IPsecME Working Group
Internet-Draft
Intended status: Informational
Expires: April 16, 2012

Y. Nir
Check Point
J. Veizades
Juniper
C. Ulliott
CESG
J. Mendoza
Microsoft

October 14, 2011

Creating Large Scale Mesh VPNs Problem Statement
draft-nir-ipsecme-p2p-00

Abstract

This document presents the problem of configuring a large number of IKE/IPsec systems in such a way that any two of them can use IPsec to protect the traffic between them. Manual configuration of all possible tunnels is too cumbersome in such cases, so an automated method is needed.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on April 16, 2012.

Copyright Notice

Table of Contents

1. Introduction

IPsec ([RFC4301]) is used in several different cases, including tunnel-mode site-to-site VPNs and Remote Access VPNs. Host to host communication employing transport mode also exists, but is far less commonly deployed. The subject of this document is large scale deployments. These may be a large collection of VPN gateways and hosts, all administered within the same administrative domain, or they may be a smaller collection of VPN gateways, with many remote access clients connecting to any of them, or they may be several collections of gateways, each collection administered by a different domain, or they may be combinations of all of the above.

Section 4.4 of RFC 4301 describes the major IPsec databases needed for IPsec processing. It requires an extensive configuration for each tunnel, so manually configuring a "mesh" of several gateways becomes inconvenient.

One way to handle this is what has been termed a "star topology", or a "trunk topology". In this case one gateway, or a few gateways are defined as "core gateways", while the rest, whether remote-access clients or gateways are defined as "satellites". The satellites never connect to other satellites. They only open tunnels with the core gateways.

For a large number of gateways in one administrative domain, one gateway may be defined as the core, and the rest of the gateways and remote access clients connect only to that gateway. If the packet destination is behind another gateway, then the core gateway will re-encrypt the traffic, and send it through the other tunnel. If we have two collections of gateways under two administrative domains, then each domain has its own "core", and the administrators only need to define an IPsec tunnel between the two cores. This tunnel is often referred to as a "trunk".

The problem with stars and trunks is that it creates a high load on

the core gateways as well as on the trunk connection. This load is both in processing power and in network bandwidth. A single packet in the trunk scenario can be encrypted and decrypted three times. It would be much preferable if these gateways and clients could initiate tunnels between them, bypassing the core gateways. Additionally, the path bandwidth to these core gateways may be lower than that of the path between the satellites. For example, two remote access users may be in the same building with high-speed wifi (for example, at an IETF meeting). Channeling their conversation through the core gateways of their respective employers seems extremely wasteful, as well as having lower bandwidth.

The challenge is how to build large scale, fully meshed IPsec protected networks that can dynamically change with minimum administrative overhead.

The difficulty is that all the configuration mentioned in RFC 4301 is not superfluous. IKE implementations need to know the identity and credentials of all possible peer systems, as well as the addresses of hosts and/or networks behind them. A simplified mechanism for establishing ad-hoc tunnels is needed. Section 2 contains several use cases that led to the publishing of this document.

1.1. Conventions Used in This Document

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].

"Administrative Domain" is used in this document for the entity, whether human, team, or computer, that configures VPN gateways and clients. Gateways are said to be under the same administrative domain if they are configured by a single entity and implement the same policy. Some products have the ability to configure multiple VPN gateways or clients, which would solve the problem presented in this document for gateways under the same administrative domain, but they do not solve the problem for multiple administrative domains.

2. Use Cases

This section presents the use cases that have motivated this document in no particular order.

2.1. The Service Provider Use Case

A service provider wishes to control communication between network elements with authentication and encryption as provided by standard protocols like IPsec. This is possible today but the amount of configuration information on each system is currently order n squared so from an operational standpoint this can be challenging as the size of the enterprise network grows. In short service providers wish to minimize the configuration data that is required by any one system to initiate a secure communication link to any other arbitrary system that is part of the service provider enterprise.

These same service providers wish to extend these secure communication links to partners that have similar systems. Again they wish to minimize the amount of configuration needed to initiate these secure connections to arbitrary systems at an arbitrary partner. Additionally they required a directory of connection

information that can be updated independently to manage the identity of the connection endpoints at each one of their partners.

2.2. Cross Domain Mesh Use Case

This section describes requirements for dynamically creating a mesh of VPN endpoints although those endpoints belong to different administrative domains.

2.2.1. Scenario 1

Multiple users, connected to a corporate remote access solution are participating in high bandwidth peer to peer communications. It is required that to optimise bandwidth and latency (subject to policy), the solution is able to establish links between remote peers rather than through a central gateway.

2.2.2. Scenario 2

Rather than remote hosts, the next scenario covers the connectivity between gateways. Behind each gateway there are a number of individual hosts who aren't aware of the protection being offered by the gateway. As each client send traffic to a host at a different site, the gateway is required to identify the location of the remote host and selects the most approprate gateway. Having made this decision, it dynamically establishes a secure tunnel and forwards the

traffic.

2.2.3. Scenario 3

The third scenario is a combination of the first two, where a remote user is no longer tied to using a specific remote access gateway. Should the remote host need to communicate with an entity protected by a gateway as described above, it would be possible for it to identify a suitable gateway and establish a dynamic SA / tunnel and communicate via the most effective route (subject to policy) It is essential that any solution that meets the above scenarios, that we specify a mechanism for identifying permitted hosts / gateways and deploying a policy to each gateway and participating host. The solution also needs to work in an environment where gateways / hosts are administered by different entitites or management domains.

2.3. The Consultant Use Case

This section describes use cases for a consultant who works for multiple organizations but is not an employee of any of them.

2.3.1. Scenario A: Mobile worker and multiple domains

A consultant is hired by corporations (A and B) each of them with their own isolated domains and resources protected with IPsec authentication. The consultant has signed NDA and the corporation granted some level of trust in the form of an authentication ID. This level of trust allows the contractor to access secured resources and networks protected by IPsec until such trust is revoked.

In any given work week the consultant would be providing services on site or remotely to multiple corporations. This is possible today, yet unmanageable due to the amount of configuration required in order for the consultant to dynamically identify the parameters to use when:

- He/She needs to get connected to secure resources when on premises (E2E client to server secured connection)
- He/She needs to use a secure access point when working remotely (Client to Edge connection)

One key aspect of this problem is that the consultant may be providing consulting services to Corp A and Corp B, for privacy reasons this information should be protected.

2.3.2. Scenario B: Consultants sharing securely

Consultant team A and team B have hired by corporation C and are working together in a project that requires collaboration, however

because they are from different consulting firms half of the consultants are based in WA and half in CA. As in the scenario above they have been entrusted with authentication ID. They have a need to share folders with sensitive files in order to work efficiently towards a tight deadline.

They have a need to securely handle this information hence they have a need to discover what type of security should be used when

attempting to share information among themselves.

3. Security Considerations

The solution to the problems presented in this draft may involve dynamic updates to databases defined by RFC 4301, such as the Security Policy Database (SPD) or the Peer Authorization Database (PAD).

RFC 4301 is silent about the way these databases are populated, and it is implied that these databases are static and pre-configured by a human. Allowing dynamic updates to these databases must be thought out carefully, because it allows the protocol to alter the security policy that the IPsec endpoints implement.

One obvious attack to watch out for is stealing traffic to a particular site. The IP address for www.example.com is 192.0.43.10. If we add an entry to an IPsec endpoint's SPD that says that traffic to 192.0.43.10 is protected through peer Gw-Mallory, then this allows Gw-Mallory to either pretend to be www.example.com or to proxy and read all traffic to that site. Updates to this database requires a clear trust model.

More to be added.

4. IANA Considerations

No actions are required from IANA for this informational document.

5. Acknowledgements

The authors would like to thank Geoffrey Huang, Suresh Melam, Andreas Stephen, and Brian Weis for their discussion and comments on early versions of this draft. We would also like to thank Stephen Hanna for gathering the group that has produced this draft.

6. 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.

Authors' Addresses

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

Email: ynir@checkpoint.com

John Veizades
Juniper Networks, Inc.
1194 N. Mathilda ave.
Sunnyvale, CA 94089
USA

Email: jveizades at juniper dot net

Chris Ulliott
CESG
Hubble Road
Cheltenham GL51 0EX
UK

Email: Chris.Ulliott@cesg.gsi.gov.uk

Jorge Coronel Mendoza
Microsoft Corporation
1 Microsoft Way
Redmond, WA 98052
USA

Email: jcoronel@microsoft.com