CSA GCR cloud security GREATER CHINA REGION alliance ®

腾讯安全

CSA SDP2.0标准发布
暨零信任技术研讨会

SDP2.0标准规范详解

陈本峰 CSA（大中华区）零信任工作组组长、云深互联创始人

2022/05/17

- SDP v2.0概况
- SDP v2.0详解
- SDP 未来研究

零信任SDP的政策指导

《网络安全产业高质量三年行动计划（征求意见稿）》中提出“软件定义边界”(SDP)保障云安全

中华人民共和国工业和信息化部
Ministry of Industry and Information Technology of the People's Republic of China

访客预约 | RSS订阅

统一搜索

看新闻 找文件 查办事 提意见 查数据 要投诉

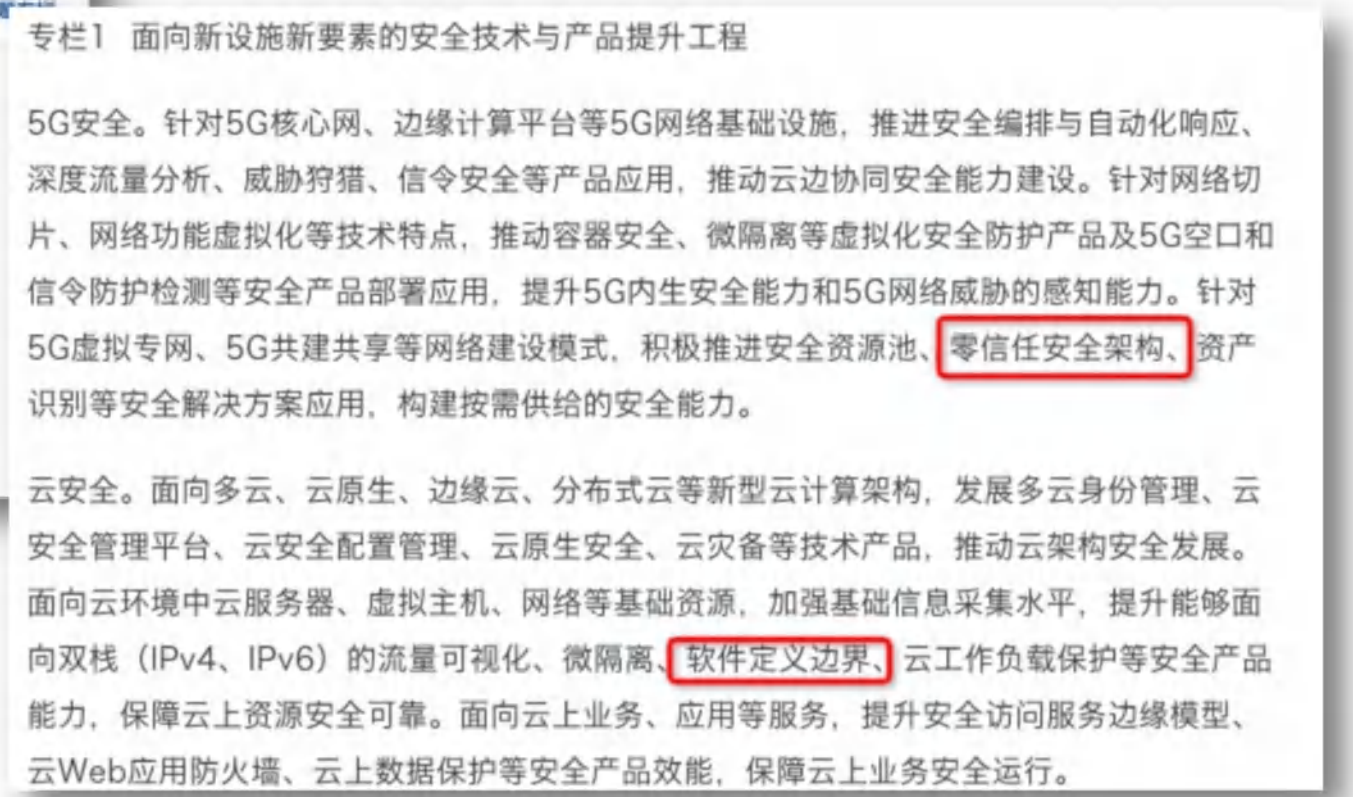
工业和信息化部 新闻动态 政务公开 政务服务 公众参与 工信数据

首页 > 公众参与 > 意见征集

公开征求对《网络安全产业高质量发展三年行动计划（2021-2023年）（征求意见稿）》的意见

状态：已结束 发布日期：2021-07-12 截止日期：2021-07-16 来源：网络安全管理局

为深入贯彻党中央、国务院关于制造强国和网络强国的战略决策部署，落实《中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要》有关要求，加快推动网络安全产业高质量发展，提升网络安全产业综合实力，工业和信息化部起草了《网络安全产业高质量发展三年行动计划（2021-2023年）（征求意见稿）》（见附件）。为进一步听取社会各界意见，现予以公示。如有意见或建议，请于2021年7月16日（周五）前反馈。



专栏1 面向新设施新要素的安全技术与产品提升工程

5G安全。针对5G核心网、边缘计算平台等5G网络基础设施，推进安全编排与自动化响应、深度流量分析、威胁狩猎、信令安全等产品应用，推动云边协同安全能力建设。针对网络切片、网络功能虚拟化等技术特点，推动容器安全、微隔离等虚拟化安全防护产品及5G空口和信令防护检测等安全产品部署应用，提升5G内生安全能力和5G网络威胁的感知能力。针对5G虚拟专网、5G共建共享等网络建设模式，积极推进安全资源池、零信任安全架构、资产识别等安全解决方案应用，构建按需供给的安全能力。

云安全。面向多云、云原生、边缘云、分布式云等新型云计算架构，发展多云身份管理、云安全管理平台、云安全配置管理、云原生安全、云灾备等技术产品，推动云架构安全发展。面向云环境中云服务器、虚拟主机、网络等基础资源，加强基础信息采集水平，提升能够面向双栈（IPv4、IPv6）的流量可视化、微隔离、软件定义边界、云工作负载保护等安全产品能力，保障云上资源安全可靠。面向云上业务、应用等服务，提升安全访问服务边缘模型、云Web应用防火墙、云上数据保护等安全产品效能，保障云上业务安全运行。

SDP标准规范概况

SDP v2.0 标准规范

	V1.0	V2.0
页数	**28**	**39**
发布时间	**2014.04**	**2022.04**
编写周期	**2013~2014**	**2019 ~2022**
参编作者	**13位**	**9位**

秉承CSA精神，SDP 2.0是一项国际合作的成果

Acknowledgments

Lead Authors

Jason Garbis
Juanita Koilpillai

Contributors

Junaid Islam
Bob Flores
Daniel Bailey
Benfeng Chen
Eitan Bremler
Michael Roza
Ahmed Refaey Hussein

Special Thanks

Larry Hughes

Reviewers

Alistair Cockeram
Takahiro Ono
T Prasad
Nya Murray
Michael Rash

CSA Analyst

Shamun Mahmud

CSA Global Staff

Claire Lehnert

Version 1.0 Contributors

Brent Bilger, Alan Boehme, Bob Flores, Zvi Guterman, Mark Hoover, Michaela Iorga, Junaid Islam, Marc Kolenko, Juanita Koilpillai, Gabor Lengyel, Gram Ludlow, Ted Schroeder and Jeff Schweitzer

CSA Analyst

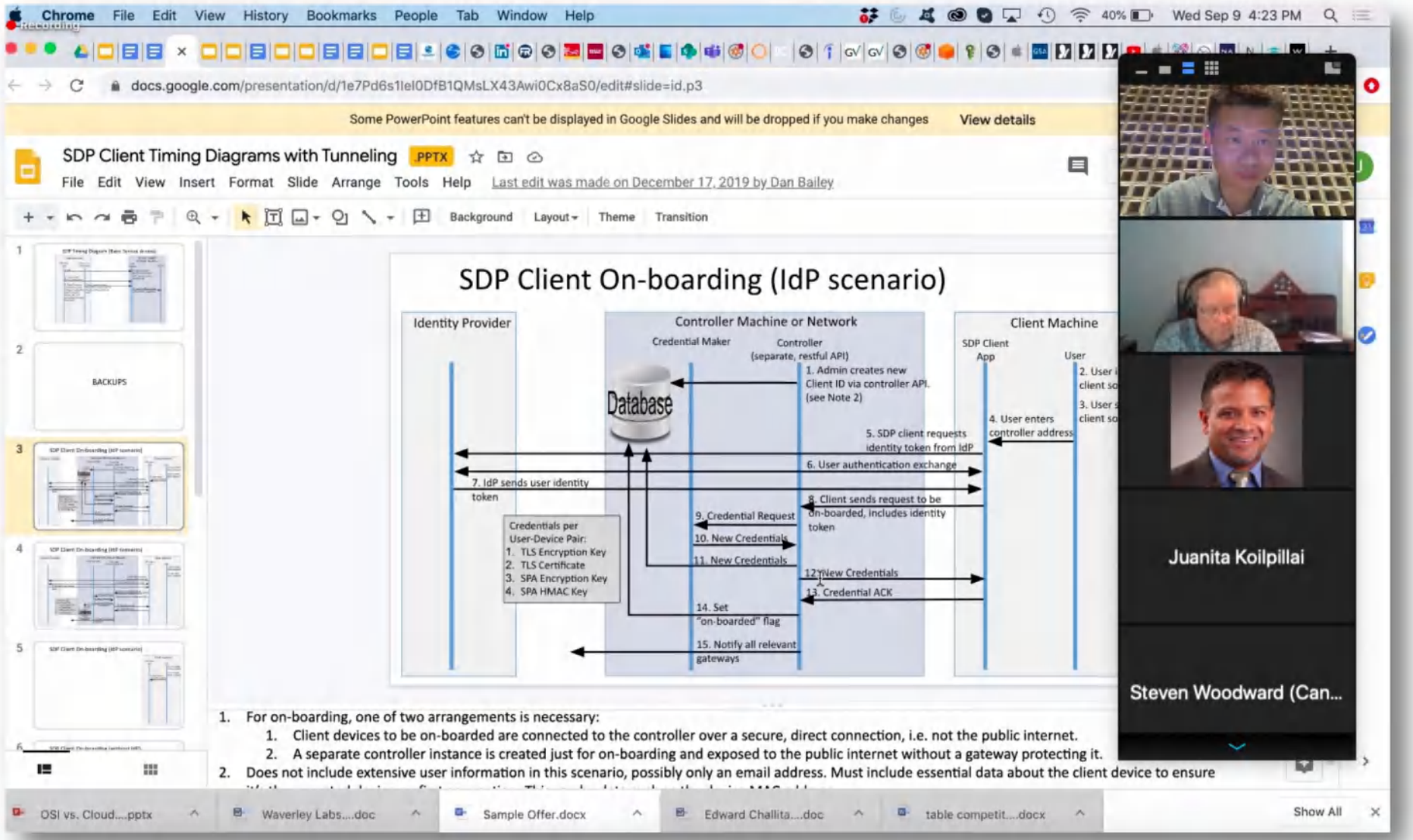
The Software-Defined Perimeter (SDP) and Zero Trust Working Group is a Cloud Security Alliance (CSA) research working group that advocates for and promotes the adoption of Zero Trust security principles. It provides practical and sound guidance on how to apply Zero Trust to cloud and non-cloud environments. This group will build on and leverage the NIST Zero Trust research and methodologies. It will recommend SDP as a fundamental architecture for applying Zero Trust principles. It will revise and expand the SDP specification, to capture and codify a wealth of knowledge based on experience. Lastly, the SDP group recognizes the need for an inclusive approach to SDP. As such, it also supports alternative architectures so long as they align with Zero Trust principles.

Benfeng Chen （陈本峰）

SM3国密算法

ClientID	256-bit numeric identifier, assigned per user-device pair. This field is used to distinguish the user, device, or logical group that is sending the packet.
Nonce	16-bit random data field prevents replay attack by avoiding SPA packet reuse
Timestamp	Prevents servicing outdated SPA packets, by ensuring a short time period of validity (for example, 15 to 30 seconds). This also provides a mechanism to reduce the replay-detection caching required for the recipient.
Source IP Address	The *publicly visible* IP address of the initiating host. This is included so that the Accepting Host does not rely on the source IP address in the packet header, which is easily modified en route. The IH must be able to obtain the IP address for use by the AH as the origination of packets.
Message Type	This field is optional - it may be used to inform the recipient what type of message to expect from the IH after the connection is established.
Message String	This field is optional and will be dependent on the Message Type field. For example, this field could be used to specify the services that an IH will be requesting if known at connection time.
HOTP	This hashed one-time password (hashed OTP) is generated by an algorithm as described by RFC 4226, based on a shared secret. The use of an OTP is required in SPA packets to establish authenticity; other OTP algorithms can be substituted with the overarching goal of providing authenticity of the SPA packet.
HMAC	Calculated over all fields above. Algorithm choices are SHA256 (recommended), SHA384, SHA512, SM3, Equihash, or other efficient and robust algorithms. The HMAC is calculated using a shared (secret) seed. The HMAC is calculated over all prior fields of the message and then used by the AH to verify message integrity. The HMAC validation is computationally lightweight, and therefore can be used to provide resiliency against DoS attacks. Any SPA packets with invalid HMACs are immediately discarded.

SDP 2.0标准规范编委会会议



SDP 2.0标准规范中文版

SDP v2.0 标准规范（中文版） 编委会

感谢以下**专家**共同编译SDP v2.0 （排名不分先后）：

- 组 长：陈本峰
- 专家组：单美晨、何国锋、何伊圣、贺志生、黄超、梁小毅、林冠烨、刘洪森、穆珹博、秦益飞、苏泰泉、汪海、王彪、王贵宗、王亮、许木娣、姚凯、于新宇、余强、余晓光

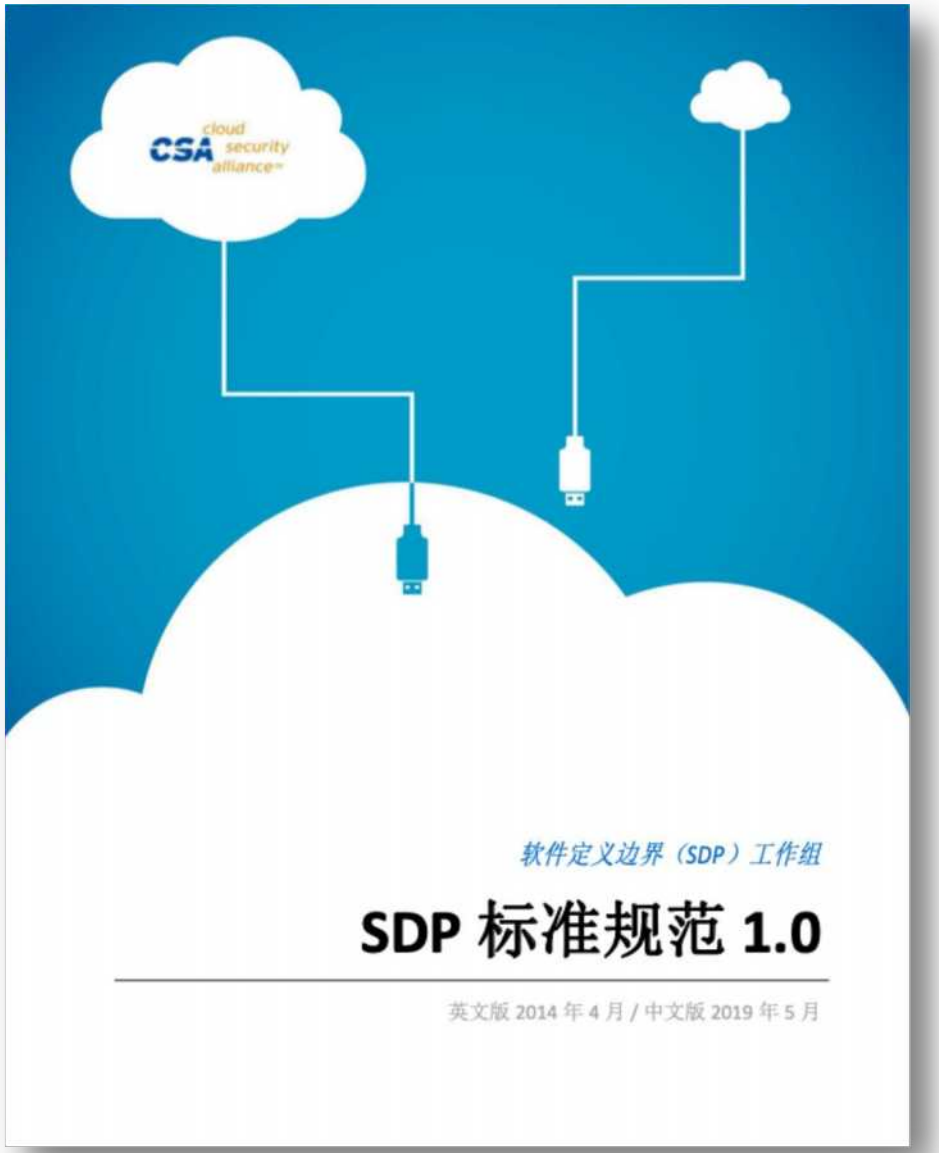
SDP 2.0标准规范中文版

SDP v2.0 标准规范（中文版） 编委会

感谢以下**单位**对本次中文版编译的支持 （排名不分先后）：

- 云深互联(北京)科技有限公司
- 中国信息通信研究院
- 中国电信研究院安全技术研究所
- 腾讯云计算（北京）有限责任公司
- 深信服科技股份有限公司
- 上海安几科技有限公司
- 北京山石网科信息技术有限公司
- 启明星辰信息技术集团股份有限公司
- 江苏易安联网络技术有限公司
- 华为技术有限公司
- 北京奇虎科技有限公司
- 北京天融信网络安全技术有限公司
- 安易科技（北京）有限公司
- 北京北森云计算股份有限公司
- 北京中宇万通科技股份有限公司
- 北京赛虎网络空间安全技术发展有限公司

SDP 1.0标准规范中文版



SDP v1.0 标准规范（中文版） 编委会

感谢以下**专家/单位**支持编译SDP v1.0 （排名不分先后）：

- 组长：陈本峰（云深互联）
- 组员：靳明星（易安联）、李钠（奇安信）、吴涛（华云数据）、袁初成（缔安科技）、张泽洲（奇安信）、刘洪森、王贵宗、姚凯
- 研究协调员：高健凯、朱晓璐

- SDP v2.0概况
- SDP v2.0详解
- SDP 未来研究

SDP 2.0标准规范—目录

Introduction 7
Purpose 7
Scope 7
Audience 7
SDP Design 8
SDP Concept 9
SDP Architecture and Components 10
SDP Controller 11
SDP Initiating Hosts (and SDP Clients) 12
SDP Accepting Hosts (AH) 12
SDP Deployment Models 13
SDP Workflows 15
Controller Onboarding Workflows 15
Accepting Host (AH) Onboarding Workflow 16
Initiating Host (IH) Onboarding Workflow 16
Access Workflow 17
IH Onboarding Workflow Example 18
Single Packet Authorization (SPA) 19
SPA Message Format 20
SPA as a Secure, Self-Contained, Connectionless Message Transmission Protocol 21
Alternatives to SPA 22
Mutual Transport Layer Authentication Between Components 22
Device Validation 23
SDP and IoT Devices 24
Access Policies 25
SDP Protocol 26
AH-Controller Protocol 27
AH to Controller Sequence Diagram 27
a. SPA 27
b. Open connection and establish mutually authenticated communications 27
c. Login (SDP Join) Request Message 28

SDP概念、架构组件、以及部署模型

工作流程

SPA消息格式

SDP通信协议

SDP 2.0标准规范目录

d. Login (SDP Join) Response Message....28
e. Logout Request Message....29
f. Keep-Alive Message....29
g. AH Service Messages....29
h. Reserved for Private Use....30
IH-Controller Protocol....30
IH to Controller Sequence Diagram....30
a. SPA....31
b. Open connection and establish mutually authenticated communications....31
c. Login (SDP Join) Request Message....31
d. Login Response Message....31
e. Keep-Alive Message....32
f. IH Services Message....32
g. IH Authenticated Message....33
h. Logout Request Message....34
z. Reserved for Private Use....34
IH-AH Protocol....34
IH to AH Sequence Diagram....34
a. SPA....35
b. Open connection and establish mutually authenticated communications....35
c. Open Connection Request Message....36
d. Open Appropriate Connection Type....36
e. Open Connection Response Message....36
f. Data Message....36
g. Connection Closed Message....37
z. User-Defined Message....37
Logging....37
Fields of a log message....37
Operations Logs....37
Security/Connection Logs....38
Summary....40

SDP通信协议

总结

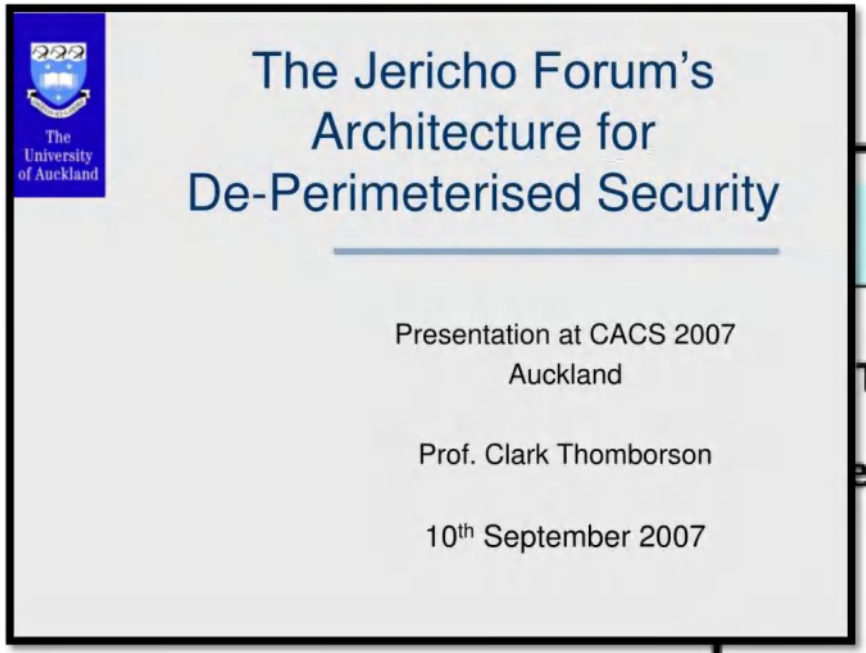
SDP 2.0标准规范对比v1.0标准规范

v1.0 ➔ v2.0 主要更新：

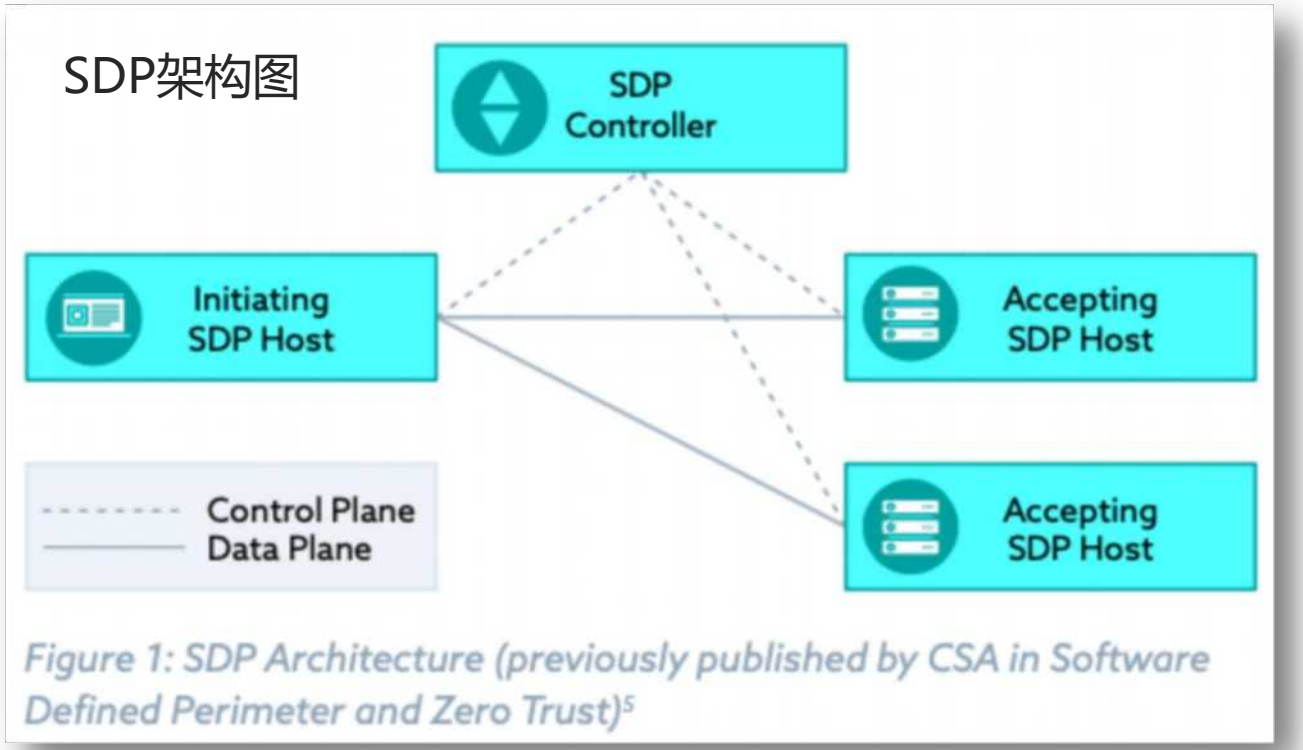
- ✓ SDP概念及其与零信任的关系
- ✓ SDP架构、组件及部署模型细化
- ✓ 加载和访问流程
- ✓ 新的SPA消息格式
- ✓ SDP通信协议的安全改进
- ✓ 对于物联网设备的支持

SDP 2.0：SDP与零信任的关系

虽然“零信任“的概念于2010年正式提出，但是早在2004年，耶律哥（Jericho）论坛就开始了相关学术研究。该技术理念很早就被美国国防部（DoD）应用于涉密网络里面。



SDP 2.0：SDP概念与零信任的关系

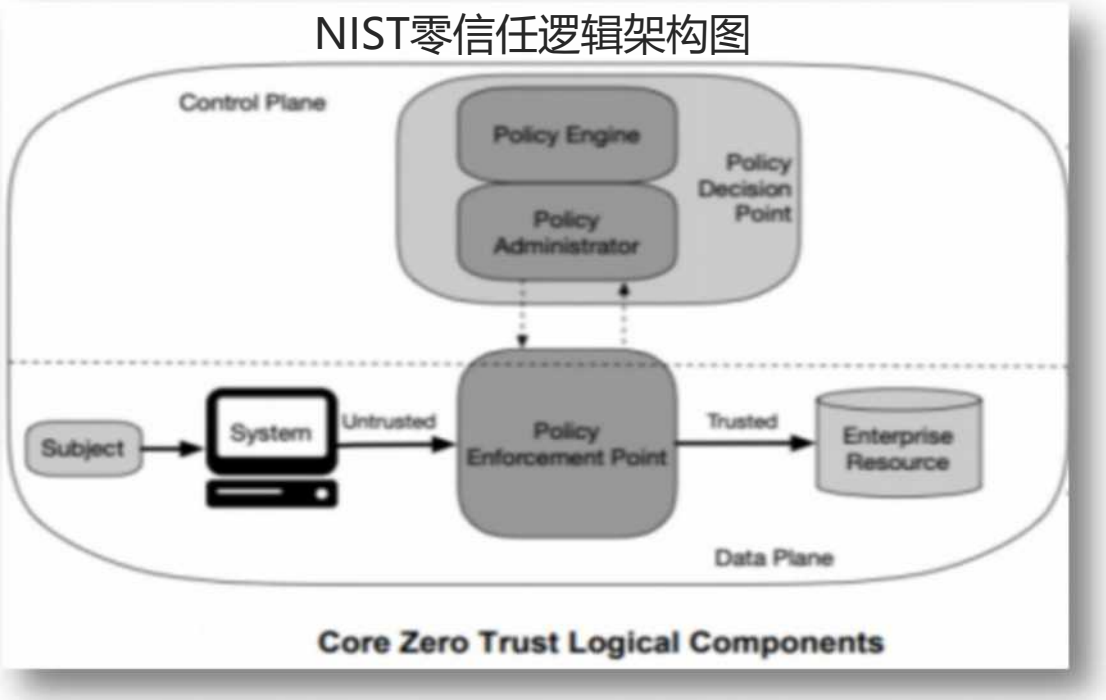


SDP的核心目标：

- 部署动态的“软件定义”边界
- 隐藏网络和资源
- 防止非授权访问企业的服务
- 实施以身份为中心的访问策略模型

SDP有效实现了NIST零信任架构（ZTA）定义的基本原则以及业务逻辑：

- 数据平面 (Data Plane)与控制平面(Control Plane)分离
- 资源对未授权的用户/设备不可见（网络隐身）
- 最小授权原则
- 所有流量加密，等等...



SDP 2.0： SDP与零信任的关系

SDP访问策略

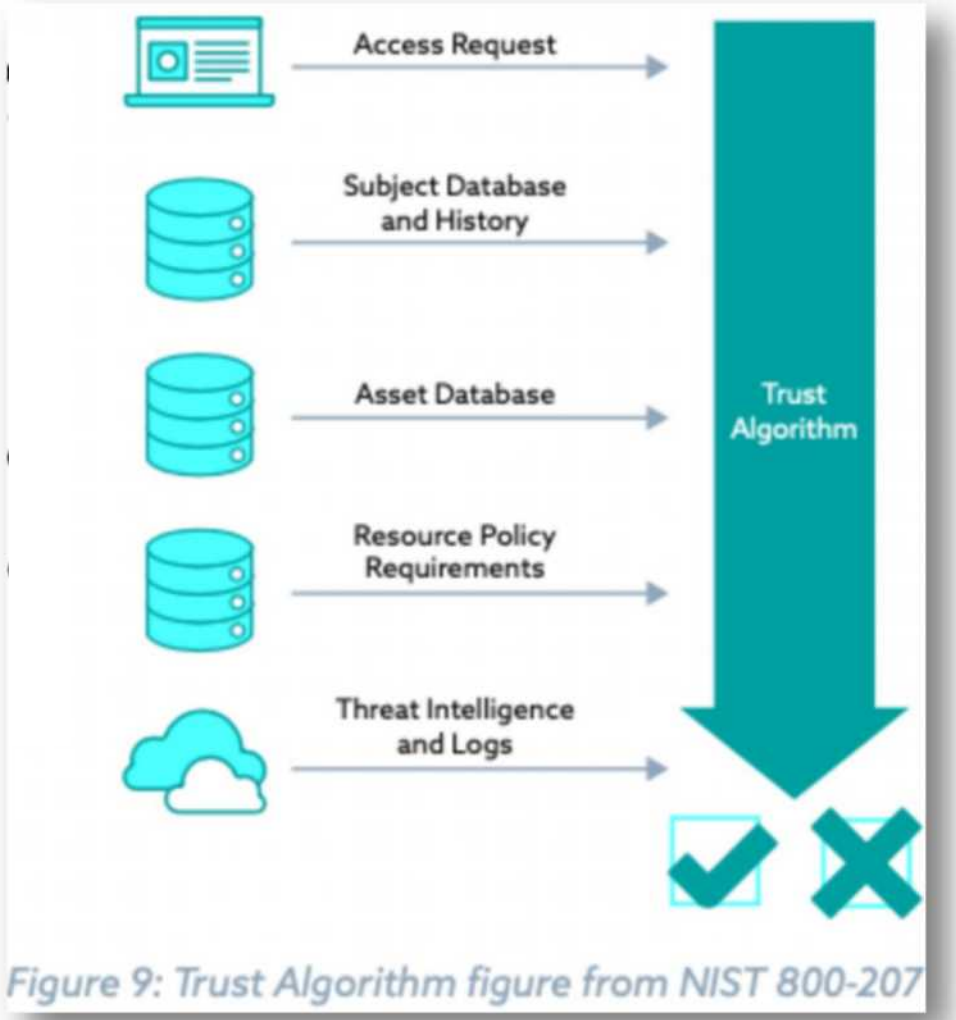
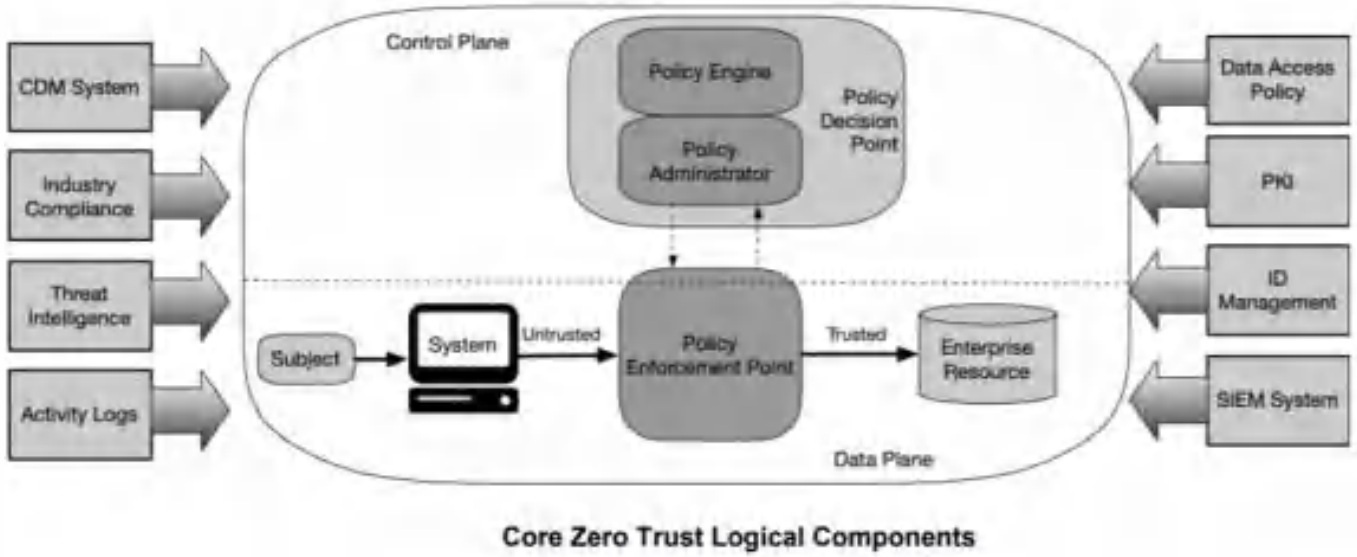


Figure 9: Trust Algorithm figure from NIST 800-207

SDP的访问策略模型与NIST零信任逻辑架构图保持一致

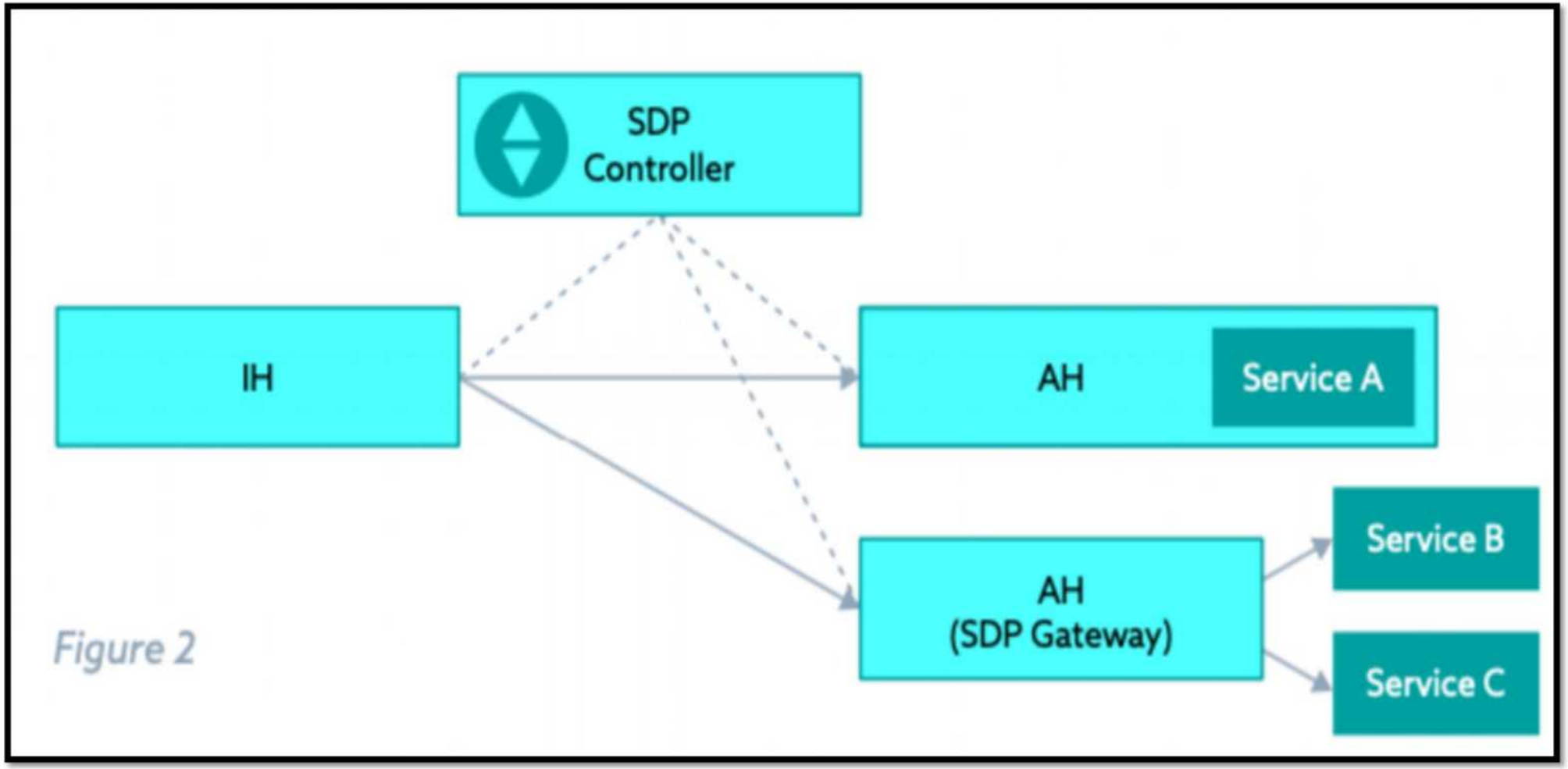


Core Zero Trust Logical Components

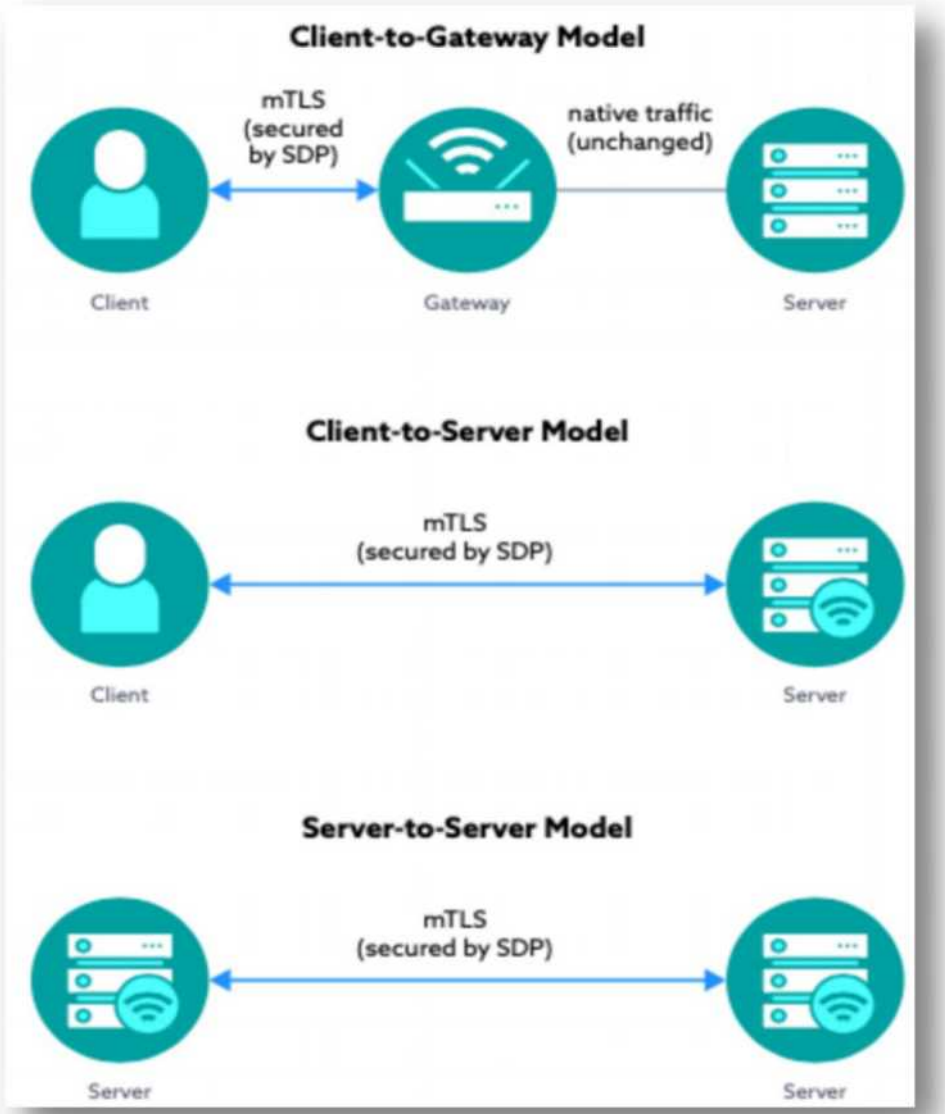
NIST零信任逻辑架构图

SDP 2.0：架构以及部署模型细化

V2.0架构图：明确了AH与服务Service的关系

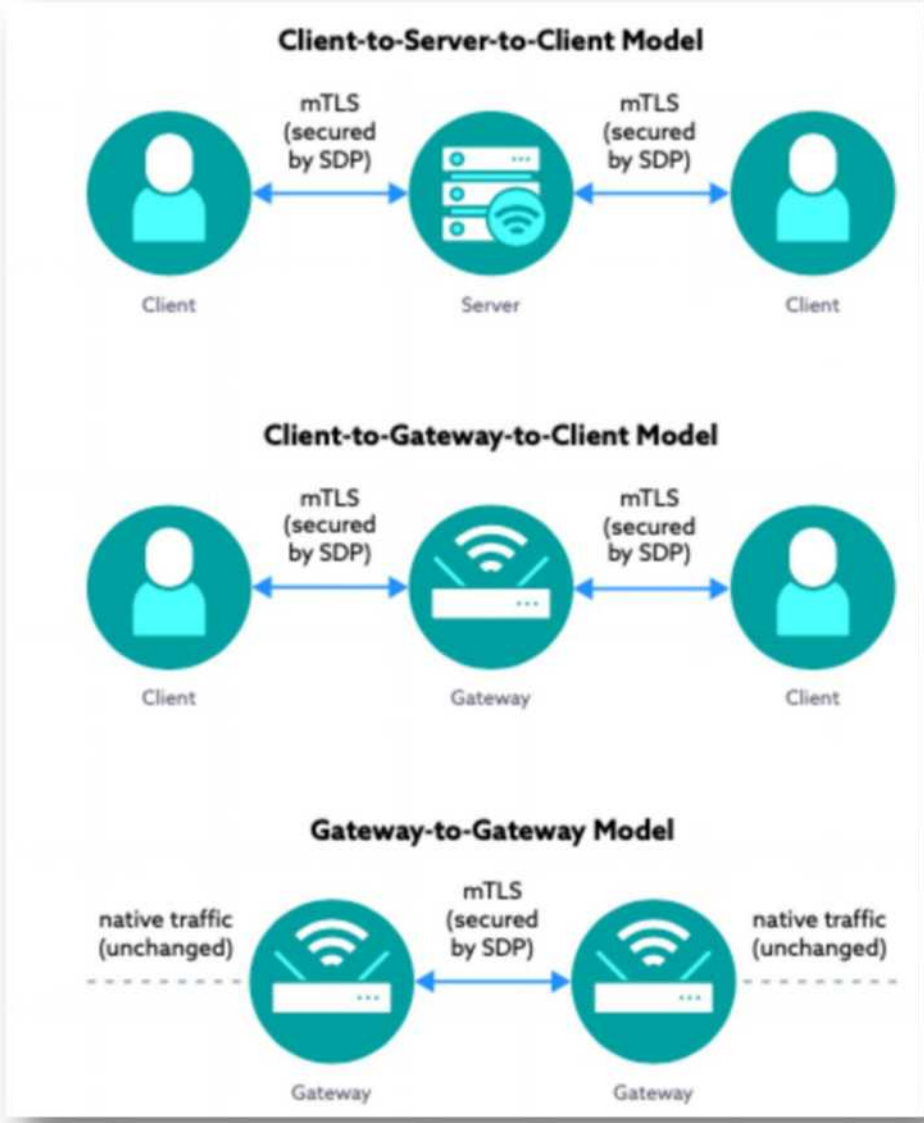


SDP 2.0：架构以及部署模型细化

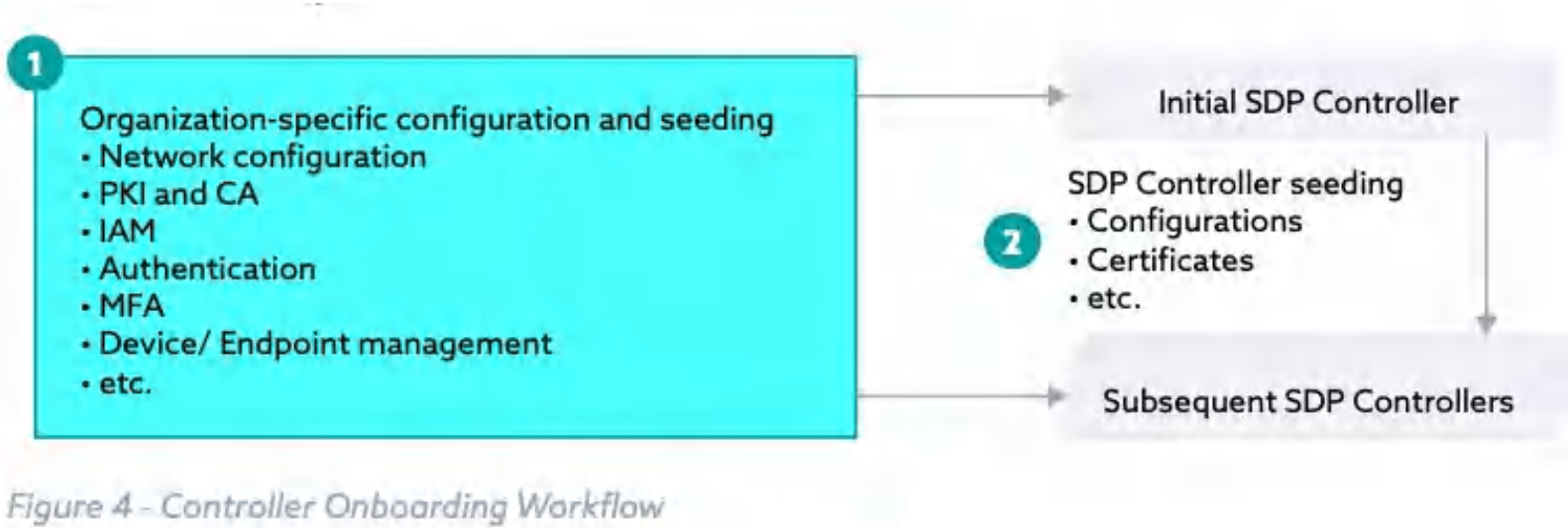


6大

部署模型



SDP 2.0：加载和访问工作流程



控制器加载流程

Figure 4 - Controller Onboarding Workflow

AH加载流程

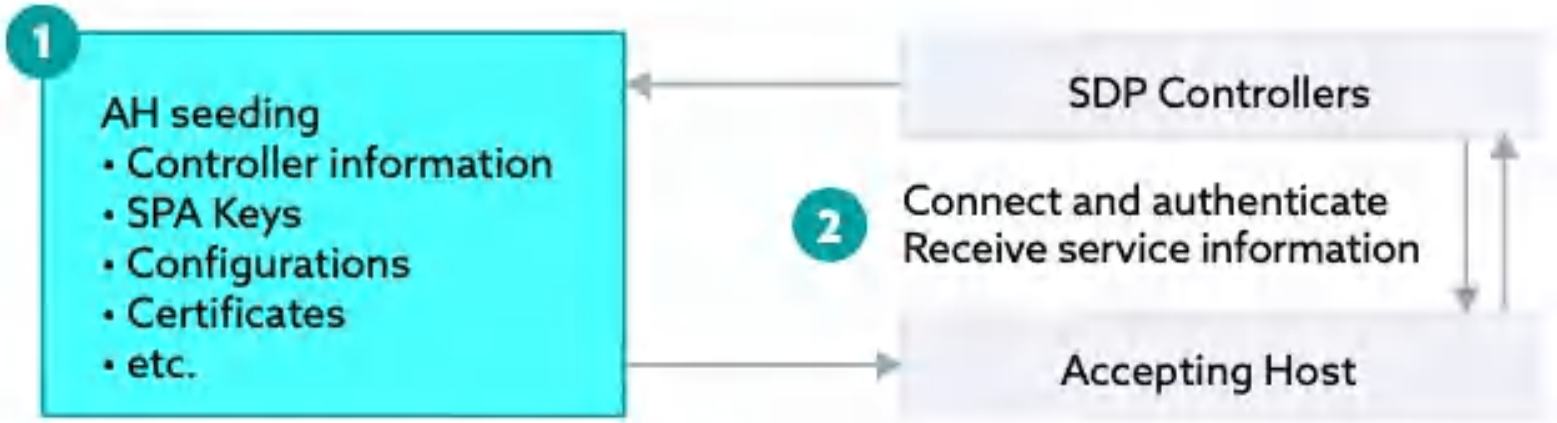
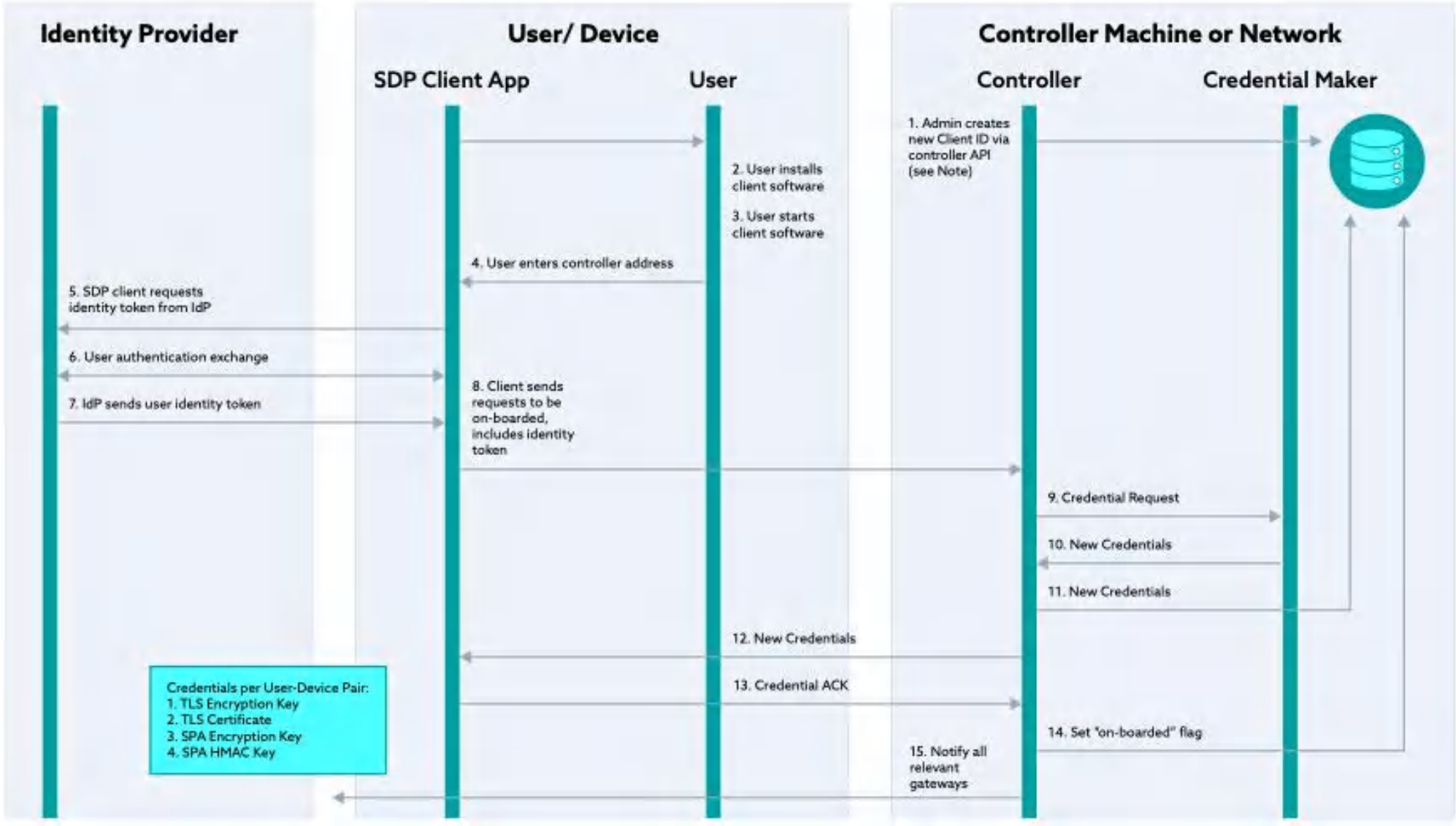


Figure 5 - Accepting Host Onboarding Workflow

SDP 2.0：加载和访问工作流程



IH加载流程

SDP 2.0：加载和访问流程

业务访问流程

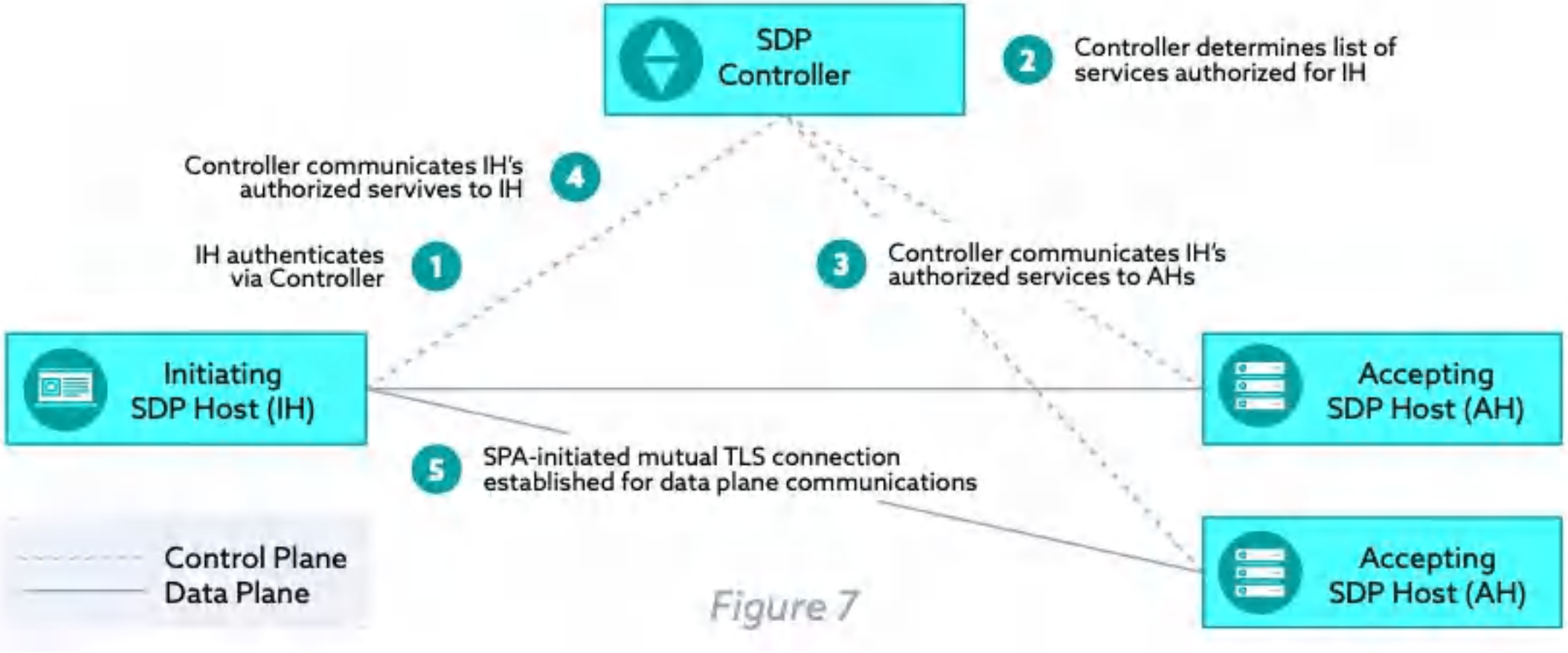


Figure 7

SDP 2.0：新的SPA消息格式

ClientID	256-bit numeric identifier, assigned per user-device pair. This field is used to distinguish the user, device, or logical group that is sending the packet.
Nonce	16-bit random data field prevents replay attack by avoiding SPA packet reuse
Timestamp	Prevents servicing outdated SPA packets, by ensuring a short time period of validity (for example, 15 to 30 seconds). This also provides a mechanism to reduce the replay-detection caching required for the recipient.
Source IP Address	The *publicly visible* IP address of the initiating host. This is included so that the Accepting Host does not rely on the source IP address in the packet header, which is easily modified en route. The IH must be able to obtain the IP address for use by the AH as the origination of packets.
Message Type	This field is optional - it may be used to inform the recipient what type of message to expect from the IH after the connection is established.
Message String	This field is optional and will be dependent on the Message Type field. For example, this field could be used to specify the services that an IH will be requesting if known at connection time.
HOTP	This hashed one-time password (hashed OTP) is generated by an algorithm as described by RFC 4226, based on a shared secret. The use of an OTP is required in SPA packets to establish authenticity; other OTP algorithms can be substituted with the overarching goal of providing authenticity of the SPA packet.
HMAC	Calculated over all fields above. Algorithm choices are SHA256 (recommended), SHA384, SHA512, SM3, Equihash, or other efficient and robust algorithms. The HMAC is calculated using a shared (secret) seed. The HMAC is calculated over all prior fields of the message and then used by the AH to verify message integrity. The HMAC validation is computationally lightweight, and therefore can be used to provide resiliency against DoS attacks. Any SPA packets with invalid HMACs are immediately discarded.

SPA 2.0的消息格式：

- 更安全（N、Time、SrcIP、HMAC等）
- 更易扩展（Msg Type、String）

- **Client**: RFC 4226 uses the term "client" to refer to the generator of the SPA packet. In the SDP architecture, the client is either the IH or the AH.
- **Server**: RFC 4226 uses the term "server" to refer to the authenticator of the SPA packet In the SDP architecture, the server is either the Controller or the AH.
- **Seed**: The seed is a 32-bit unsigned integer shared between each communicating pair (i.e., IH-Controller, AH-Controller, and IH-AH). The seed must be kept secret.
- **Counter**: The counter is a 64-bit unsigned integer that must be synchronized between communicating pairs. In RFC 4226, this is done via a "look-ahead window" (because the typical use case for RFC 4226 is a hardware OTP token). However, for the SDP protocol, the counter can be sent in the SDP packet obviating the need for a look-ahead window and the potential for the communicating pair to be out of sync. Note that the counter does not need to be kept secret.
- **Password**: The HOTP value generated by the RFC 4226 algorithm.
- **Password Length**: The password length is fixed to 8 digits.

SPA 不仅仅作为网络隐身协议，还可以作为数据传输协议

If the SPA seed is unique to a given client (identified by the ClientID in the SPA packet), then the Message String field can be used to transmit meaningful data by the client. This does not require any further processing or policy evaluation, and does not require establishing a TCP or TLS connection.

This can be useful for a set of distributed IoT sensors, for example, which need to transmit small amounts of data regularly. Embedding the data within a SPA packet permits these devices to accomplish this without incurring the overhead of establishing a TCP and TLS connection. Of course, this mechanism has some downsides. The recipient (AH) must be expecting this data, and because this is a unidirectional transmission, the sender receives no verification that the data was actually received with the 'fire and forget' SPA packet transmission. Nonetheless, this could be a useful way to apply SPA for some environments as long as the data is not significant and/or not critical.

SDP 2.0：SDP通信协议的安全改进

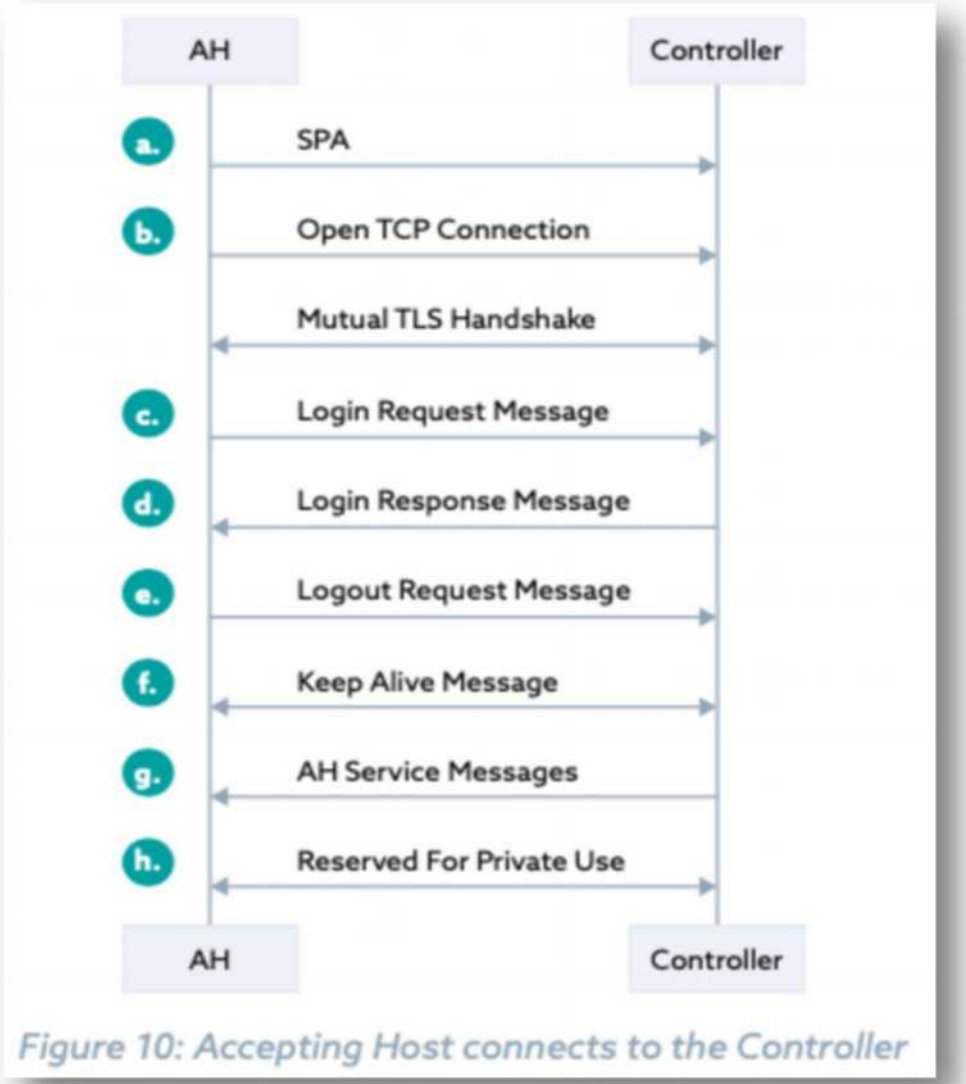


Figure 10: Accepting Host connects to the Controller

AH与控制器通信

IH与控制器通信

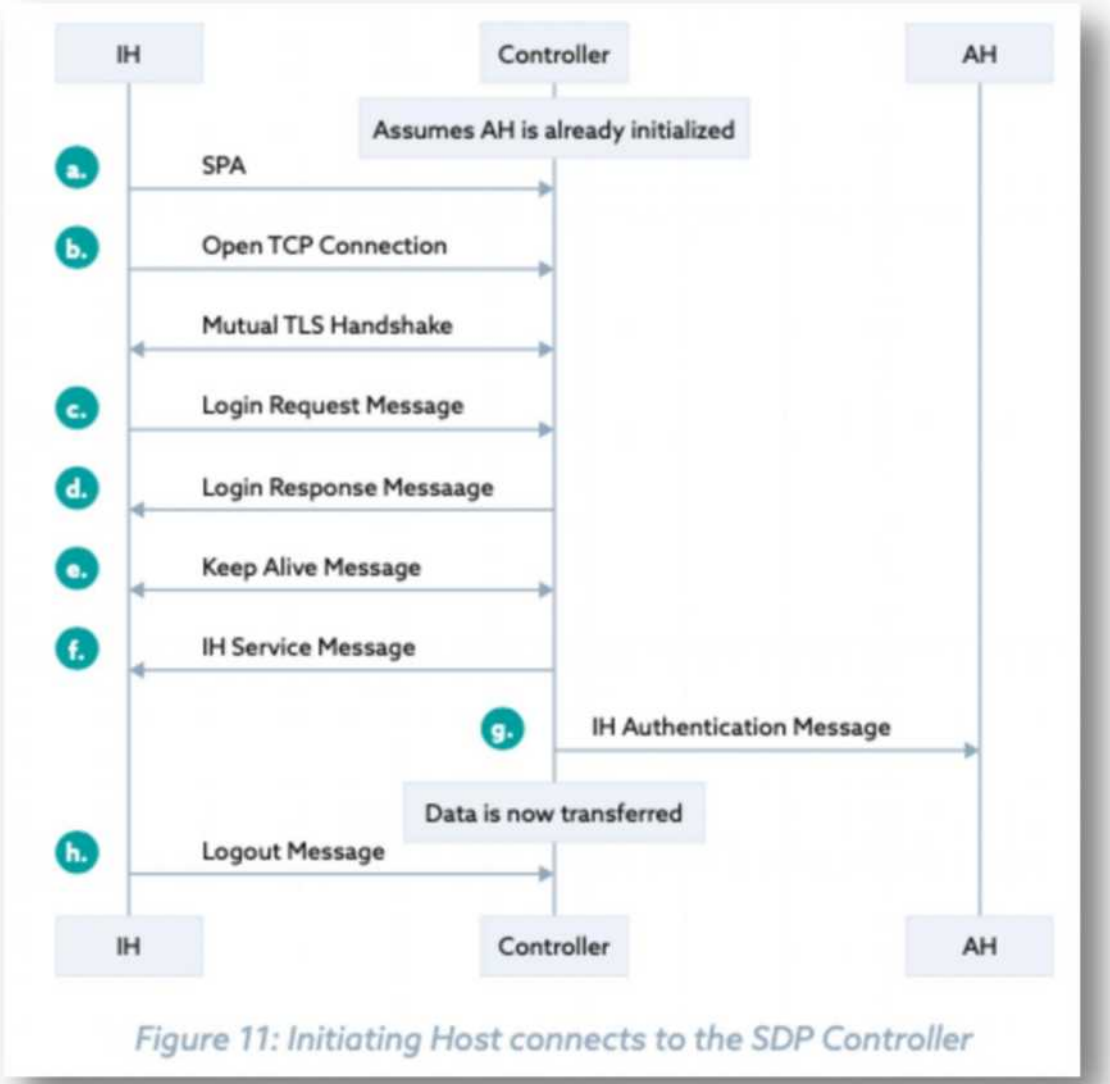


Figure 11: Initiating Host connects to the SDP Controller

SDP 2.0：SDP通信协议的安全改进

IH与AH通信

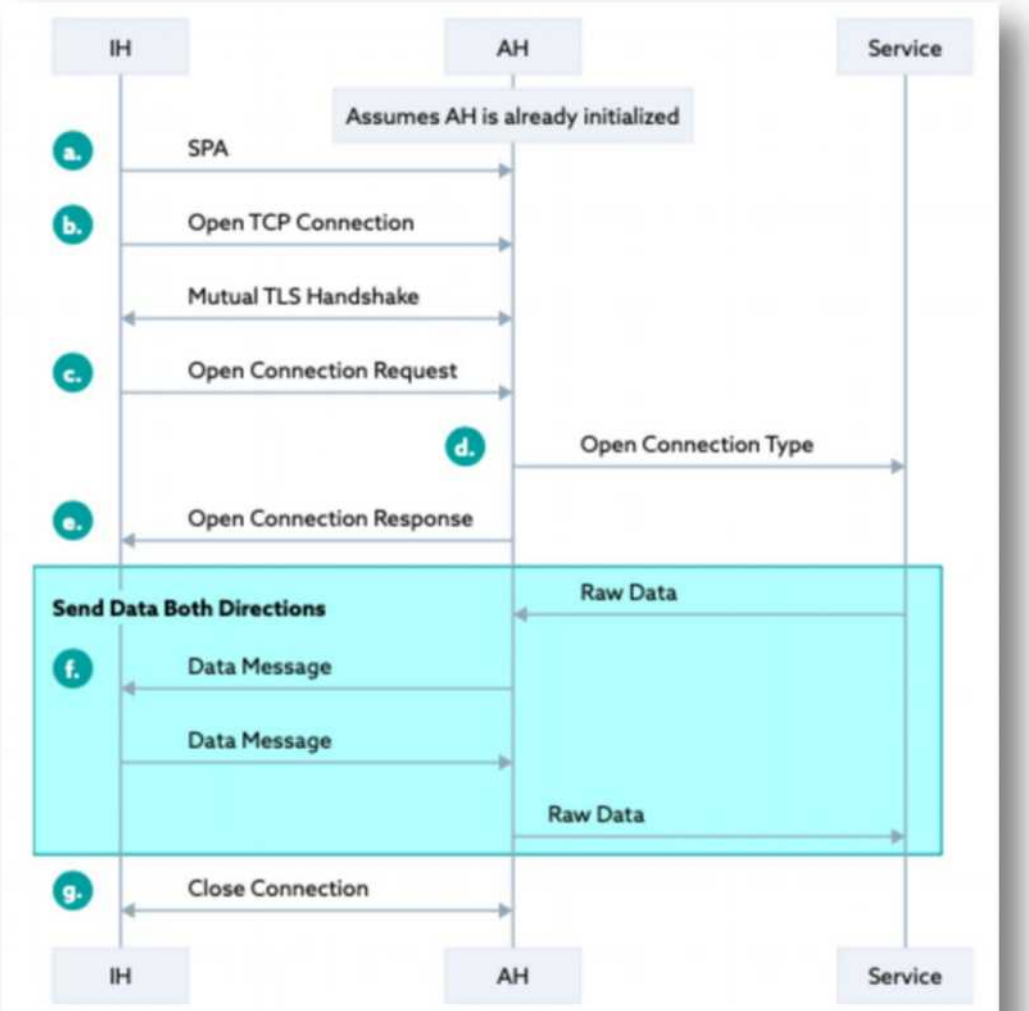
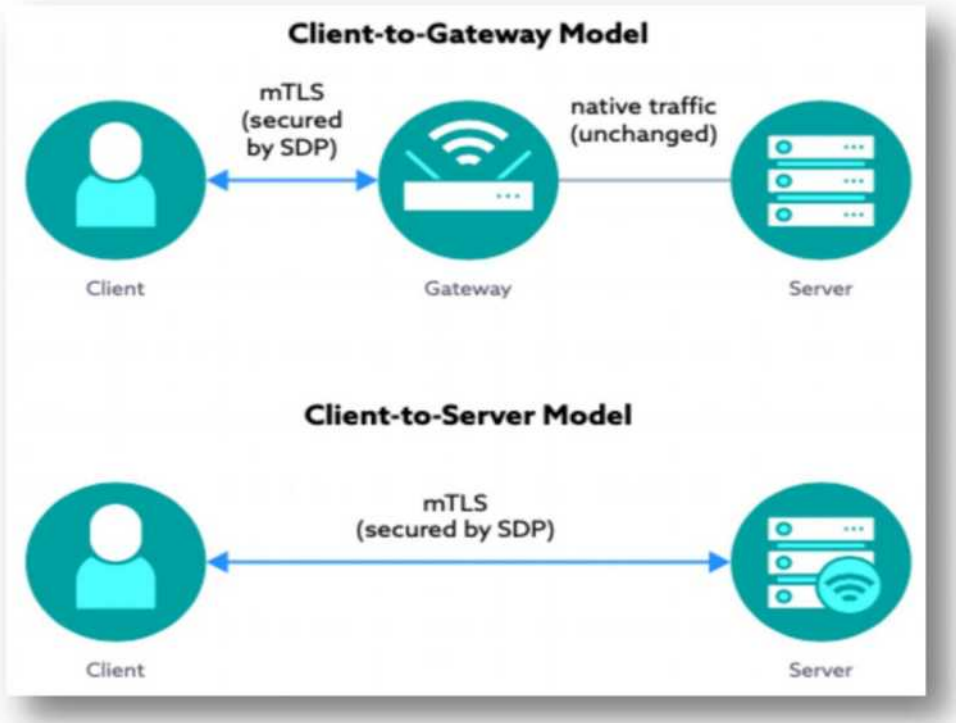
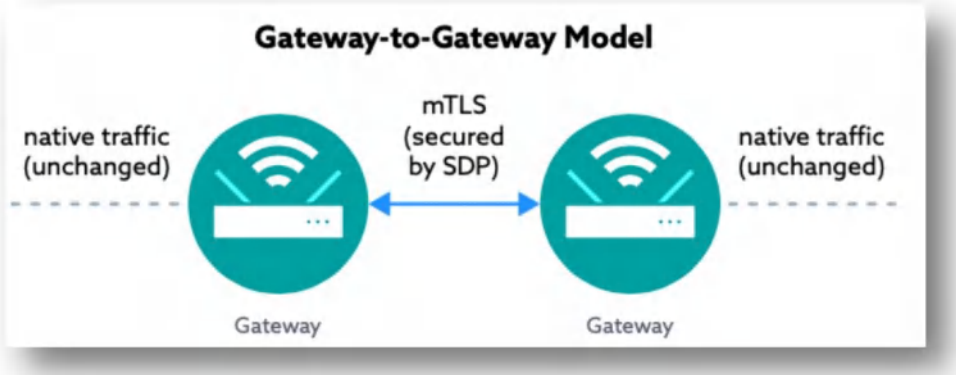


Figure 12: IH connects to an AH and then sends data to a Service

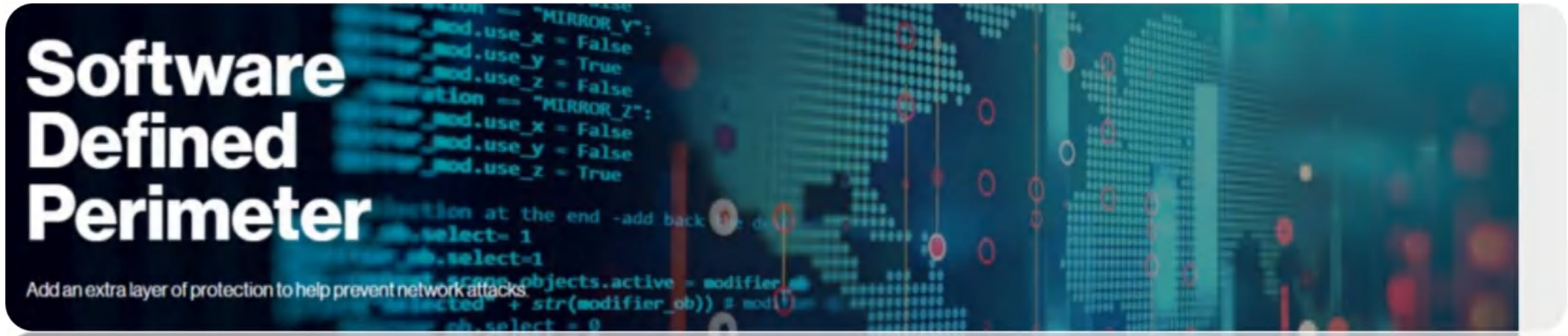
SDP 2.0：对于物联网设备的支持





- SDP v2.0概况
- SDP v2.0详解
- SDP 未来研究

SDP 未来研究方向



- 零信任策略模型和SDP（通过策略决策点（PDP）和相应的策略执行点（PEP）进行访问）
- 使用 SDP 实现物联网零信任安全
- SDP 密钥的安全存储和轮换
- 设备校验

CSA大中华区零信任工作组简介

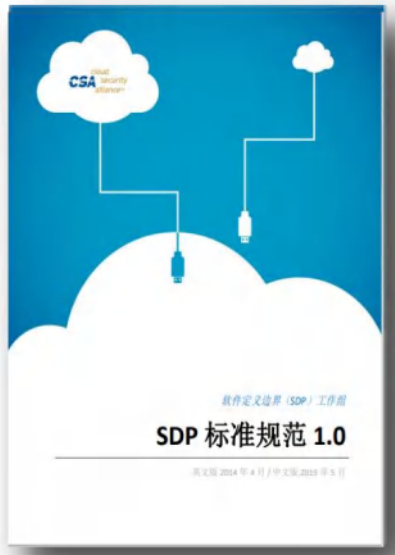
为认真贯彻落实国家网络安全战略，响应党的号召，更好推动网络安全新理念新技术在数字经济中的重大作用，有效帮助企业在数字化转型中遇到的安全问题，有效推广零信任/SDP理念及技术在中国企业的应用，并促进中国的零信任安全市场的发展，CSA（大中华区）于2019年3月成立软件定义边界（SDP）工作组，并于2021年升级为零信任工作组。目前工作组已经发展到近百名行业顶尖专家，来自于业内头部的50多个成员单位。经过工作组专家们近3年的无私辛勤的努力，目前工作组已经输出上千页国内有影响力的白皮书、教材PPT、图书等资料文档，为中国新一代网络安全技术创新和实践作出了重要的贡献。

2019.3工作组成立大会的合影

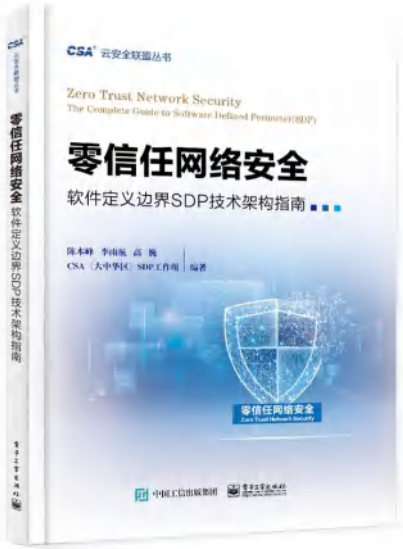
工作组目标：促进零信任理念及相关技术在中国的应用实践，

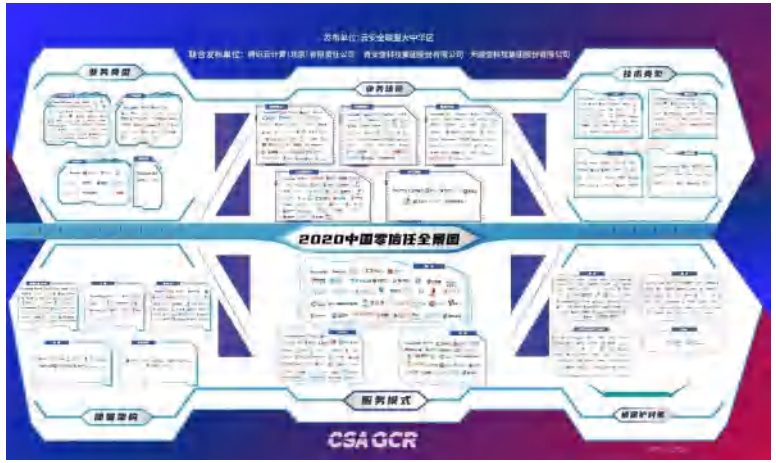
让每一家企业了解零信任、用好零信任！

CSA（大中华区）零信任工作组研究成果



CSA（大中华区）零信任工作组研究成果





《零信任专家认证CZTP》教材

600多页PPT

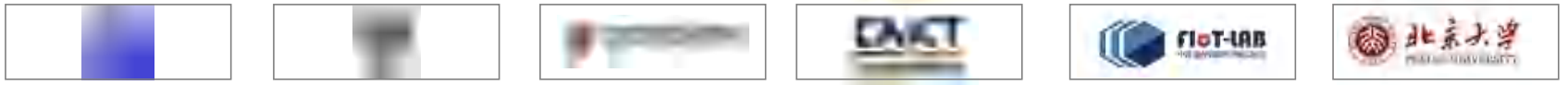
更多CSA零信任和SDP的研究成果，可在CSA GCR官网下载：
https://c-csa.cn/research/results/i-1/page-1.html

CSA （大中华区）零信任工作组专家成员单位 (部分)

CSA GCR cloud security GREATER CHINA REGION alliance ®

腾讯安全

政府/事业单位:



大型科技/
安全企业:

云服务商/用户:

创新企业:

CSA （大中华区）零信任工作组会员单位/专家招募

- 专家申请：https://c-csa.cn/member/personal/pro/
- 成员单位申请：https://c-csa.cn/member/enterprise/

CSA官方微信

个人微信

CSA GCR cloud security GREATER CHINA REGION alliance ®

腾讯安全

CSA SDP2.0标准发布
暨零信任技术研讨会

谢　谢