Network Working Group
Request for Comments: 5619
Category: Standards Track

S. Yamamoto
NICT/KDDI R&D Labs
C. Williams
H. Yokota
KDDI R&D Labs
F. Parent
Beon Solutions

August 2009

Softwire Security Analysis and Requirements

Abstract

This document describes security guidelines for the softwire "Hubs and Spokes" and "Mesh" solutions. Together with discussion of the softwire deployment scenarios, the vulnerability to security attacks is analyzed to provide security protection mechanisms such as authentication, integrity, and confidentiality to the softwire control and data packets.

Status of This Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Table of Contents

1. Introduction 3
2. Terminology 4
2.1. Abbreviations 4
2.2. Requirements Language 5
3. Hubs and Spokes Security Guidelines 5
3.1. Deployment Scenarios 5
3.2. Trust Relationship 7
3.3. Softwire Security Threat Scenarios 8
3.4. Softwire Security Guidelines 11
3.4.1. Authentication 12
3.4.2. Softwire Security Protocol 13
3.5. Guidelines for Usage of IPsec in Softwire 13
3.5.1. Authentication Issues 14
3.5.2. IPsec Pre-Shared Keys for Authentication 15
3.5.3. Inter-Operability Guidelines 15
3.5.4. IPsec Filtering Details 16
4. Mesh Security Guidelines 19
4.1. Deployment Scenario 19
4.2. Trust Relationship 20
4.3. Softwire Security Threat Scenarios 20
4.4. Applicability of Security Protection Mechanism 21
4.4.1. Security Protection Mechanism for Control Plane . . . 21
4.4.2. Security Protection Mechanism for Data Plane 22
5. Security Considerations 23
6. Acknowledgments 23
7. References 23
7.1. Normative References 23
7.2. Informative References 24
Appendix A. Examples 26
A.1. IPv6-over-IPv4 Softwire with L2TPv2 Example for IKE . . . 26
A.2. IPv4-over-IPv6 Softwire with Example for IKE 26

1. Introduction

The Softwire Working Group specifies the standardization of discovery, control, and encapsulation methods for connecting IPv4 networks across IPv6 networks and IPv6 networks across IPv4 networks. The softwire provides connectivity to enable the global reachability of both address families by reusing or extending existing technology. The Softwire Working Group is focusing on the two scenarios that emerged when discussing the traversal of networks composed of differing address families. This document provides the security guidelines for two such softwire solution spaces: the "Hubs and Spokes" and "Mesh" scenarios. The "Hubs and Spokes" and "Mesh" problems are described in [RFC4925] Sections 2 and 3, respectively. The protocols selected for softwire connectivity require security considerations on more specific deployment scenarios for each solution. The scope of this document provides analysis on the security vulnerabilities for the deployment scenarios and specifies the proper usage of the security mechanisms that are applied to the softwire deployment.

The Layer Two Tunneling Protocol (L2TPv2) is selected as the phase 1 protocol to be deployed in the "Hubs and Spokes" solution space. If L2TPv2 is used in the unprotected network, it will be vulnerable to various security attacks and MUST be protected by an appropriate security protocol, such as IPsec as described in [RFC3193]. The new implementation SHOULD use IKEv2 (Internet Key Exchange Protocol version 2) as the key management protocol for IPsec because it is a more reliable protocol than IKEv1 and integrates the required protocols into a single platform. This document provides implementation guidance and specifies the proper usage of IPsec as the security protection mechanism by considering the security vulnerabilities in the "Hubs and Spokes" scenario. The document also addresses cases where the security protocol is not necessarily mandated.

The softwire "Mesh" solution MUST support various levels of security mechanisms to protect the data packets being transmitted on a softwire tunnel from the access networks with one address family across the transit core operating with a different address family [RFC4925]. The security mechanism for the control plane is also required to be protected from control-data modification, spoofing attacks, etc. In the "Mesh" solution, BGP is used for distributing softwire routing information in the transit core; meanwhile, security issues for BGP are being discussed in other working groups. This document provides the proper usage of security mechanisms for softwire mesh deployment scenarios.

2. Terminology

2.1. Abbreviations

The terminology is based on the "Softwire Problem Statement" [RFC4925].

AF(i) - Address Family. IPv4 or IPv6. Notation used to indicate that prefixes, a node, or network only deal with a single IP AF.

AF(i,j) - Notation used to indicate that a node is dual-stack or that a network is composed of dual-stack nodes.

Address Family Border Router (AFBR) - A dual-stack router that interconnects two networks that use either the same or different address families. An AFBR forms peering relationships with other AFBRs, adjacent core routers, and attached Customer Edge (CE) routers; performs softwire discovery and signaling; advertises client ASF(i) reachability information; and encapsulates/decapsulates customer packets in softwire transport headers.

Customer Edge (CE) - A router located inside an AF access island that peers with other CE routers within the access island network and with one or more upstream AFBRs.

Customer Premise Equipment (CPE) - An equipment, host or router, located at a subscriber’s premises and connected with a carrier’s access network.

Provider Edge (PE) - A router located at the edge of a transit core network that interfaces with the CE in an access island.

Softwire Concentrator (SC) - The node terminating the softwire in the service provider network.

Softwire Initiator (SI) - The node initiating the softwire within the customer network.

Softwire Encapsulation Set (SW-Encap) - A softwire encapsulation set contains tunnel header parameters, order of preference of the tunnel header types, and the expected payload types (e.g., IPv4) carried inside the softwire.

Softwire Next_Hop (SW-NHOP) - This attribute accompanies client AF reachability advertisements and is used to reference a softwire on the ingress AFBR leading to the specific prefixes. It contains a softwire identifier value and a softwire next_hop IP address denoted as <SW ID:SW-NHOP address>. Its existence in the presence of client

AF prefixes (in advertisements or entries in a routing table) infers the use of softwire to reach that prefix.

2.2. Requirements Language

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].

3. Hubs and Spokes Security Guidelines

3.1. Deployment Scenarios

To provide the security guidelines, discussion of the possible deployment scenario and the trust relationship in the network is important.

The softwire initiator (SI) always resides in the customer network. The node in which the SI resides can be the CPE access device, another dedicated CPE router behind the original CPE access device, or any kind of host device, such as a PC, appliance, sensor, etc.

However, the host device may not always have direct access to its home carrier network, to which the user has subscribed. For example, the SI in the laptop PC can access various access networks such as Wi-Fi hot-spots, visited office networks, etc. This is the nomadic case, which the softwire SHOULD support.

As the softwire deployment model, the following three cases as shown in Figure 1 should be considered. Cases 2 and 3 are typical for a nomadic node, but are also applicable to a stationary node. In order to securely connect a legitimate SI and SC to each other, the authentication process between SI and SC is normally performed using Authentication, Authorization, and Accounting (AAA) servers.

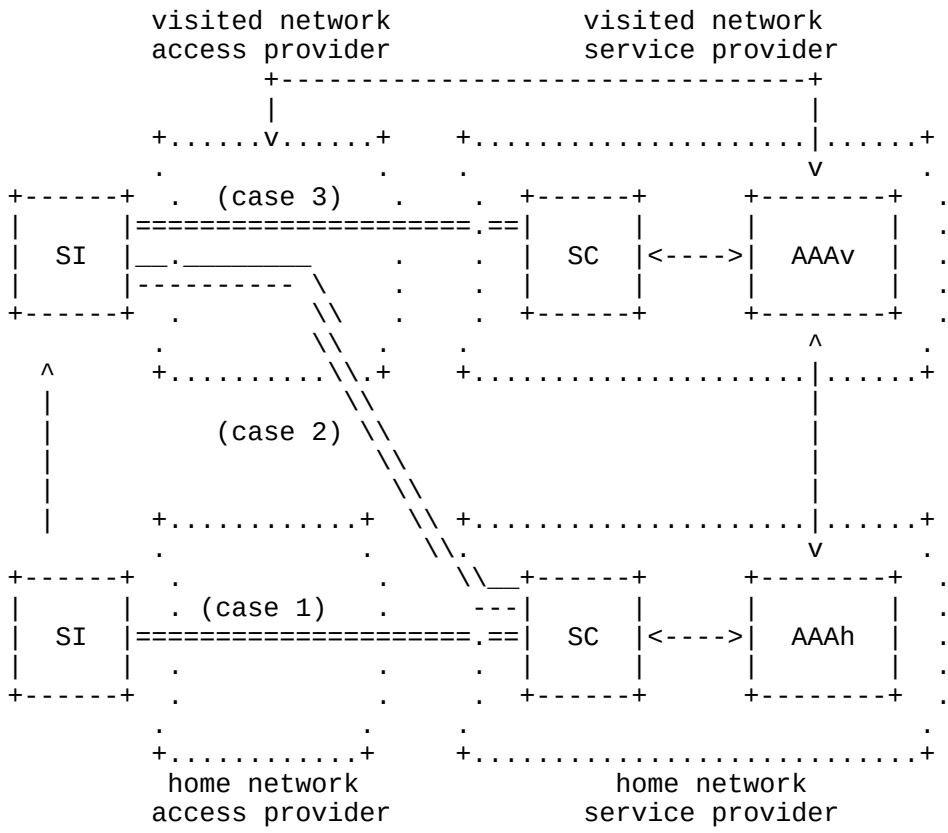

Figure 1: Authentication Model for Hubs and Spokes

The AAA server shown in Figure 1 interacts with the SC, which acts as a AAA client. The AAA may consists of multiple AAA servers, and the proxy AAA may be intermediate between the SC and the AAA servers. This document refers to the AAA server in the home network service provider as the home AAA server (AAAh) and to that in the visited network service provider as the visited AAA server (AAAv).

The "Softwire Problem Statement" [RFC4925] states that the softwire solution must be able to be integrated with commonly deployed AAA solutions. L2TPv2 used in softwire supports PPP and L2TP authentications that can be integrated with common AAA servers.

When the softwire is used in an unprotected network, a stronger authentication process is required (e.g., IKEv2). The proper selection of the authentication processes is discussed in Section 3.4 with respect to the various security threats.

Case 1: The SI connects to the SC that belongs to the home network service provider via the home access provider network that operates a different address family. It is assumed that the home access provider network and the home network service provider for the SC are under the same administrative system.

Note that the IP address of the host device, in which the SI resides, is static or dynamic depending on the subscribed service. The discovery of the SC may be automatic. But in this document, the information on the SC, e.g., the DNS name or IP address, is assumed to be configured by the user or the provider of the SI in advance.

Case 2: The SI connects to the SC that belongs to the home network service provider via the visited access network. For the nomadic case, the SI/user does not subscribe to the visited access provider. For network access through the public network, such as Wi-Fi hot-spots, the home network service provider does not have a trust relationship with the access network.

Note that the IP address of the host device, in which the SI resides, may be changed periodically due to the home network service provider's policy.

Case 3: The SI connects to the SC that belongs to the visited network service provider via the visited access network. This is typical of the nomadic access case. When the SI is mobile, it may roam from the home ISP providing the home access network to the visited access network, e.g., Wi-Fi hot-spot network provided by the different ISP. The SI does not connect to the SC in the home network, for example, due to geographical reasons. The SI/user does not subscribe to the visited network service provider, but the visited network service provider has some roaming agreement with the home network service provider.

Note that the IP address of the host, in which the SI resides, is provided with the visited network service provider's policy.

3.2. Trust Relationship

The establishment of a trust relationship between the SI and SC is different for three cases. The security considerations must be taken into account for each case.

In Case 1, the SC and the home AAA server in the same network service provider MUST have a trust relationship and communications between them MUST be secured. When the SC authenticates the SI, the SC transmits the authentication request message to the home AAA server and obtains the accept message together with the Attribute Value Pair

for the SI authentication. Since the SI is in the service provider network, the provider can take measures to protect the entities (e.g., SC, AAA servers) against a number of security threats, including the communication between them.

In Case 2, when the SI is mobile, access to the home network service provider through the visited access network provider is allowed. The trust relationship between the SI and the SC in the home network MUST be established. When the visited access network is a public network, various security attacks must be considered. Especially for SI to connect to the legitimate SC, the authentication from SI to SC MUST be performed together with that from SC to SI.

In Case 3, if the SI roams into a different network service provider's administrative domain, the visited AAA server communicates with the home AAA server to obtain the information for SI authentication. The visited AAA server MUST have a trust relationship with the home AAA server and the communication between them MUST be secured in order to properly perform the roaming services that have been agreed upon under specified conditions.

Note that the path for the communications between the home AAA server and the visited AAA server may consist of several AAA proxies. In this case, the AAA proxy threat model SHOULD be considered [RFC2607]. A malicious AAA proxy may launch passive or active security attacks. The trustworthiness of proxies in AAA proxy chains will weaken when the hop counts of the proxy chain is longer. For example, the accounting information exchanged among AAA proxies is attractive for an adversary. The communication between a home AAA server and a visited AAA server MUST be protected.

3.3. Softwire Security Threat Scenarios

Softwire can be used to connect IPv6 networks across public IPv4 networks and IPv4 networks across public IPv6 networks. The control and data packets used during the softwire session are vulnerable to the security attacks.

A complete threat analysis of softwire requires examination of the protocols used for the softwire setup, the encapsulation method used to transport the payload, and other protocols used for configuration (e.g., router advertisements, DHCP).

The softwire solution uses a subset of the Layer Two Tunneling Protocol (L2TPv2) functionality ([RFC2661], [RFC5571]). In the softwire "Hubs and Spokes" model, L2TPv2 is used in a voluntary tunnel model only. The SI acts as an L2TP Access Concentrator (LAC) and PPP endpoint. The L2TPv2 tunnel is always initiated from the SI.

The generic threat analysis done for L2TP using IPsec [RFC3193] is applicable to softwire "Hubs and Spokes" deployment. The threat analysis for other protocols such as MIPv6 (Mobile IPv6) [RFC4225], PANA (Protocol for Carrying Authentication for Network Access) [RFC4016], NSIS (Next Steps in Signaling) [RFC4081], and Routing Protocols [RFC4593] are applicable here as well and should be used as references.

First, the SI that resides in the customer network sends a Start-Control-Connection-Request (SCCRQ) packet to the SC for the initiation of the softwire. L2TPv2 offers an optional tunnel authentication system (which is similar to CHAP -- the Challenge Handshake Authentication Protocol) during control connection establishment. This requires a shared secret between the SI and SC and no key management is offered for this L2TPv2.

When the L2TPv2 control connection is established, the SI and SC optionally enter the authentication phase after completing PPP Link Control Protocol (LCP) negotiation. PPP authentication supports one-way or two-way CHAP authentication, and can leverage existing AAA infrastructure. PPP authentication does not provide per-packet authentication.

PPP encryption is defined but PPP Encryption Control Protocol (ECP) negotiation does not provide for a protected cipher suite negotiation. PPP encryption provides a weak security solution [RFC3193]. PPP ECP implementation cannot be expected. PPP authentication also does not provide scalable key management.

Once the L2TPv2 tunnel and PPP configuration are successfully established, the SI is connected and can start using the connection.

These steps are vulnerable to man-in-the-middle (MITM), denial-of-service (DoS), and service-theft attacks, which are caused by the following adversary actions.

Adversary attacks on softwire include:

1. An adversary may try to discover identities and other confidential information by snooping data packets.

2. An adversary may try to modify both control and data packets. This type of attack involves integrity violations.

3. An adversary may try to eavesdrop and collect control messages. By replaying these messages, an adversary may successfully hijack the L2TP tunnel or the PPP connection inside the tunnel. An adversary might mount MITM, DoS, and theft-of-service attacks.

4. An adversary can flood the softwire node with bogus signaling messages to cause DoS attacks by terminating L2TP tunnels or PPP connections.

5. An adversary may attempt to disrupt the softwire negotiation in order to weaken or remove confidentiality protection.

6. An adversary may wish to disrupt the PPP LCP authentication negotiation.

When AAA servers are involved in softwire tunnel establishment, the security attacks can be mounted on the communication associated with AAA servers. Specifically, for Case 3 stated in Section 3.2, an adversary may eavesdrop on the packets between AAA servers in the home and visited network and compromise the authentication data. An adversary may also disrupt the communication between the AAA servers, causing a service denial. Security of AAA server communications is out of scope of this document.

In environments where the link is shared without cryptographic protection and weak authentication or one-way authentication is used, these security attacks can be mounted on softwire control and data packets.

When there is no prior trust relationship between the SI and SC, any node can pretend to be a SC. In this case, an adversary may impersonate the SC to intercept traffic (e.g., "rogue" softwire concentrator).

The rogue SC can introduce a denial-of-service attack by blackholing packets from the SI. The rogue SC can also eavesdrop on all packets sent from or to the SI. Security threats of a rogue SC are similar to a compromised router.

The deployment of ingress filtering is able to control malicious users' access [RFC4213]. Without specific ingress filtering checks in the decapsulator at the SC, it would be possible for an attacker to inject a false packet, leaving the system vulnerable to attacks such as DoS. Using ingress filtering, invalid inner addresses can be rejected. Without ingress filtering of inner addresses, another kind of attack can happen. The malicious users from another ISP could start using its tunneling infrastructure to get free inner-address connectivity, effectively transforming the ISP into an inner-address transit provider.

Ingress filtering does not provide complete protection in the case that address spoofing has happened. In order to provide better protection against address spoofing, authentication with binding

between the legitimate address and the authenticated identity MUST be implemented. This can be implemented between the SC and the SI using IPsec.

3.4. Softwire Security Guidelines

Based on the security threat analysis in Section 3.3 of this document, the softwire security protocol MUST support the following protections.

1. Softwire control messages between the SI and SC MUST be protected against eavesdropping and spoofing attacks.

2. The softwire security protocol MUST be able to protect itself against replay attacks.

3. The softwire security protocol MUST be able to protect the device identifier against the impersonation when it is exchanged between the SI and the SC.

4. The softwire security protocol MUST be able to securely bind the authenticated session to the device identifier of the client, to prevent service theft.

5. The softwire security protocol MUST be able to protect disconnect and revocation messages.

The softwire security protocol requirement is comparable to [RFC3193].

For softwire control packets, authentication, integrity, and replay protection MUST be supported, and confidentiality SHOULD be supported.

For softwire data packets, authentication, integrity, and replay protection SHOULD be supported, and confidentiality MAY be supported.

The "Softwire Problem Statement" [RFC4925] provides some requirements for the "Hubs and Spoke" solution that are taken into account in defining the security protection mechanisms.

1. The control and/or data plane MUST be able to provide full payload security when desired.

2. The deployed technology MUST be very strongly considered.

This additional security protection must be separable from the softwire tunneling mechanism.

Note that the scope of this security is on the L2TP tunnel between the SI and SC. If end-to-end security is required, a security protocol SHOULD be used in the payload packets. But this is out of scope of this document.

3.4.1. Authentication

The softwire security protocol MUST support user authentication in the control plane in order to authorize access to the service and provide adequate logging of activity. Although several authentication protocols are available, security threats must be considered to choose the protocol.

For example, consider the SI/user using Password Authentication Protocol (PAP) access to the SC with a cleartext password. In many circumstances, this represents a large security risk. The adversary may spoof as a legitimate user by using the stolen password. The Challenge Handshake Authentication Protocol (CHAP) [RFC1994] encrypts a password with a "challenge" sent from the SC. The theft of password can be mitigated. However, as CHAP only supports unidirectional authentication, the risk of a man-in-the-middle or rogue SC cannot be avoided. Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) [RFC5216] mandates mutual authentication and avoids the rogue SC.

When the SI established a connection to the SC through a public network, the SI may want proof of the SC identity. Softwire MUST support mutual authentication to allow for such a scenario.

In some circumstances, however, the service provider may decide to allow non-authenticated connection [RFC5571]. For example, when the customer is already authenticated by some other means, such as closed networks, cellular networks at Layer 2, etc., the service provider may decide to turn authentication off. If no authentication is conducted on any layer, the SC acts as a gateway for anonymous connections. Running such a service MUST be configurable by the SC administrator and the SC SHOULD take some security measures, such as ingress filtering and adequate logging of activity. It should be noted that anonymous connection service cannot provide the security functionalities described in this document (e.g., integrity, replay protection, and confidentiality).

L2TPv2 selected as the softwire phase 1 protocol supports PPP authentication and L2TPv2 authentication. PPP authentication and L2TPv2 have various security threats, as stated in Section 3.3. They will be used in the limited condition as described in the next subsections.

3.4.1.1. PPP Authentication

PPP can provide mutual authentication between the SI and SC using CHAP [RFC1994] during the connection-establishment phase (via the Link Control Protocol, LCP). PPP CHAP authentication can be used when the SI and SC are on a trusted, non-public IP network.

Since CHAP does not provide per-packet authentication, integrity, or replay protection, PPP CHAP authentication MUST NOT be used unprotected on a public IP network. If other appropriate protected mechanisms have been already applied, PPP CHAP authentication MAY be used.

Optionally, other authentication methods such as PAP, MS-CHAP, and EAP MAY be supported.

3.4.1.2. L2TPv2 Authentication

L2TPv2 provides an optional CHAP-like tunnel authentication during the control connection establishment [RFC2661], Section 5.1.1. L2TPv2 authentication MUST NOT be used unprotected on a public IP network, similar to the same restriction applied to PPP CHAP authentication.

3.4.2. Softwire Security Protocol

To meet the above requirements, all softwire-security-compliant implementations MUST implement the following security protocols.

IPsec ESP [RFC4303] in transport mode is used for securing softwire control and data packets. The Internet Key Exchange (IKE) protocol [RFC4306] MUST be supported for authentication, security association negotiation, and key management for IPsec. The applicability of different versions of IKE is discussed in Section 3.5.

The softwire security protocol MUST support NAT traversal. UDP encapsulation of IPsec ESP packets[RFC3948] and negotiation of NAT-traversal in IKE [RFC3947] MUST be supported when IPsec is used.

3.5. Guidelines for Usage of IPsec in Softwire

When the softwire "Hubs and Spokes" solution implemented by L2TPv2 is used in an untrustworthy network, softwire MUST be protected by appropriate security protocols, such as IPsec. This section provides guidelines for the usage of IPsec in L2TPv2-based softwire.

[RFC3193] discusses how L2TP can use IKE [RFC2409] and IPsec [RFC2401] to provide tunnel authentication, privacy protection,

integrity checking, and replay protection. Since the publication of [RFC3193], the revisions to IPsec protocols have been published (IKEv2 [RFC4306], ESP [RFC4303], NAT-traversal for IKE [RFC3947], and ESP [RFC3948]).

Given that deployed technology must be very strongly considered [RFC4925] for the 'time-to-market' solution, [RFC3193] MUST be supported. However, the new implementation SHOULD use IKEv2 [RFC4306] for IPsec because of the numerous advantages it has over IKE [RFC2409]. In new deployments, IKEv2 SHOULD be used as well.

Although [RFC3193] can be applied in the softwire "Hubs and Spokes" solution, softwire requirements such as NAT-traversal, NAT-traversal for IKE [RFC3947], and ESP [RFC3948] MUST be supported.

Meanwhile, IKEv2 [RFC4306] integrates NAT-traversal. IKEv2 also supports EAP authentication, with the authentication using shared secrets (pre-shared key) or a public key signature (certificate).

The selection of pre-shared key or certificate depends on the scale of the network for which softwire is to be deployed, as described in Section 3.5.2. However, pre-shared keys and certificates only support the machine authentication. When both machine and user authentications are required as, for example, in the nomadic case, EAP SHOULD be used.

Together with EAP, IKEv2 [RFC4306] supports legacy authentication methods that may be useful in environments where username- and password-based authentication is already deployed.

IKEv2 is a more reliable protocol than IKE [RFC2409] in terms of replay-protection capability, DoS-protection-enabled mechanism, etc. Therefore, new implementations SHOULD use IKEv2 over IKE.

The following sections will discuss using IPsec to protect L2TPv2 as applied in the softwire "Hubs and Spokes" model. Unless otherwise stated, IKEv2 and the new IPsec architecture [RFC4301] is assumed.

3.5.1. Authentication Issues

IPsec implementation using IKE only supports machine authentication. There is no way to verify a user identity and to segregate the tunnel traffic among users in the multi-user machine environment. IKEv2 can support user authentication with EAP payload by leveraging the existing authentication infrastructure and credential database. This enables traffic segregation among users when user authentication is used by combining the legacy authentication. The user identity asserted within IKEv2 will be verified on a per-packet basis.

If the AAA server is involved in security association establishment between the SI and SC, a session key can be derived from the authentication between the SI and the AAA server. Successful EAP exchanges within IKEv2 run between the SI and the AAA server to create a session key, which is securely transferred to the SC from the AAA server. The trust relationship between the involved entities follows Section 3.2 of this document.

3.5.2. IPsec Pre-Shared Keys for Authentication

With IPsec, when the identity asserted in IKE is authenticated, the resulting derived keys are used to provide per-packet authentication, integrity, and replay protection. As a result, the identity verified in the IKE is subsequently verified on reception of each packet.

Authentication using pre-shared keys can be used when the number of SI and SC is small. As the number of SI and SC grows, pre-shared keys become increasingly difficult to manage. A softwire security protocol MUST provide a scalable approach to key management. Whenever possible, authentication with certificates is preferred.

When pre-shared keys are used, group pre-shared keys MUST NOT be used because of its vulnerability to man-in-the-middle attacks ([RFC3193], Section 5.1.4).

3.5.3. Inter-Operability Guidelines

The L2TPv2/IPsec inter-operability concerning tunnel teardown, fragmentation, and per-packet security checks given in [RFC3193], Section 3 must be taken into account.

Although the L2TP specification allows the responder (SC in softwire) to use a new IP address or to change the port number when sending the Start-Control-Connection-Request-Reply (SCCRP), a softwire concentrator implementation SHOULD NOT do this ([RFC3193], Section 4).

However, for some reasons, for example, "load-balancing" between SCs, the IP address change is required. To signal an IP address change, the SC sends a StopCCN message to the SI using the Result and Error Code AVP in an L2TPv2 message. A new IKE_SA and CHILD_SA MUST be established to the new IP address.

Since ESP transport mode is used, the UDP header carrying the L2TP packet will have an incorrect checksum due to the change of parts of the IP header during transit. Section 3.1.2 of [RFC3948] defines 3 procedures that can be used to fix the checksum. A softwire implementation MUST NOT use the "incremental update of checksum"

(option 1 described in [RFC3948]) because IKEv2 does not have the information required (NAT-OA payload) to compute that checksum. Since ESP is already providing validation on the L2TP packet, a simple approach is to use the "do not check" approach (option 3 in [RFC3948]).

3.5.4. IPsec Filtering Details

If the old IPsec architecture [RFC2401] and IKE [RFC2409] are used, the security policy database (SPD) examples in [RFC3193], Appendix A can be applied to softwire model. In that case, the initiator is always the client (SI), and the responder is the SC. IPsec SPD examples for IKE [RFC2409] are also given in Appendix A of this document.

The revised IPsec architecture [RFC4301] redefined the SPD entries to provide more flexibility (multiple selectors per entry, list of address range, peer authentication database (PAD), "populate from packet" (PFP) flag, etc.). The Internet Key Exchange (IKE) has also been revised and simplified in IKEv2 [RFC4306]. The following sections provide the SPD examples for softwire to use the revised IPsec architecture and IKEv2.

3.5.4.1. IPv6-over-IPv4 Softwire L2TPv2 Example for IKEv2

If IKEv2 is used as the key management protocol, [RFC4301] provides the guidance of the SPD entries. In IKEv2, we can use the PFP flag to specify the SA, and the port number can be selected with the TSr (Traffic Selector - Responder) payload during CREATE_CHILD_SA. The following describes PAD entries on the SI and SC, respectively. The PAD entries are only example configurations. The PAD entry on the SC matches user identities to the L2TP SPD entry. This is done using a symbolic name type specified in [RFC4301].

```
SI PAD:
- IF remote_identity = SI_identity
     Then authenticate (shared secret/certificate/)
     and authorize CHILD_SA for remote address SC_address

SC PAD:
- IF remote_identity = user_1
     Then authenticate (shared secret/certificate/EAP)
     and authorize CHILD_SAs for symbolic name "l2tp_spd_entry"
```

The following describes the SPD entries for the SI and SC, respectively. Note that IKEv2 and ESP traffic MUST be allowed (bypass). These include IP protocol 50 and UDP port 500 and 4500.

The IPv4 packet format when ESP protects and L2TPv2 carries an IPv6 packet is shown in Table 1, which is similar to Table 1 in [RFC4891].

Components (first to last)	Contains
IPv4 header	(src = IPv4-SI, dst = IPv4-SC)
ESP header	
UDP header	(src port=1701, dst port=1701)
L2TPv2 header	
PPP header	
IPv6 header	
(payload)	
ESP ICV	

Table 1: Packet Format for L2TPv2 with ESP Carrying IPv6 Packet

SPD for Softwire Initiator:

```
Softwire Initiator SPD-S
- IF local_address=IPv4-SI
     remote_address=IPv4-SC
     Next Layer Protocol=UDP
     local_port=1701
     remote_port=ANY (PFP=1)
 Then use SA ESP transport mode
 Initiate using IDi = user_1 to address IPv4-SC
```

SPD for Softwire Concentrator:

```
Softwire Concentrator SPD-S
- IF name="l2tp_spd_entry"
     local_address=IPv4-SC
     remote_address=ANY (PFP=1)
     Next Layer Protocol=UDP
     local_port=1701
     remote_port=ANY (PFP=1)
 Then use SA ESP transport mode
```

3.5.4.2. IPv4-over-IPv6 Softwire L2TPv2 Example for IKEv2

The PAD entries for SI and SC are shown as examples. These example configurations are similar to those in Section 3.5.4.1 of this document.

```
SI PAD:
- IF remote_identity = SI_identity
     Then authenticate (shared secret/certificate/)
     and authorize CHILD_SA for remote address SC_address

SC PAD:
- IF remote_identity = user_2
     Then authenticate (shared secret/certificate/EAP)
     and authorize CHILD_SAs for symbolic name "l2tp_spd_entry"
```

The following describes the SPD entries for the SI and SC, respectively. In this example, the SI and SC are denoted with IPv6 addresses IPv6-SI and IPv6-SC, respectively. Note that IKEv2 and ESP traffic MUST be allowed (bypass). These include IP protocol 50 and UDP port 500 and 4500.

The IPv6 packet format when ESP protects and L2TPv2 carries an IPv4 packet is shown in Table 2, which is similar to Table 1 in [RFC4891].

Components (first to last)	Contains
IPv6 header	(src = IPv6-SI, dst = IPv6-SC)
ESP header	
UDP header	(src port=1701, dst port=1701)
L2TPv2 header	
PPP header	
IPv4 header	
(payload)	
ESP ICV	

Table 2: Packet Format for L2TPv2 with ESP Carrying IPv4 Packet

SPD for Software Initiator:

```
Softwire Initiator SPD-S
- IF local_address=IPv6-SI
     remote_address=IPv6-SC
     Next Layer Protocol=UDP
     local_port=1701
     remote_port=ANY (PFP=1)
 Then use SA ESP transport mode
 Initiate using IDi = user_2 to address IPv6-SC
```

SPD for Softwire Concentrator:

```
Softwire Concentrator SPD-S
- IF name="l2tp_spd_entry"
     local_address=IPv6-SC
     remote_address=ANY (PFP=1)
     Next Layer Protocol=UDP
     local_port=1701
     remote_port=ANY (PFP=1)
 Then use SA ESP transport mode
```

4. Mesh Security Guidelines

4.1. Deployment Scenario

In the softwire "Mesh" solution ([RFC4925], [RFC5565]), it is required to establish connectivity to access network islands of one address family type across a transit core of a differing address family type. To provide reachability across the transit core, AFBRs are installed between the access network island and transit core network. These AFBRs can perform as Provider Edge routers (PE) within an autonomous system or perform peering across autonomous systems. The AFBRs establish and encapsulate softwires in a mesh to the other islands across the transit core network. The transit core network consists of one or more service providers.

In the softwire "Mesh" solution, a pair of PE routers (AFBRs) use BGP to exchange routing information. AFBR nodes in the transit network are Internal BGP speakers and will peer with each other directly or via a route reflector to exchange SW-encap sets, perform softwire signaling, and advertise AF access island reachability information and SW-NHOP information. If such information is advertised within an autonomous system, the AFBR node receiving them from other AFBRs does not forward them to other AFBR nodes. To exchange the information among AFBRs, the full mesh connectivity will be established.

The connectivity between CE and PE routers includes dedicated physical circuits, logical circuits (such as Frame Relay and ATM), and shared medium access (such as Ethernet-based access).

When AFBRs are PE routers located at the edge of the provider core networks, this architecture is similar to the L3VPN described in [RFC4364]. The connectivity between a CE router in an access island network and a PE router in a transit network is established statically. The access islands are enterprise networks accommodated through PE routers in the provider’s transit network. In this case, the access island networks are administrated by the provider’s autonomous system.

The AFBRs may have multiple connections to the core network, and also may have connections to multiple client access networks. The client access networks may connect to each other through private networks or through the Internet. When the client access networks have their own AS number, a CE router located inside access islands forms a private BGP peering with an AFBR. Further, an AFBR may need to exchange full Internet routing information with each network to which it connects.

4.2. Trust Relationship

All AFBR nodes in the transit core MUST have a trust relationship or an agreement with each other to establish softwires. When the transit core consists of a single administrative domain, it is assumed that all nodes (e.g., AFBR, PE, or Route Reflector, if applicable) are trusted by each other.

If the transit core consists of multiple administrative domains, intermediate routers between AFBRs may not be trusted.

There MUST be a trust relationship between the PE in the transit core and the CE in the corresponding island, although the link(s) between the PE and the CE may not be protected.

4.3. Softwire Security Threat Scenarios

As the architecture of the softwire mesh solution is very similar to that of the provider-provisioned VPN (PPVPN). The security threat considerations on the PPVPN operation are applicable to those in the softwire mesh solution [RFC4111].

Examples of attacks to data packets being transmitted on a softwire tunnel include:

1. An adversary may try to discover confidential information by sniffing softwire packets.

2. An adversary may try to modify the contents of softwire packets.

3. An adversary may try to spoof the softwire packets that do not belong to the authorized domains and to insert copies of once-legitimate packets that have been recorded and replayed.

4. An adversary can launch denial-of-service (DoS) attacks by deleting softwire data traffic. DoS attacks of the resource exhaustion type can be mounted against the data plane by spoofing a large amount of non-authenticated data into the softwire from the outside of the softwire tunnel.

5. An adversary may try to sniff softwire packets and to examine aspects or meta-aspects of them that may be visible even when the packets themselves are encrypted. An attacker might gain useful information based on the amount and timing of traffic, packet sizes, source and destination addresses, etc.

The security attacks can be mounted on the control plane as well. In the softwire mesh solution, softwire encapsulation will be set up by using BGP. As described in [RFC4272], BGP is vulnerable to various security threats such as confidentiality violation; replay attacks; insertion, deletion, and modification of BGP messages; man-in-the-middle attacks; and denial-of-service attacks.

4.4. Applicability of Security Protection Mechanism

Given that security is generally a compromise between expense and risk, it is also useful to consider the likelihood of different attacks. There is at least a perceived difference in the likelihood of most types of attacks being successfully mounted in different deployment.

The trust relationship among users in access networks, transit core providers, and other parts of networks described in Section 4.2 is a key element in determining the applicability of the security protection mechanism for the specific softwire mesh deployment.

4.4.1. Security Protection Mechanism for Control Plane

The "Softwire Problem Statement" [RFC4925] states that the softwire mesh setup mechanism to advertise the softwire encapsulation MUST support authentication, but the transit core provider may decide to turn it off in some circumstances.

The BGP authentication mechanism is specified in [RFC2385]. The mechanism defined in [RFC2385] is based on a one-way hash function (MD5) and use of a secret key. The key is shared between a pair of peer routers and is used to generate 16-byte message authentication code values that are not readily computed by an attacker who does not have access to the key.

However, the security mechanism for BGP transport (e.g., TCP-MD5) is inadequate in some circumstances and also requires operator interaction to maintain a respectable level of security. The current deployments of TCP-MD5 exhibit some shortcomings with respect to key management as described in [RFC3562].

Key management can be especially cumbersome for operators. The number of keys required and the maintenance of keys (issue/revoke/

renew) has had an additive effect as a barrier to deployment. Thus, automated means of managing keys, to reduce operational burdens, is available in the BGP security system ([BGP-SEC], [RFC4107]).

Use of IPsec counters the message insertion, deletion, and modification attacks, as well as man-in-the-middle attacks by outsiders. If routing data confidentiality is desired, the use of IPsec ESP could provide that service. If eavesdropping attacks are identified as a threat, ESP can be used to provide confidentiality (encryption), integrity, and authentication for the BGP session.

4.4.2. Security Protection Mechanism for Data Plane

To transport data packets across the transit core, the mesh solution defines multiple encapsulations: L2TPv3, IP-in-IP, MPLS (LDP-based and RSVP-TE based), and GRE. To securely transport such data packets, the softwire MUST support IPsec tunnel.

IPsec can provide authentication and integrity. The implementation MUST support ESP with null encryption [RFC4303] or else AH (IP Authentication Header) [RFC4302]. If some part of the transit core network is not trusted, ESP with encryption MAY be applied.

Since the softwires are created dynamically by BGP, the automated key distribution MUST be performed by IKEv2 [RFC4306] with either pre-shared key or public key management. For dynamic softwire IPsec tunnel creation, the pre-shared key will be the same in all routers. Namely, pre-shared key indicates here "group key" instead of "pairwise-shared" key.

If security policy requires a stronger key management, the public key SHOULD be used. If a public key infrastructure is not available, the IPsec Tunnel Authentication sub-TLV specified in [RFC5566] MUST be used before SA is established.

If the link(s) between the user’s site and the provider’s PE is not trusted, then encryption MAY be used on the PE-CE link(s).

Together with the cryptographic security protection, the access-control technique reduces exposure to attacks from outside the service provider networks (transit networks). The access-control technique includes packet-by-packet or packet-flow-by-packet-flow access control by means of filters as well as by means of admitting a session for a control/signaling/management protocol that is being used to implement softwire mesh.

The access-control technique is an important protection against security attacks of DoS, etc., and a necessary adjunct to

cryptographic strength in encapsulation. Packets that match the criteria associated with a particular filter may be either discarded or given special treatment to prevent an attack or to mitigate the effect of a possible future attack.

5. Security Considerations

This document discusses various security threats for the softwire control and data packets in the "Hubs and Spokes" and "Mesh" time-to-market solutions. With these discussions, the softwire security protocol implementations are provided by referencing "Softwire Problem Statement" [RFC4925], "Securing L2TP using IPsec" [RFC3193], "Security Framework for PPVPNs" [RFC4111], and "Guidelines for Specifying the Use of IPsec" [RFC5406]. The guidelines for the security protocol employment are also given considering the specific deployment context.

Note that this document discusses softwire tunnel security protection and does not address end-to-end protection.

6. Acknowledgments

The authors would like to thank Tero Kivinen for reviewing the document and Francis Dupont for substantive suggestions. Acknowledgments to Jordi Palet Martinez, Shin Miyakawa, Yasuhiro Shirasaki, and Bruno Stevant for their feedback.

We would like also to thank the authors of the Softwire Hub & Spoke Deployment Framework document [RFC5571] for providing the text concerning security.

7. References

7.1. Normative References

[RFC1994] Simpson, W., "PPP Challenge Handshake Authentication Protocol (CHAP)", RFC 1994, August 1996.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2385] Heffernan, A., "Protection of BGP Sessions via the TCP MD5 Signature Option", RFC 2385, August 1998.

[RFC2661] Townsley, W., Valencia, A., Rubens, A., Pall, G., Zorn, G., and B. Palter, "Layer Two Tunneling Protocol "L2TP"", RFC 2661, August 1999.

[RFC3193] Patel, B., Aboba, B., Dixon, W., Zorn, G., and S. Booth, "Securing L2TP using IPsec", RFC 3193, November 2001.

[RFC3947] Kivinen, T., Swander, B., Huttunen, A., and V. Volpe, "Negotiation of NAT-Traversal in the IKE", RFC 3947, January 2005.

[RFC3948] Huttunen, A., Swander, B., Volpe, V., DiBurro, L., and M. Stenberg, "UDP Encapsulation of IPsec ESP Packets", RFC 3948, January 2005.

[RFC4107] Bellovin, S. and R. Housley, "Guidelines for Cryptographic Key Management", BCP 107, RFC 4107, June 2005.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

[RFC4302] Kent, S., "IP Authentication Header", RFC 4302, December 2005.

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, December 2005.

[RFC4306] Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", RFC 4306, December 2005.

7.2. Informative References

[BGP-SEC] Christian, B. and T. Tauber, "BGP Security Requirements", Work in Progress, November 2008.

[RFC2401] Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

[RFC2409] Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November 1998.

[RFC2607] Aboba, B. and J. Vollbrecht, "Proxy Chaining and Policy Implementation in Roaming", RFC 2607, June 1999.

[RFC3562] Leech, M., "Key Management Considerations for the TCP MD5 Signature Option", RFC 3562, July 2003.

[RFC4016] Parthasarathy, M., "Protocol for Carrying Authentication and Network Access (PANA) Threat Analysis and Security Requirements", RFC 4016, March 2005.

[RFC4081] Tschofenig, H. and D. Kroeselberg, "Security Threats for Next Steps in Signaling (NSIS)", RFC 4081, June 2005.

[RFC4111] Fang, L., "Security Framework for Provider-Provisioned Virtual Private Networks (PPVPNs)", RFC 4111, July 2005.

[RFC4213] Nordmark, E. and R. Gilligan, "Basic Transition Mechanisms for IPv6 Hosts and Routers", RFC 4213, October 2005.

[RFC4225] Nikander, P., Arkko, J., Aura, T., Montenegro, G., and E. Nordmark, "Mobile IP Version 6 Route Optimization Security Design Background", RFC 4225, December 2005.

[RFC4272] Murphy, S., "BGP Security Vulnerabilities Analysis", RFC 4272, January 2006.

[RFC4364] Rosen, E. and Y. Rekhter, "BGP/MPLS IP Virtual Private Networks (VPNs)", RFC 4364, February 2006.

[RFC4593] Barbir, A., Murphy, S., and Y. Yang, "Generic Threats to Routing Protocols", RFC 4593, October 2006.

[RFC4891] Graveman, R., Parthasarathy, M., Savola, P., and H. Tschofenig, "Using IPsec to Secure IPv6-in-IPv4 Tunnels", RFC 4891, May 2007.

[RFC4925] Li, X., Dawkins, S., Ward, D., and A. Durand, "Softwire Problem Statement", RFC 4925, July 2007.

[RFC5216] Simon, D., Aboba, B., and R. Hurst, "The EAP-TLS Authentication Protocol", RFC 5216, March 2008.

[RFC5406] Bellovin, S., "Guidelines for Specifying the Use of IPsec Version 2", BCP 146, RFC 5406, February 2009.

[RFC5565] Wu, J., Cui, Y., Metz, C., and E. Rosen, "Softwire Mesh Framework", RFC 5565, June 2009.

[RFC5566] Berger, L., White, R., and E. Rosen, "BGP IPsec Tunnel Encapsulation Attribute", RFC 5566, June 2009.

[RFC5571] Storer, B., Pignataro, C., Dos Santos, M., Stevant, B., Toutain, L., and J. Tremblay, "Softwire Hub and Spoke Deployment Framework with Layer Two Tunneling Protocol Version 2 (L2TPv2)", RFC 5571, June 2009.

Appendix A. Examples

If the old IPsec architecture [RFC2401] and IKE [RFC2409] are used, the SPD examples in [RFC3193] are applicable to the "Hub & Spokes" model. In this model, the initiator is always the client (SI), and the responder is the SC.

A.1. IPv6-over-IPv4 Softwire with L2TPv2 Example for IKE

IPv4 addresses of the softwire initiator and concentrator are denoted by IPv4-SI and IPv4-SC, respectively. If NAT traversal is used in IKE, UDP source and destination ports are 4500. In this SPD entry, IKE refers to UDP port 500. * denotes wildcard and indicates ANY port or address.

Local	Remote	Protocol	Action
IPV4-SI	IPV4-SC	ESP	BYPASS
IPV4-SI	IPV4-SC	IKE	BYPASS
IPv4-SI	IPV4-SC	UDP, src 1701, dst 1701	PROTECT(ESP, transport)
IPv4-SC	IPv4-SI	UDP, src * , dst 1701	PROTECT(ESP, transport)

Softwire Initiator SPD

Remote	Local	Protocol	Action
*	IPV4-SC	ESP	BYPASS
*	IPV4-SC	IKE	BYPASS
*	IPV4-SC	UDP, src * , dst 1701	PROTECT(ESP, transport)

Softwire Concentrator SPD

A.2. IPv4-over-IPv6 Softwire with Example for IKE

IPv6 addresses of the softwire initiator and concentrator are denoted by IPv6-SI and IPv6-SC, respectively. If NAT traversal is used in IKE, UDP source and destination ports are 4500. In this SPD entry, IKE refers to UDP port 500. * denotes wildcard and indicates ANY port or address.

Local	Remote	Protocol	Action
IPV6-SI	IPV6-SC	ESP	BYPASS
IPV6-SI	IPV6-SC	IKE	BYPASS
IPv6-SI	IPV6-SC	UDP, src 1701, dst 1701	PROTECT(ESP, transport)
IPv6-SC	IPv6-SI	UDP, src * , dst 1701	PROTECT(ESP, transport)

Softwire Initiator SPD

Remote	Local	Protocol	Action
*	IPV6-SC	ESP	BYPASS
*	IPV6-SC	IKE	BYPASS
*	IPV6-SC	UDP, src * , dst 1701	PROTECT(ESP, transport)

Softwire Concentrator SPD

Authors' Addresses

Shu Yamamoto
NICT/KDDI R&D Labs
1-13-16 Hakusan, Bunkyo-ku
Tokyo 113-0001
Japan

Phone: +81-3-3868-6913
EMail: shu@nict.go.jp

Carl Williams
KDDI R&D Labs
Palo Alto, CA 94301
USA

Phone: +1-650-279-5903
EMail: carlw@mcsr-labs.org

Hidetoshi Yokota
KDDI R&D Labs
2-1-15 Ohara
Fujimino, Saitama 356-8502
Japan

Phone: +81-49-278-7894
EMail: yokota@kddilabs.jp

Florent Parent
Beon Solutions
Quebec, QC
Canada

EMail: Florent.Parent@beon.ca