



IPsec VPN Security between Aruba Remote Access Points and Mobility Controllers

Application Note

Revision 1.0
10 February 2011

IPsec VPN Security between Aruba Remote Access Points and Mobility Controllers

Table of Contents

Introduction	3
IPsec VPN setup and L2TP/PPP operation between the Aruba RAP and Mobility Controller	4

Introduction

ArubaOS supports the Layer 2 Tunneling Protocol (L2TP) with IPsec VPN client termination to create a VPN tunnel from an Aruba Remote Access Point (RAP) to an Aruba Mobility Controller at the data center or headquarters.

L2TP is a UDP protocol (Port 1701) that is used to tunnel a Layer 2 protocol like PPP across a Layer 3 network like the Internet. The RAP first sets up an IPsec tunnel (secure channel) and then sets up an L2TP tunnel within IPsec. It then starts a PPP connection within L2TP/IPsec, which is authenticated. The Mobility Controller assigns an inner-IP that the RAP uses for all traffic originating from it. The inner-IP packet is tunneled within PPP/L2TP and secured via the IPsec tunnel.

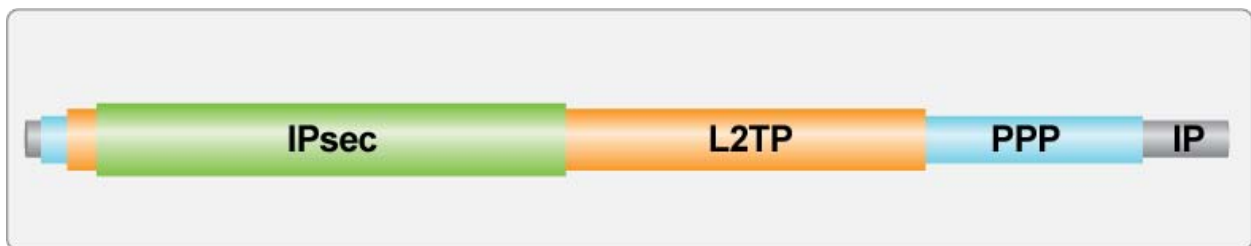


Figure 1 : Original IP packet is tunneled through an L2TP tunnel and encapsulated using IPsec encryption.

The Aruba Mobility Controller must have VPN server functionality configured to terminate the secure RAPs. The configuration consists of the authentication protocols, an address pool for RAPs, DNS information, shared secret for RAPs, and a policy governing the shared secret, including priority, encryption, hash algorithm, authentication, group and lifetime.

This document describes the steps involved in creating the secure IPsec channel between the RAP and the Mobility Controller, and highlights some of the key algorithms that are used in the IPsec tunnel negotiation and setup.

IPsec VPN setup and L2TP/PPP operation between the Aruba RAP and Mobility Controller

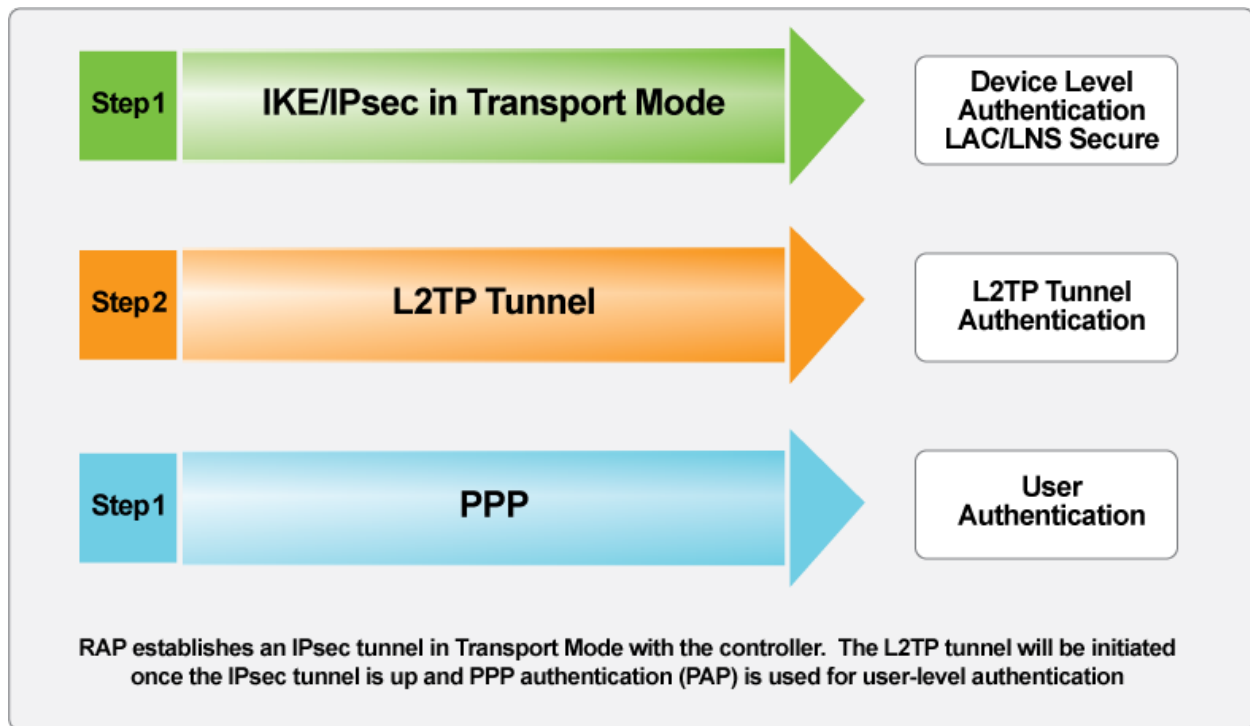


Figure 2 : IPsec secure tunnel and L2TP tunnel setup between the Aruba RAP and Mobility Controller.

Prior to sending any data from the remote sites to the data center or headquarters, the RAP (client) first sets up an IPsec tunnel and then sets up a L2TP tunnel within IPsec.

The process of setting up an L2TP/IPsec VPN between the Aruba RAP and Mobility Controller is as follows:

1. Internet key Exchange (IKE) protocol v1: The negotiation of IPsec security association (SA) is done using IKE v1. IKE authentication can be configured to use either pre-shared keys (PSK) or digital certificates to provide authentication (RSA Signature Algorithm).

IKE provides NAT-T capabilities for RAPs that may be behind a NAT device. If there is a NAT device in the path between the two VPN endpoints, the IKE protocol will automatically detect the presence of

the NAT device by comparing a set of hashes, which are based on the IP address and UDP port of the IKE packet. If there is a hash mismatch, IKE detects the presence of the NAT device.

In most implementations, IKE uses UDP Port 500 and UDP 4500. IKE sta

rts the initial negotiation with Port 500 and then floats the port to 4500 if NAT is detected. However, only Port 4500 has to be enabled to allow RAP to establish its tunnel to the Mobility Controller. The general recommendation is to enable both ports on the Internet-facing firewall to allow for wider compatibility with other operating systems. IKE can be configured to use Diffie-Helman (DH) groups 1 or 2 for the key exchange or for Perfect Forward Secrecy (PFS) in Phase 2. 160-bit SHA1 can be configured for Phase 1 and 2.

IKE also provides the Dead Peer Detection (DPD) functionality, which is the keep-alive mechanism that detects if the peer is down. The controller will not send out DPDs in the remote access scenario and will only respond with DPD ACKs to ensure that the RAP will keep the IKE/IPsec tunnels up.

On the Aruba Mobility Controller, which is the VPN termination point, the Policy Enforcement Firewall (PEF) and AP licenses¹ are required for VPN termination of the RAP. A RAP is identified by a specific vendor-ID during IKE main-mode SA establishment. This is used to check the number of APs that are connected to the controller. For more information regarding required licenses and the licensing limits, please refer to the user guide.

The second step is the creation of the IPsec Security Associations (IPsec SAs). This is Phase 2 of the VPN tunnel establishment and is the creation of the Encapsulating Security Payload (ESP) communication. The IP protocol number for ESP is 50. At this point, a secure channel or VPN tunnel has been established between the RAP and the Mobility Controller. The IPsec tunnel between the RAP and the Mobility Controller uses transport mode with L2TP.

IPsec Maximum Transmission Unit (MTU) can be configured – the default is set to 1550.

IPsec Encryption

The following cryptographic algorithms are available for encryption in ArubaOS: 3DES and AES 128-bit or 256-bit.

ESP-NUL is a no-encryption option and is also available. However, this is not a recommended option since it does not provide any data confidentiality.

¹ The AP license will apply to all APs connected to the controller regardless of whether they are campus APs, remote APs and mesh APs.

When the double encryption feature is enabled, data traffic from a wireless client connected to a tunneled SSID is encrypted at Layer 2. This encrypted data is then re-encrypted in the IPsec tunnel that is setup from the RAP to the Mobility Controller. Disabling the double encryption will cause the wireless frames to be encrypted only using IPsec from the RAP to the Mobility Controller.

However, the 802.11 traffic from the client to the RAP will be sent in the clear. The recommendation is to always use WPA/WPA-2, TKIP or AES encryption for the 802.11 traffic, even though the traffic is being re-encrypted with IPsec from the RAP to the Mobility Controller.

2. Once the IPsec tunnel (Phase 2) has been created, the negotiation and establishment of the L2TP tunnel happens between the SA endpoints. The actual negotiation of parameters takes place over the SA's secure channel and within the IPsec encryption.

The L2TP packets between the endpoints are ESP encapsulated by IPsec, which ensures the security of the internal private network.

A key point to note is that the L2TP port, UDP 1701, does not have to be open on the firewall since the L2TP packets are encrypted and will not be processed until after decryption, which happens on the endpoints (RAP and Mobility Controller).

With IKE and L2TP/PPP, two-level authentication is supported – device authentication and user authentication. Password authentication protocol (PAP) is the method of authentication supported for the RAP client.

L2TP hellos detect if the peer is gone, bring down the L2TP tunnel and then signal IKE to bring down the IKE/IPsec tunnel. This can be configured on the Mobility Controller.

In the tunnel mode of operation, the 802.11 data packets, action frames and EAPOL frames are sent to the Mobility Controller. They are not processed on the Remote AP. The 802.11 data packets and frames are encapsulated in GRE and sent over the IPsec tunnel to the Mobility Controller.

© 2011 Aruba Networks, Inc. AirWave®, Aruba Networks®, Aruba Mobility Management System®, Bluescanner, For Wireless That Works®, Mobile Edge Architecture®, People Move. Networks Must Follow®, RFprotect®, The All Wireless Workplace Is Now Open For Business, Green Island, and The Mobile Edge Company® are trademarks of Aruba Networks, Inc. All rights reserved. Aruba Networks reserves the right to change, modify, transfer, or otherwise revise this publication and the product specifications without notice. While Aruba uses commercially reasonable efforts to ensure the accuracy of the specifications contained in this document, Aruba will assume no responsibility for any errors or omissions. Note: All scaling metrics outlined in this document are maximum supported values. The scale may vary depending upon the deployment scenario and features enabled.

