WHITE PAPER

IPSEC UDP MODE IN ARUBA EDGECONNECT

aruba
a Hewlett Packard Enterprise company

TABLE OF CONTENTS

CHALLENGES WITH TRADITIONAL IKE BASED IPSEC

Traditional site-to-site IP VPNs use IKE (Internet Key Exchange) to establish a security association (SA) between two endpoints. While traditional IKE has been well-established as the control plane for IPSec VPNs, it suffers from the following challenges.

Operating With Address Translation

In order to conserve and protect private address spaces, enterprises deploy Network Address translation (NAT) which can be limited to just addresses (NAT) or ports (PAT). This can be implemented by enterprise IT teams or by carriers that provide WAN transport or by both. When implemented by carriers, it is referred to as Carrier-Grade NAT (CG-NAT). The NAT traversal feature in IKE helps solve the address translation problem to some extent. However, it fails if there are multiple devices at the branch, including other non-Aruba devices like client machines, laptops, mobile devices, other branch firewalls and routers that may have their own VPN requirements.

When 4G LTE WAN circuits are used, network admins cannot dedicate public static IP addresses. A reliable mechanism is needed to connect the different branch appliances through different carrier networks and addressing schemes.

Disabling Stolen Devices

IPsec with IKE was designed for an environment where the parties on both sides of a connection don't trust each other. IKE traditionally provides pre-shared keys or certificate-based authentication. Public Key Infrastructure (PKI) or Certificate authentication is considered better than pre-shared keys for authentication and key distribution, as it is based on digital signatures and a trusted hierarchical model.

However, the PKI model falls short when handling stolen appliances. Those appliances can still communicate to the network until the certificates expire in days, weeks or months or until they are revoked by human intervention. If many appliances are involved, it is far more complicated to revoke all of them. Therefore, the PKI model alone is not sufficient for SD-WAN networks with branch appliances.

Secure Scalability Challenge

SD-WAN network topologies can be hub and spoke or full mesh or both. The number of sites can be several hundreds or even thousands. IPsec with IKE is intended for site-to-site VPNs and is not designed for full mesh IPsec connections in an SD-WAN network; it poses a problem of exponential complexity in an SD-WAN network. For example, n sites in a fully meshed topology require (n*(n-1))/2 tunnels, which can be approximated by n2. Operationally, managing key distribution, key rotation or rekey and tunnel setup and teardown for thousands of tunnels in a secure and timely manner without loss of network or site availability is very complex, time-consuming and subject to human error. Although PKI solves the key distribution problem better than pre-shared keys, in that there are no shared secrets, PKI still requires n2 key material negotiations and does not solve the scalability challenge.

Blocking By Nation State Firewalls

Traditional IKE uses well known ports – port 500 – so it is easy for a nation state to configure its firewall to block IKE.

Rate-Limiting By Carriers

Carriers providing WAN transport can also rate-limit or block traffic easily as the ports are well known.

WHAT IPSEC UDP SOLVES

A Aruba EdgeConnect SD-WAN builds its virtual WAN overlays, referred to as Business Intent Overlays, using end-to-end IPsec VPN tunnels. IPsec UDP mode, also known as 'IKE-less' mode, is used. This is the recommended and default mode of automatically setting up IPsec tunnels between EdgeConnect appliances. It is extremely flexible, secure and robust and is deployed in production by many Aruba global customers. Aruba also supports the legacy IKE mode to build third party IPsec tunnels with non-Aruba devices.

IPsec UDP mode uses standards-based IPsec encryption, with standard UDP encapsulation. The control channel, however, does not use IKE, but uses the Aruba Orchestrator for authentication, key distribution and management.

Orchestrator is a trusted entity. It is deployed in the enterprise data center and is a protected asset. Aruba also provides a fully-managed Cloud Orchestrator that is implemented on an SOC-3 and FedRAMP compliant AWS infrastructure. In either case, Orchestrator performs the function of a Certificate Authority in terms of distributing key material and authenticating EdgeConnect appliances.

IPsec UDP tunnels help solve the following challenges and issues:

Operating With Address Translation

- Multiple IPsec devices at the same branch
  IPsec UDP mode in EdgeConnect supports NAT traversal, PAT and CG-NAT. In a particular branch, there may be more than one EdgeConnect appliance in standalone or EdgeConnect HA mode. There may be other non-Aruba devices with VPN requirements.
- Support 4G LTE WAN circuits
  When 4G LTE is used as a WAN circuit, it is not possible to dedicate static public IPs for the branch. IP addresses change in an LTE circuit and there is added complexity when LTE is used with other wireline (ethernet, fiber) WAN circuits that have different address translation mechanisms.

In all cases of address translation, the IPsec UDP mode helps reliably connect one or more devices at the branch to other branches, hubs, data centers or the internet through different forms of NAT. More detailed use cases are discussed in the NAT section below.

Exposure From Stolen Devices is Strictly Contained

By using a trusted entity like Aruba Orchestrator in the data center or hosted in the cloud, EdgeConnect simplifies the authentication process, to provide security at all times in the lifecycle of an appliance. If an appliance is stolen, lost in shipment or RMA-ed, it cannot contact the Orchestrator in the data center or cloud and key rotation fails. The appliance is automatically removed from the network and alarms are sent to the administrator. A stolen device can also be immediately taken out of the network by an IT administrator with a single click in the Orchestrator.

Secure Scalability and Operational Efficiency With Orchestration

Aruba uses unique encryption keys that are never repeated. For example, the encryption key for tunnels is directionally unique; the key for tunnels between appliances A->B is different from that for tunnels between appliances B->A. Key rotation ensures that a possible future compromise does not affect previous tunnels between the two appliances since the encryption key at any point in time cannot be used to derive past encryption keys. Aruba Orchestrator is employed to manage the unique encryption keys which reduces the tunnel setup time required with IKE. This is efficient for SD-WAN networks with hundreds and thousands of tunnels. Re-key or key rotation happens in a timely manner and there is no loss of service when tunnels are re-keyed.

Traversal of Nation State Firewalls

Aruba has several successful implementations of IPsec UDP tunnels deployed by global enterprises in countries where there is a known nation state firewall.

Mitigation of Carrier Rate Limiting

Multiple, different UDP ports over IPsec can be easily orchestrated for hundreds of sites. This makes it more difficult for carriers to rate limit or block the traffic using upstream firewalls.

TABLE 1. COMPARISON OF PRE-SHARED KEYS, PKI AND IPSEC UDP

Properties	IKE Pre-shared keys with IPsec	IKE PKI based auth with IPsec	Aruba "IKEless" IPsec UDP
Blocking & rate limiting	Easy to block ports 500, 4500	Easy to block ports 500, 4500	Cannot block changing UDP ports
Multiple VPN devices behind NAT	Cannot distinguish multiple IPsec devices behind upstream NAT	Cannot distinguish multiple IPsec devices behind upstream NAT	NAT discovery and NAT traversal helps solve the multiple devices with VPNs and NAT problem
Exposure from stolen devices	No protection	Cannot protect as is; needs proper revocation management in place; also requires human intervention to revoke certificates	Stolen device cannot communicate with the SD-WAN network after the next key rotation interval since it cannot reach Orchestrator in the customer's data center; an administrator can permanently revoke access to the device by removing the device approval in the Orchestrator
Scalability	Though pre-shared keys (PSKs) are simpler to manage, it still requires n2 key negotiations for n sites in full mesh	Uses device certificates for authentication; still requires n2 key negotiations and extensive certificate lifecycle management	Key negotiation, rotation happens automatically and in a timely manner for hundreds/thousands of appliances
Operational efficiency	Need to configure PSKs for all tunnel pairs for hundreds or thousands of devices	Need to manage certificates and their lifecycle for hundreds or thousands of devices	Automatically managed by the Orchestrator
Key distribution and management	Uses insecure common shared secrets to build tunnels	Uses unique keys per tunnel, per device pair, per direction but requires extensive certificate lifecycle management maintained by IT admins	Uses unique keys per tunnel, per device pair, per direction, and they are automatically maintained by the Orchestrator for hundreds/thousands of appliances
Confidentiality and integrity	End-to-end encryption (using default AES-256-CBC), SHA1-SHA512 HMAC		

HOW IPSEC UDP WORKS

The following is a deeper technical drill-down on some of the properties of IPsec UDP tunnels in the Aruba EdgeConnect SD-WAN edge platform.

Secure Zero Touch Provisioning and Authentication

Secure provisioning and authentication ensure that only authorized appliances are admitted into the SD-WAN network at all times. It is "zero touch," because the provisioning of new appliances into the SD-WAN requires no special onsite IT administrators to install and configure appliances at a branch.

Device level authentication is performed through secure TLS in the management plane. The Aruba Cloud Portal and Orchestrator are trusted entities.

Cloud Portal maintains relevant licensing information, including the account name and key, licensing information, and asset serial numbers.

Customer administrators approve and authorize EdgeConnect SD-WAN appliances into the network. In addition, Orchestrator also supports multi-factor authentication to ensure additional access control. If a device is compromised, stolen or needs to be decommissioned, the customer admin can remove the device's authentication and approval from Orchestrator with one click. A stolen device can also be automatically deprovisioned through key rotation. This is discussed in the section on Key Distribution and Management.

In all cases, an unauthorized or stolen device cannot connect to the SD-WAN network; it cannot download a configuration or build tunnels and is excluded from joining the network.

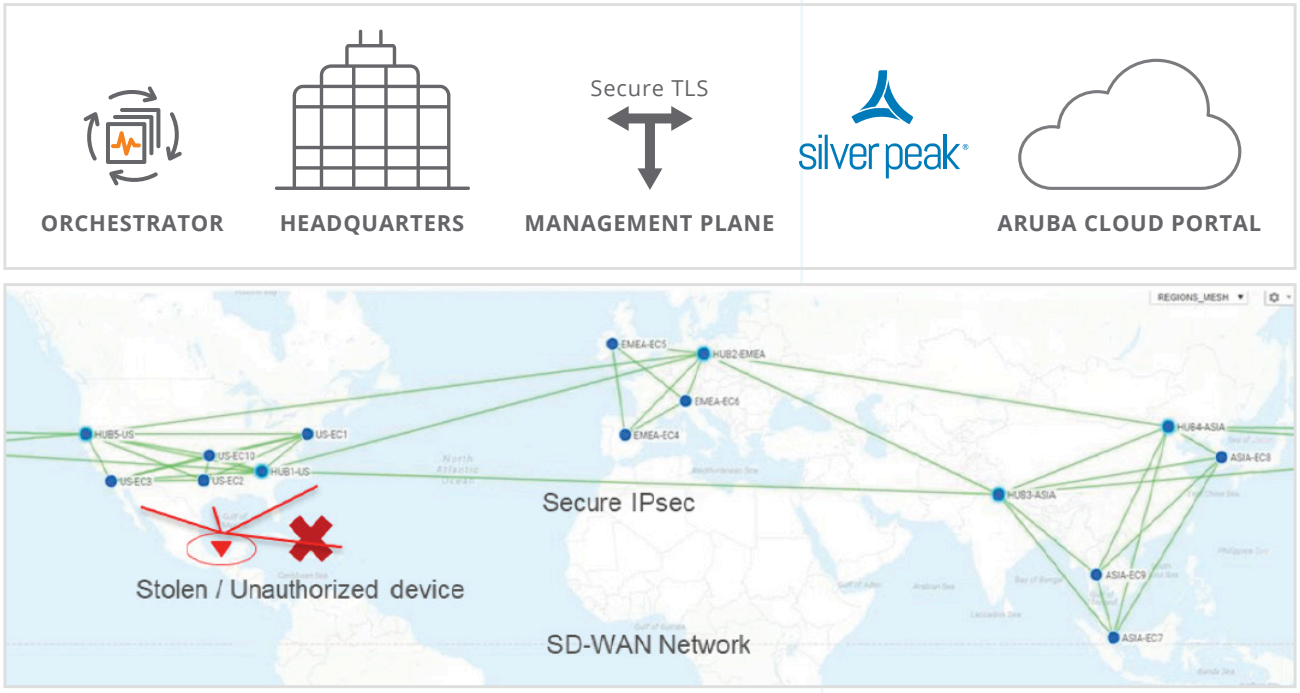


Figure 2. Secure zero-touch provisioning and authentication

Key Distribution and Management

Orchestrator automatically manages all elements of key distribution and key rotation. It generates and distributes ephemeral key material to all EdgeConnect appliances in the network and distributes them over secure TLS connections. Ephemeral key material rotation happens every 24 hours. It can be configured to be rotated as frequently as every 60 minutes if desired. Each EdgeConnect appliance also has persistent key material to encrypt communications between a pair of appliances, per direction. So, the data encryption key for the IPsec tunnel between appliances A->B is derived by combining the ephemeral key material and the persistent key material. The encryption key for the IPsec Security Association (SA) between appliances A->B is different from the key for the SA between appliances B->A.

Failure Handling and Orchestrator Reachability

Orchestrator distributes key material to all EdgeConnect appliances in the network. Just before the end of a key rotation interval, Orchestrator activates new ephemeral key material for all of the EdgeConnect appliances in the SD-WAN network. The appliances should be reachable to the Orchestrator for the key material activation. However, there are two cases of unreachability:

1. Inactive appliances: When appliances are inactive, they exist in the Orchestrator, but do not have tunnels configured to any 'active' appliances.

2. Temporary unreachability: Temporary unreachability issues occur in cases where an EdgeConnect appliance reboots or if there is a link or communication failure. In this case, Orchestrator will not activate the new key material until all active appliances are reachable and have received the new key material. If the appliance is unreachable for a period longer than the key rotation interval, it will be treated as an inactive appliance.

Re-authorization: Inactive appliances that become active at a later point in time, will be reauthorized to receive the current key material. Only then they will be able to download configuration and build tunnels.

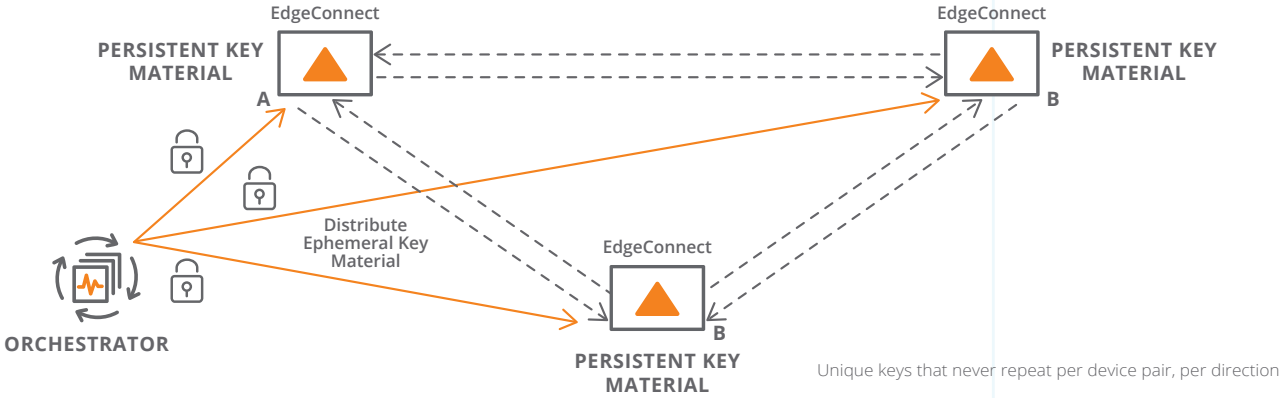
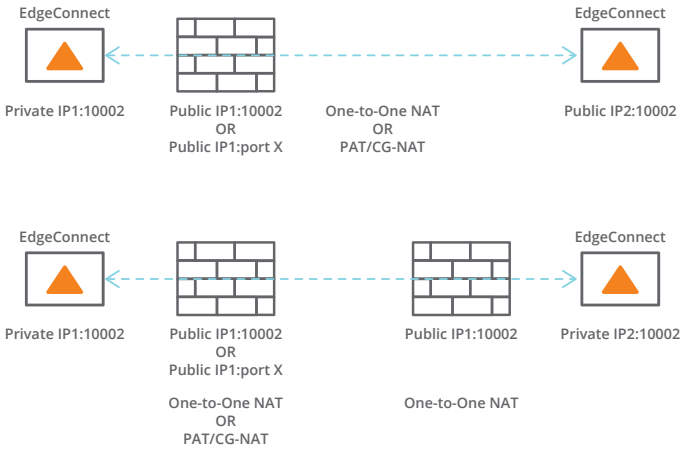


Figure 3. Aruba IPsec Key Management

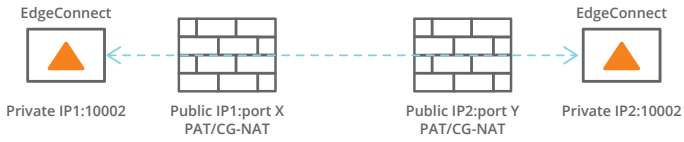
Support for NAT

The following are the use cases or combinations of possible types of NAT between any pair of connected EdgeConnect appliances. UDP source ports indicated below are assigned by the Orchestrator for IPsec UDP tunnels. The firewall devices shown by black icons, indicated below, depict upstream NAT performed by the enterprise or by carriers. Port 10002, 11002 are default IPsec UDP ports used by Aruba.



Unsupported Use Case:

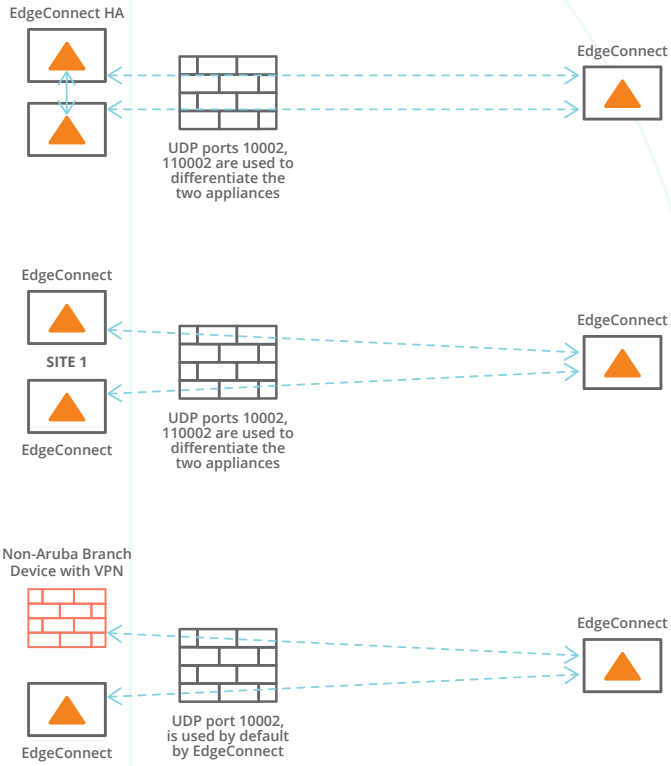
Currently, CG-NAT or PAT at both ends is not supported. This is usually eliminated by having one-to-one NAT or public IP addresses on the other end as depicted in the earlier use case.



Multiple Branch Devices

Multiple Aruba EdgeConnect appliances at a branch can be configured in EdgeConnect HA mode. There may also be multiple appliances at a site that are not configured for HA. There can be other non-Aruba devices at the branch that operate their own VPNs. All of these deployment options may be supported at a branch.

As depicted in the Support for NAT section, an Edge HA configuration of the EdgeConnect appliances at the remote destination can have a public IP address, one-to-one NAT but not PAT or CG-NAT.



PACKET FORMATS

Control Plane

IKE or ISAKMP packets are used to negotiate the control channel in legacy 'IPsec' mode that uses IKE. Since UDP ports 500 are used for source and destination, it can be easily blocked.

Figure 4. IKE/ISAKMP packet

Data Plane

Traditional Ike, Ipsec Packet Formats

The original packet to be encrypted is a regular TCP/IP or UDP/IP packet. Hereafter, it is referred to as 'Encrypted Packet' in the subsequent IPsec packets.

Figure 5. Original packet (to be encrypted)

Figure 6. Traditional IPsec (ESP) packet

Figure 7. Traditional IPsec (ESP) packet with NAT-Traversal

Aruba Overlay Encapsulations

Aruba encapsulation shown in green uses a GRE header to encapsulate a proprietary Aruba header. Aruba header contains fields for loss, latency measurements, overlay identification and WAN optimization.

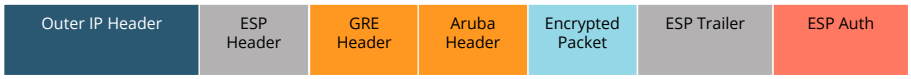


Figure 8. Traditional IPsec (ESP) packet Aruba encapsulation

When NAT Traversal is on in the legacy IPsec mode (with IKE), the UDP source/destination ports are 4500. They can be easily blocked by ISPs or nation state firewalls.

Figure 9. Traditional IPsec (ESP) packet with NAT-Traversal and Aruba encapsulation

IPsec UDP with Aruba encapsulations use configurable UDP ports for source and destination which makes it difficult to block by ISPs or nation state firewalls.

Figure 10. IPsec UDP (ESP) packet with Aruba encapsulation

CONCLUSION

With more than 1,000 EdgeConnect production deployments around the world and growing, Aruba has gained extensive field experience providing secure SD-WAN solutions for the world's largest global enterprises. IPsec UDP deployments comprise approximately 15 percent of these deployments to date and are rapidly increasing as security concerns become an increasing important SD-WAN criterion. Aruba provides the most holistic approach to SD-WAN security in the industry including a robust IPsec UDP implementation for EdgeConnect-to-Edge- Connect secure tunnels and business intent overlays.

FAQ

1. Can I still use standard IKE/IPsec instead of IPsec UDP for EdgeConnect to EdgeConnect tunnels?

Yes, the legacy 'IPsec' mode, which is IPsec with IKE is still supported.

2. What about IPsec to non-Aruba devices?

The legacy 'IPsec' mode (with IKE) is used to build tunnels to non-Aruba devices supporting standards-based IPsec.

3. Is there a pre-shared key per overlay or a pre-shared key per overlay and connection?

It is not a pre-shared key. The data path key is unique to an appliance, per tunnel, per direction per key rotation interval. It consists of an ephemeral key material that changes every hour and a persistent key material per tunnel. See the key distribution and management section for details.

4. Is there a separate unidirectional key for each overlay for encrypting the traffic between two nodes?

Each direction of each underlay tunnel is assigned a unique encryption key that changes every hour.

5. How is the random seed (key material) generated for IKE-less IPsec?

We use the Java random number library in Orchestrator for generating all of the key material for both the ephemeral and persistent keys.

6. How are the data encryption keys derived in in IPsec UDP/IKEless IPsec?

Data encryption key = ephemeral key material + persistent key material

(ephemeral key material changes every hour, so the data encryption key changes every hour)

The data encryption key is unique per appliance, per underlay tunnel, per direction, per key rotation interval.

7. How are the data encryption keys exchanged when using IPsec UDP/IKE-less IPsec?

Keys are not exchanged because Orchestrator communicates with the EdgeConnect devices and provides the key material for the devices to generate the keys themselves. So, the data encryption keys are never sent out on the wire.

8. What additional authentication is provided by the Orchestrator to be granted write/push access to the EdgeConnect devices?

Aruba uses server certificates and TLS1.2 sessions to authenticate and encrypt communication between Orchestrator and EdgeConnect.

9. Orchestrator acts as the key server for PSKs and random seed. Can the role of Orchestrator as the key server be limited to zero in order to limit dependencies and to reduce the attack surface?

Orchestrator is a trusted entity. Apart from key distribution and management, it configures and manages the entire network. Orchestrator is a vital part of the SD-WAN solution and it is important that it is secured in the data center. According to Aruba SD-WAN management best practices, control of the Orchestrator is more critical than the control of the keys.

10. Are there plans to support certificates? If yes, what are they?

We support device certificates for the EdgeConnect and Orchestrator. We plan to add support for certificate authentication (PKI) for third party IPsec tunnels. For EdgeConnect to EdgeConnect overlays, we recommend using IPsec UDP as it is more secure. Refer to the section on What IPsec UDP solves.

11. What changes are made to the original packet when assigned to an overlay? Alternatively, what changes are made to the packet during encryption?

The packet payload and IP header can be compressed when Aruba Boost WAN Optimization is applied. A Aruba packet header and trailer may be added. IPsec UDP encapsulation is added after these functions. On the receiving side, the EdgeConnect appliance reverses the process to recover the contents of the original packet. The Packet Format section has more details.

12. Is a strict header check taking place for the data plane?

Yes, the packet is dropped if there are errors in the header.

13. How are external third-party network encryption products supported?

Customers are welcome to deploy transparent third-party encryption devices. We also interoperate with other third-party network encryption products through IPsec with IKE.

14. Are there plans to support PCI-based third-party encryption boards?

Not at this time. We use the Intel AES-NI instruction set, and it provides more than 5Gbps of throughput per CPU core which is more than sufficient for our SD-WAN and WAN Optimization applications.

15. How does IPsec UDP's provisioning and Orchestration compare with the properties of standards-based PKI or certificate authentication?

See table below.

TABLE 2.

Standards-based Public Key Infrastructure (PKI) or Certificate Authentication	IPsec UDP Secure Provisioning and Orchestration
Certificate Authorities like Verisign, Comodo are trusted.	Aruba Cloud Portal, Orchestrator are trusted (organizational compliance ensures this).
Authentication, authorization is provided by certificate parameters. It is NOT a two-step process. Additional multi-factor authentication is optional.	Two-step authentication, authorization with multi-factor authentication supported by Orchestrator. Aruba Cloud portal has account key, authorized serial numbers, #base licenses for account. Customer admins approve, authorize appliances into the network.
Stolen appliances – Certificate expiry and revocation handles device lifecycle, managed by customer's IT admins.	Stolen appliances – Customer revokes access through the Orchestrator; simpler lifecycle management by Aruba.
Unauthorized appliances – cannot establish TLS connection, needs revocation by enterprise IT.	Unauthorized appliances – drop all traffic, additional advantage: cannot download configuration.
Non-repudiation – The assurance that someone cannot deny something is provided via digital signature in the certificate.	Non-repudiation – This assurance is provided when customer clicks 'authorize' in the Orchestrator.

aruba
a Hewlett Packard Enterprise company

WP_IPsecUDPMode_101221 a00118462enw

Contact Us