Network Working Group
Internet Draft

Naganand Doraswamy (FTP Software)
12 March, 1997

Implementation of Virtual Private Network (VPNs) with IP Secrity

<draft-ietf-ipsec-vpn-00.txt>

Status of This Memo

Distribution of this memo is unlimited.

This document is an Internet-Draft. 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 not appropriate to use Internet Drafts as reference material, or to cite them other than as a ``working draft'' or ``work in progress.''

To learn the current status of any Internet-Draft, please check the ``1id-abstracts.txt'' listing contained in the internet-drafts Shadow Directories on:

ftp.is.co.za (Africa)
nic.nordu.net (Europe)
ds.internic.net (US East Coast)
ftp.isi.edu (US West Coast)
munnari.oz.au (Pacific Rim)

Abstract

This document discusses methods for implementing Virtural Private Networks (VPN) with IP Security (IPSec). We discuss different scenarios in which VPN is implemented and the security implications for each of these scenarios.

Contents

1. Introduction

The Authentication Header (AH) [RFC-1826] provides integrity and authentication for IP datagrams. ESP provides data confidentiality, integrity, and authentication. These protocols are used to secure packets end to end and are normally called IP Security (IPSec). However, with intervening gateways (firewalls) or because of the faith in their own private networks, some organizations may choose to secure the packets only on the Intenet and let the packets travel in clear text inside the organization.

This document discusses some scenarios where IPSec can be used to achieve this functionality. We also discuss the security implications under each of this scenario.

Familiarity with the following documents is assumed: "Security Architecture for the Internet Protocol" [RFC-1825], "IP Authentication Header" [RFC-1826], "IP Encapsulated Security Payload" [RFC-1827].

1.1

This section defines certain terms used in this memo in order to communicate with greater clarity.

NODE Any system implementing the TCP/IP protocol suite.

HOST Any IP node that does not forward packets not addressed to the node itself.

ROUTER An IP node that forwards packets not addressed to itself.

FIREWALL An IP node located on the perimeter of an administrative domain that implements that domain's security policy. A firewall usually performs address and port-based packet filtering and usually has stateful proxy servers for EMAIL and other services.

ENCRYPTING FIREWALL A firewall that implements full IP Security, including AH and both tunnel-mode and transport-mode ESP.

PROXY SECURITY SERVER A node that encrypts or decrypts traffic on behalf of some other node. Encrypting Firewalls often also function as proxy security servers.

KEY MANAGEMENT PROXY A node implementing a key management protocol on behalf of some other node.

MOBILE NODE A node that is mobile and is not permanently attached to a fixed location from the perspective of IP.

PRIVATE ADDRESS An IP address that is not globally unique and is only useful within a particular private administrative domain.

NAT Network Address Translator. A router that selectively translates IP addresses in packets prior to forwarding the packets. NATs are commonly used to connect network regions where private addressing is in use to network regions having conflicting private addressing or having globally-unique addressing.

SECURE PACKET In this document this term is used to represent an IP packet with AH and/or ESP.

2. Scenarios

2.1 Remote Node into Corporate Network

Consider the case where a mobile node (host A) needs to communicate with host B behind a firewall (F). In this case, it is necessary that all packets from A to B always go through F. The firewall is configured not to let any unauthenticated packets into the network. There are a few solutions to this problem.

2.1.1 Packets tunneled to firewall

The host A establishes an SA between itself and F and sends a pkt tunneled to F with the final destination B. In this case, F decrypts/authenticates the pkt and forwards the pkt depending on the rules at F. The pkt is forwarded from F to B either in clear text or using AH/ESP. If the pkt needs to be secured the firewall needs to establish an SA between itself and B.

For outbound pkt, i.e. pkts sent from B through the firewall to A, B does not secure the packets to be sent to A. The firewall F after receiving the packet destined to A, secures the packet. B might however secure the packet to F depending on its trust on its internal network.

The problem with this is that the end host (B) has to beleive the firewall. It has to assume that the firewall is doing the necessary security on the inbound packets. Also, on the outbound packets it has to assume that they are going to be secured at the firewall.

The advantage of this is that the firewall can apply the normal filtering rules on the packet as the inner payload is not encrypted.

2.1.2 Packets secured to end host

In thiscase, the firewall (F) is authorised to act as
a key management proxy for the hosts on either side of it. So when A seeks to initiate a secure session with B, it discovers (either via

the KX record of DNS security or via manual configuration) that it should initiate the Key Management exchange with F, with F acting on behalf of B. From A's perspective, this results in a Security Association between A and B, even though the packet will transit F en route to B. In this case, F has the capability of decrypting and examining the packet contents before deciding whether to forward the packet to B or to discard it. This permits IPsec to be used between A and B even though F is still applying its packet filtering policy.

The advantage of this approach is that the end host is encrypting and decrypting packets . However, there is still an implicit assumption that the firewall is not changing any traffic.

2.1.3 Packets secured to end host and tunneled to firewall

In this case, the inner payload is secured to B (transport mode ESP and AH) , and the outer payload tunneled and secured to firewall F.

The advantage of this scheme is that the firewall is able to authenticate packets and decide whether to allow the packet or not without applying the normal filtering rules. This is typical of what happens in the networks today, where an employee gets into the corporate network via a dialup PPP.

On packets destined from B to A, the packets leaving B has transport mode ESP and AH, and the packet is tunneled from F to A after securing the packet.

2.2 Securing packets only on Internet

This case handles securing packets between two or more border routers of a topologically distributed organisation (i.e. one organisation having more than one site without direct internal connectivity between all of the organisation's sites). This scenario is applicable when the organization has faith in its private network but not Internet. This model treats Internet as a set of pipes.

In this case, Security Associations are setup between the border routers. The border routers enforce a policy where all traffic to or from another site of this organisation must be secured using IPsec before being forwarded and must arrive secured as well.

In this case, the KX record for each site probably exists and is configured to point to the border routers for that site. In this way, all nodes outside of that site know that the Border Router handles IPsec on behalf of nodes within that site.

In implementing VPN in this mode, one has to be aware of the following:

- All packets flowing between the two topologically separated facilites always use the routers that have been configured with security.

- All packets between the two routers MUST contain valid IPsec. Any packet

received at either router claiming to come from either the other router or from any node protected by the other router MUST contain valid IPsec or be dropped upon receipt. To do otherwise creates a security hole for spoofers.

2.3 Securing packets to Net 10 Hosts

This handles the case where an organisation is using IP addresses that are private (e.g. use of 10.x.x.x as per RFC-1918). When packets have to be secured to hosts that are in net 10 environment, one needs infrastructure. DNS support is needed to identify where the packets destined for the net 10 hosts can be tunneled to so that, NAT can then forward the packets to this private host.

Consider site S with border router R1. Let S1 be some node inside site S and behind R1. Consider some remote node X that is not within the same administrative domain as S or R1. Now consider that X wishes to initiate an IP session with some node S1. X performs a DNS lookup on S1 and receives an authenticated A/AAAA record with S1's address and also obtains a KX record covering S that points to R1. This enables X to know that it should initiate a key exchange session with R1 if X wishes to use IPsec to protect its session to S1. In this case, R1 is behaving as NAT as well as proxy security server.

In this scenario, NAT is responsible to impose security on the packets flowing into the net 10 environment and there could be some performance bottlenecks.

2.4 AH in tunnel mode

AH in tunnel mode is useful in cases such as Scenario 2 of section 2.1 where you may have a requiment that says that all packets flowing between two routers need to be authenticated. It is also useful in cases when the end hosts do not implement IPSecurity and decision needs to be made at firewall/router as to which packets should be let into the network.

In this scenario, it should be noted that AH does not protect the confidentiality of any data being transmitted and hence this is not strictly speaking a Virtual Private Network. VPNs separate the different logical networks via encryption while AH only provides cryptographic authentication.

Note: Some of the discussions above may change depending on the new drafts.

Acknowledgments

I would like to thank Ran Atkinson and Steve Kent for their valuable input.

References

[RFC-1825] R. Atkinson, "Security Architecture for the Internet Protocol", RFC-1852, Naval Research Laboratory, July 1995.

[RFC-1826] R. Atkinson, "IP Authentication Header", RFC-1826, August 1995.

[RFC-1827] R. Atkinson, "IP Encapsulate Security Payload" RFC-1827, August 1995.

[RFC-1918] Net 10 (need to add more into)

Contact

Naganand Doraswamy
FTP Software Inc.,
2 High St.,
North Andover, MA 01845
naganand@ftp.com