acceptable set of proxies for an IPSec SA that protects it (and if the responder does not examine its SPD, it MUST discard the packet). If that packet type is protected, and if TED response is enabled for that SPD entry, then the reponder MUST make a best effort attempt to send a TED Reply based on that SPD entry.

TED Reply Format

A TED Replay is an IKE packet, with the source IP being the IP address of the encrypting peer, and the destination IP address the IP address of the initiator, whose exchange type is 241, message ID zero, the initiator cookie from the TED Probe, a unique cookie as the responder cookie, and is unencrypted. The payloads in the probe MUST include an ID payload which is the IP address of the responding IPSec host or security gateway (which MUST be the first ID payload within the response), and a second ID payload that represents the local portion of proxy entry within the SPD entry.

Processing on Receiving a TED Response

Upon receiving a TED response, the initiator SHALL determine if it corresponds to a TED probe it has recently sent. If it has, it SHALL

examine its SPD to determine its acceptable set of proxies, and combine the local portion of its matching SPD entry, the half proxy listed within the second identity to form a provisional set of proxies. The initiator SHOULD double-check that the provisional set of proxies are acceptable given the SPD, and that the original packet would fall within it.

Then, the initiator MUST make a best effort attempt to intiate a quick mode to the responding peer using the provisional proxies (first initiating a phase 1 if required).

Usage Considerations

For this to be an effective solution, the SPD should follow certain criteria:

- The SPD entries should have everything other than the source IP address and the destination IP address wildcarded. This is suggested, because the responder selects an SPD entry given only those two entries, and having SPD entries that depend on other factors would allow the responder to select an incorrect entry.

Security Considerations

The use of this protocol allows an outside observer to view two aspects of the policy:

- By studying the contents of the TED probe and the TED response, an observer may be able to deduce the proxies that are protected by an IPSec SA that was created using the TED protocol.

- An observer is able to obtain the proxies that a host or security gateway is configured to protect by sending TED probes to it, and observing the TED responses.

If either of these is deemed to be unacceptable, the TED protocol MUST not be used.

Future Directions

It has been suggested that the TED Probe and Response should have signature (and certificate) payloads to add additional security. However, there was insufficient time to fully consider this idea.

Acknowledgements

This protocol is a minor modification of one designed by Dan Harkins.

The suggestion to add signatures to the probes was made by Jan Vilhuber.

References

[Bra97] Bradner, S., "Key Words for use in RFCs to indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[Har98] Harkins, D., Carrel, D. "The Internet Key Exchange (IKE)", RFC 2409, November 1998.

[Mau98] Maughan, D., Schertler, M., Schneider, M., Turner, J., "Internet Security Association and Key Management Protocol (ISAKMP)", RFC 2408, November 1998.

[Pip98] Piper, D., "The Internet IP Security Domain of Interpretation for ISAKMP", RFC 2407, November 1998.

Author's Address

Scott Fluhrer
Cisco Systems
10 West Tasman Drive
San Jose, CA 95134

Phone: (405) 525-5396

EMail: sfluhrer@cisco.com