CSA GCR cloud security alliance
GREATER CHINA REGION

第二届国际零信任峰会

数字时代：零信任剑行天下

2021 ZERO TRUST SUMMIT

QINGDAO, CHINA
JUNE 25, 2021
中国·青岛
6月25日

时隔七年SDP2.0重磅发布 抢先预览2.0带来哪些变化

单位：CSA GCR零信任工作组　主讲人：陈本峰

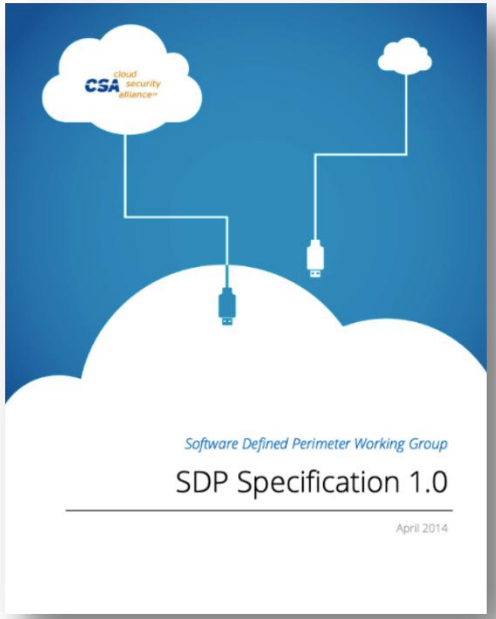
2021-06-25

目录

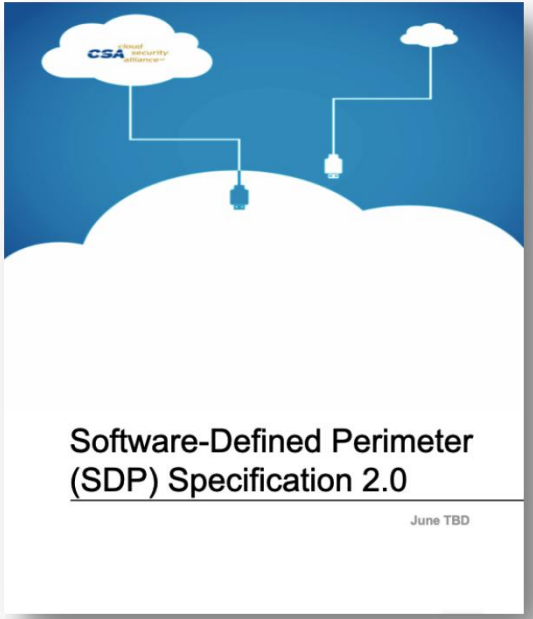
Content

时隔七年，SDP 2.0最终草案（Final Draft）重磅发布

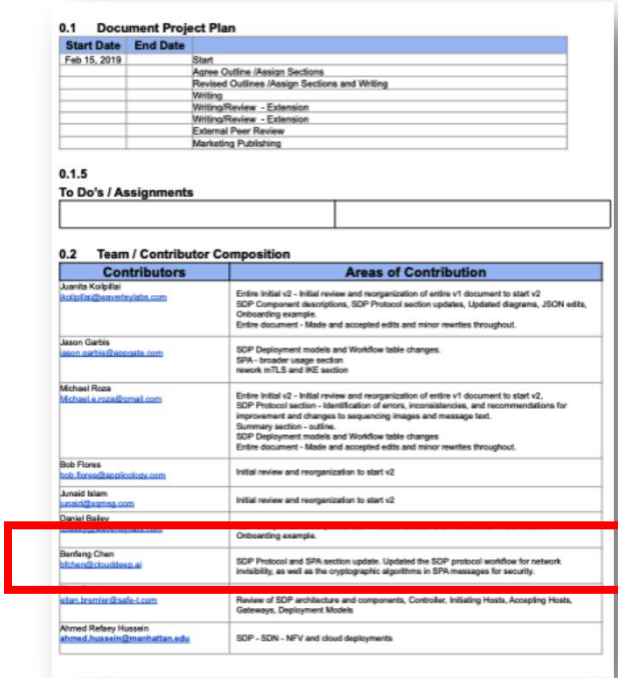
SDP标准1.0 （2014年4月）



SDP标准2.0草案 （2021年6月）



作为编委会成员之一参与SDP 2.0内容编写



0.1 Document Project Plan

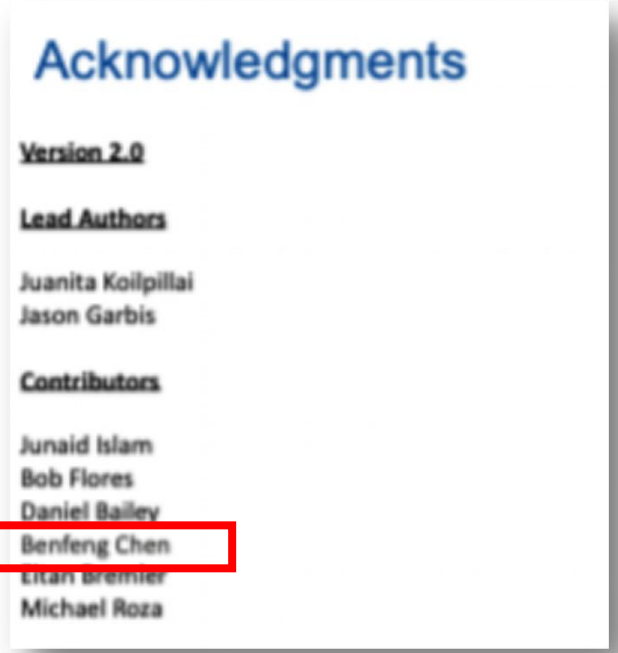
Start Date	End Date	
Feb 15, 2019		Start
		Agree Outline /Assign Sections
		Revised Outlines /Assign Sections and Writing
		Writing
		Writing/Review - Extension
		Writing/Review - Extension
		External Peer Review
		Marketing Publishing

0.1.5

To Do's / Assignments

0.2 Team / Contributor Composition

Contributors	Areas of Contribution
Juanita Koilpillai koilpillai@wavemeylabs.com	Entire Initial v2 - Initial review and reorganization of entire v1 document to start v2 SDP Component descriptions, SDP Protocol section updates, Updated diagrams, JSON edits, Onboarding example. Entire document - Made and accepted edits and minor rewrites throughout.
Jason Garbis jason.garbis@appgate.com	SDP Deployment models and Workflow table changes. SPA - broader usage section rework mTLS and IKE section
Michael Roza Michael.a.roza@gmail.com	Entire Initial v2 - Initial review and reorganization of entire v1 document to start v2, SDP Protocol section - Identification of errors, inconsistencies, and recommendations for improvement and changes to sequencing images and message text. Summary section - outline. SDP Deployment models and Workflow table changes Entire document - Made and accepted edits and minor rewrites throughout.
Bob Flores bob.flores@securicology.com	Initial review and reorganization to start v2
Junaid Islam junaid@xerring.com	Initial review and reorganization to start v2
Daniel Bailey [redacted]	Onboarding example.
Benfeng Chen bfchen@cloudsdeep.ai	SDP Protocol and SPA section update. Updated the SDP protocol workflow for network invisibility, as well as the cryptographic algorithms in SPA messages for security.
[redacted]	Review of SDP architecture and components, Controller, Initiating Hosts, Accepting Hosts, Gateways, Deployment Models
Ahmed Refaey Hussein ahmed.hussein@manhattan.edu	SDP - SDN - NFV and cloud deployments



Acknowledgments

Version 2.0

Lead Authors

Juanita Koilpillai
Jason Garbis

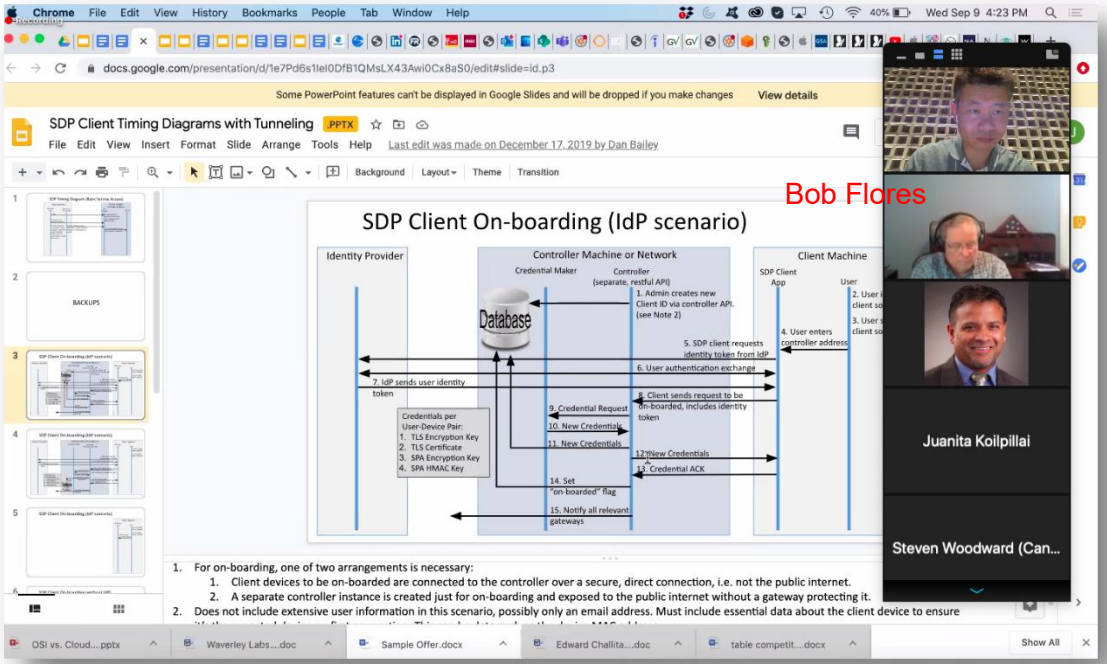
Contributors

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

SDP 2.0编委会工作过程

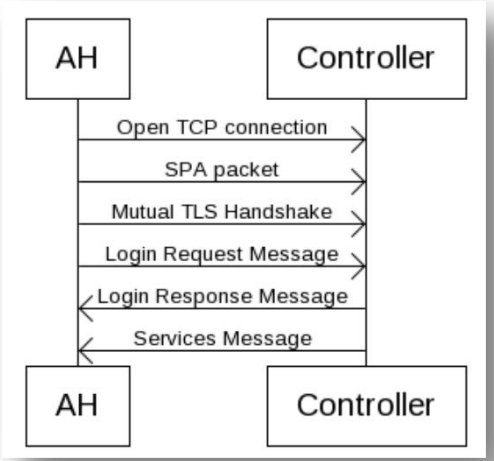
SDP 2.0编委会讨论会每两周一次ZOOM会议，美西时间下午1点

（北京时间凌晨4点）

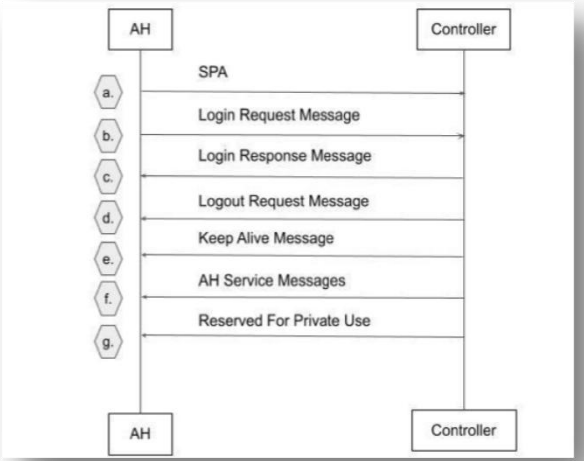


修改了SDP协议，让“网络隐身”能力更强（AH → Controller）

SDP 1.0

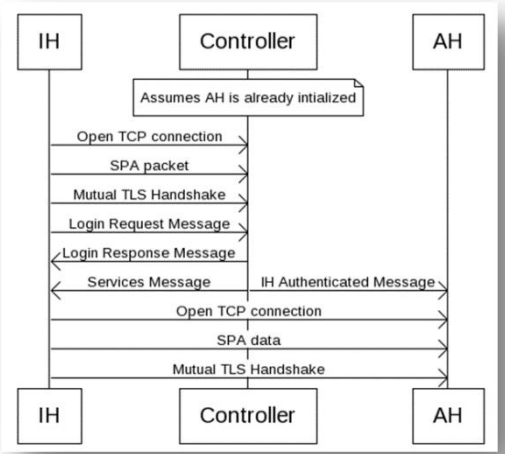


SDP 2.0

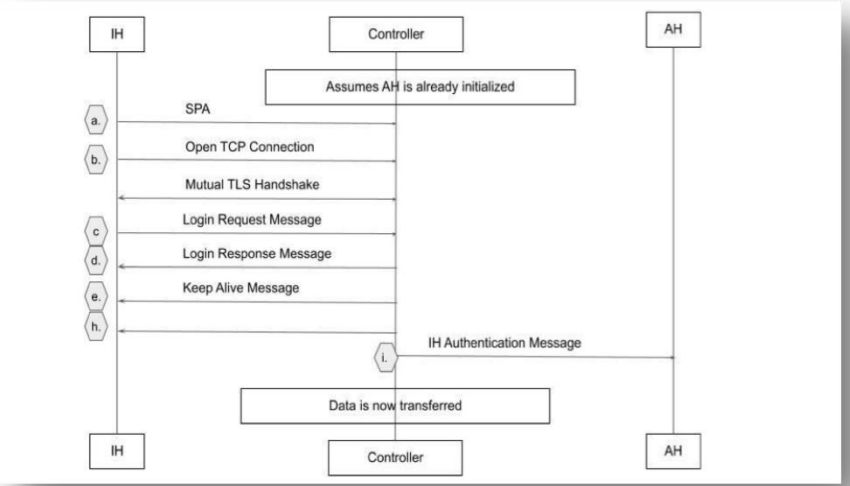


修改了SDP协议，让“网络隐身”能力更强（IH → Controller）

SDP 1.0

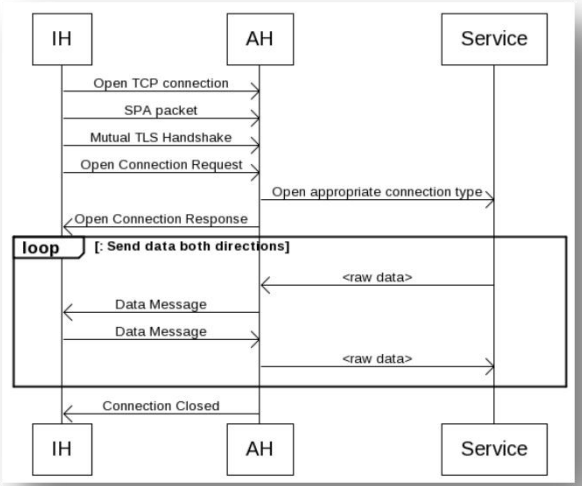


SDP 2.0

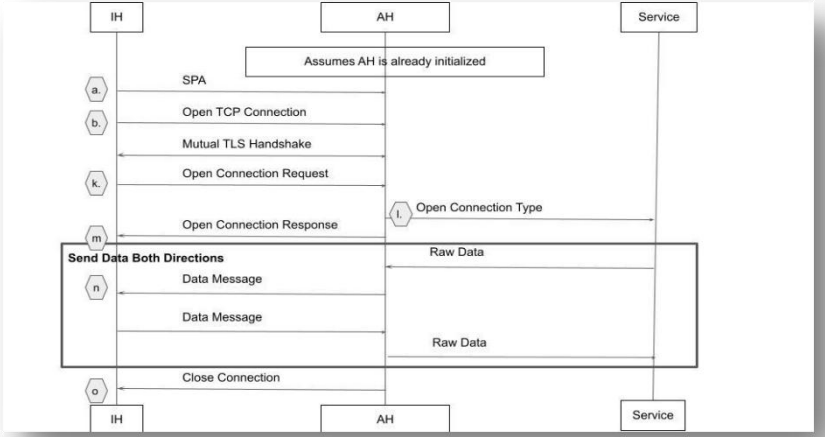


修改了SDP协议，让“网络隐身”能力更强（IH → AH）

SDP 1.0



SDP 2.0



改进了SPA报文格式，首次引入国密算法作为备选加密算法之一

SDP 1.0

SPA is based on RFC 4226 (HOTP) with the following parameters:

- **Client**: RFC 4226 uses the term "client" to refer to the generator of the SPA packet. In the S 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 t 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., 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 comm pairs. In RFC 4226, this is done via a "look-ahead window" (because the typical use case for hardware OTP token). However, for the SDP protocol, the counter can be sent in the SDP pa obviating the need for a look-ahead window and the potential for the communicating pair t 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.

For the SPA protocol, a single SPA packet is sent from the client to the server. The server does not re format of the packet is:

IP	TCP	AID (32-bit)	Password (32-bit)	Counter (64-bit)

After receiving the packet, the server must enable the client to connect via mutual TLS on port 443.

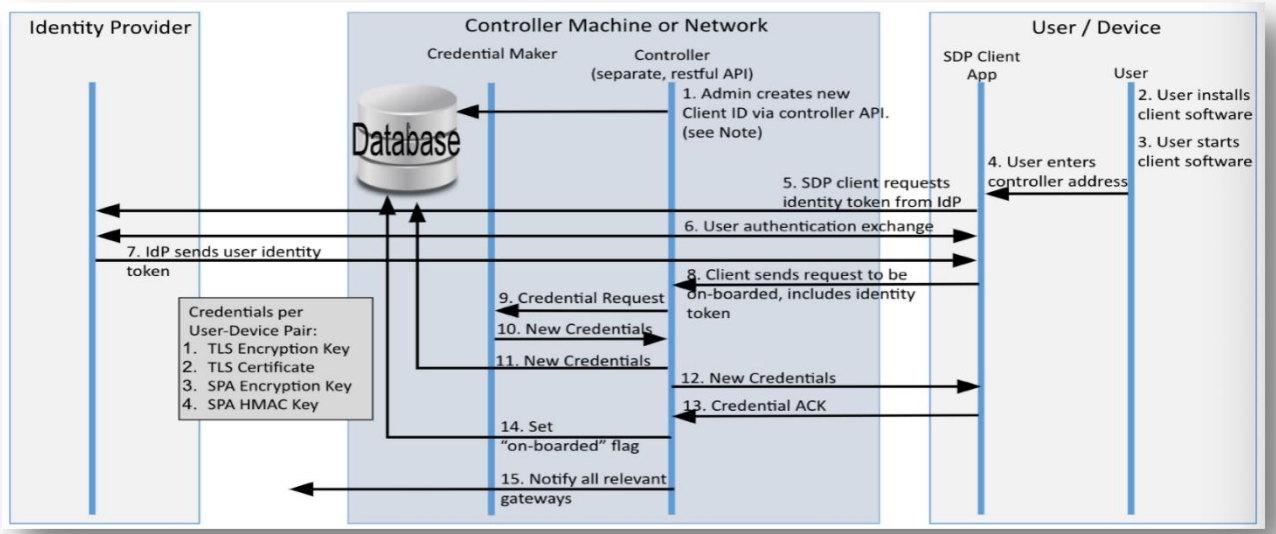
SDP 2.0

ClientID	32-bit numeric identifier, assigned per user-device pair. This field is optional, and used for SPA schemes that distinguish on a per-client basis
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 (example 15 to 30 seconds).
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 is generated by an algorithm such as RFC 4226, based on a shared secret. The use of an OTP is required in SPA packets for authenticity; other OTP algorithms can be substituted with the overarching goal of providing authenticity of the SPA packet.
Counter	The counter is a 64-bit unsigned integer intended to 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, however AHs should have mechanisms in place to avoid malicious use of very large counters, potentially denying service to (legitimate) IHs sending lower counter values. This field is optional, depending on the OTP algorithm chosen.
HMAC	Calculated over all fields above. Algorithm choices are SHA256 (recommended), SHA384, SHA512, and SM3. 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 will be immediately discarded.

改进了SPA报文格式，首次引入国密算法作为备选加密算法之一

	This field is optional, depending on the UTF algorithm chosen.
HMAC	Calculated over all fields above. Algorithm choices are SHA256 (recommended), SHA384, SHA512, and SM3. 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 will be immediately discarded.

细化了on-boarding启动过程流程图，保证SDP的实现更安全、更灵活



细化了设备校验的过程描述，保证SDP的实现更安全、更灵活

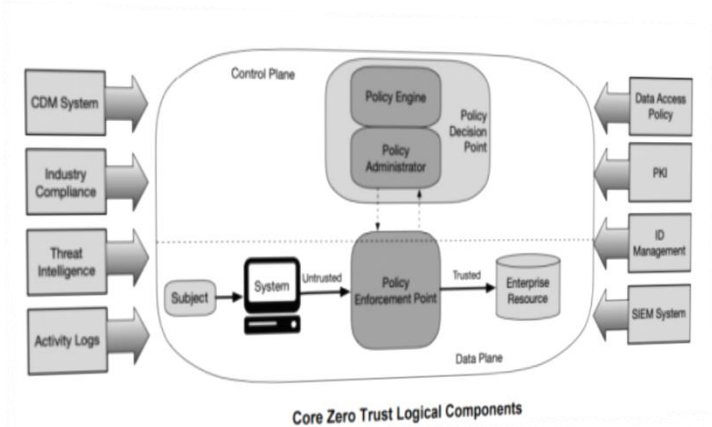
Device Validation

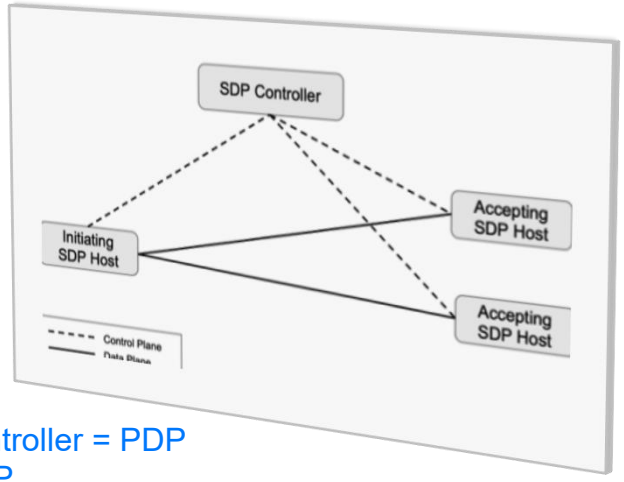
Mutual transport layer authentication proves that the device requesting access to the SDP possesses a private key that has not expired and that has not been revoked, but it does not prove that the key has not been stolen. The objective of Device Validation is to prove that the proper device holds the private key and that the software running on the device can be trusted. In the simplest form of SDP described in this document, the Controller is assumed to be a trusted device (because it exists in the most controlled environment) and the IHs and AHs must validate it. SDP Gateways that aren't also acting as accepting hosts are also assumed to be trusted components as they are under the control of the enterprise operating the SDPs.

User devices, on the other hand, require validation. Device Validation mitigates credential theft and the resultant impersonation attacks. The user's device which has been authenticated with the SPA message is allowed to connect to the SDP controller via the SDP gateway. This process ensures that an attacker will not be able to access services on or behind the AH, even if the user is in possession of the correct private keys for the connection. All packets are dropped from the user's device unless authenticated and authorized via SDP, thus preventing any incoming packets from all unauthorized user devices. Device validation protocols are enterprise and product-specific, and as such are beyond the scope of the SDP specification

SDP systems must support the ability to integrate with enterprise device management / endpoint management systems, and include their device posture checks into a device validation process. In addition, SDP systems should support the ability to perform local device posture checks, in environments where the SDP system has software running locally on the user device. For example, an SDP client could validate that a user's device contains a valid certificate issued by the enterprise. Or, it could validate that the device is running an approved Anti-Virus component. Note that these aspects are related to the overall Zero Trust approach that SDP supports -- using device information as additional context for making access policy decisions. Also note that "devices" here can also refer to servers, which can and should be validated, in many of the same ways as user devices.

明确了SDP技术架构和NIST抽象模型之间的对应关系





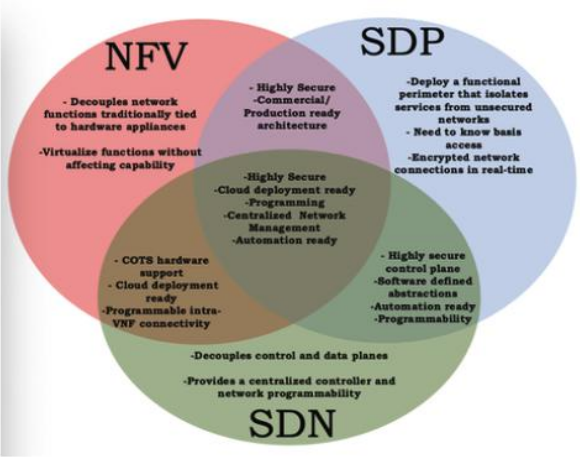
SDP Controller = PDP
AH = PEP

明确了SDP技术架构和云计算各个逻辑层级的关系，SDP适用于大多数层级

For cloud infrastructures, SDP integrates security at:

- the network layer where virtualization[1] provides computing, storage, and monitoring
- the transport layer where cloud APIs tie virtualized assets to resource pools and users
- the session layer where the underlying virtualized infrastructure is managed
- the network access layer where middleware manages application tiers and the application
- the application layer that provides business value to users

明确了SDP技术架构和SDN（软件定义网络）以及NFV（网络功能虚拟化）的关系



In short, consider the Software-Defined Network (SDN) and the Network Function Virtualization (NFV) as two sides in a network virtualization triangle, the Software-Defined Perimeter (SDP) completes the missing piece of this triangle. Even though, both SDN and SDP operate in the networking arena and have similar names, the SDN can be considered as the brain which orchestrates network operations, while the SDP introduces reliable network connectivity with zero trust concepts without significant obstruction.

扩展了SDP对IoT的支持，打造万物互联的云安全网络

SDP2.0改进总结

- 改进了SDP协议中网络隐身技术，更安全
- 改进了SDP协议中单包授权技术SPA的格式，增加了国密算法的支持
- 细化了SDP协议中on-boarding启动过程，更具体
- 细化了SDP协议中设备验证的过程，更具体
- 明确与NIST零信任架构中逻辑组件的对应关系
- 明确与云计算多个层级的应用逻辑关系
- 明确与软件定义网络SDN的对应关系
- 增加了对物联网IoT的支持

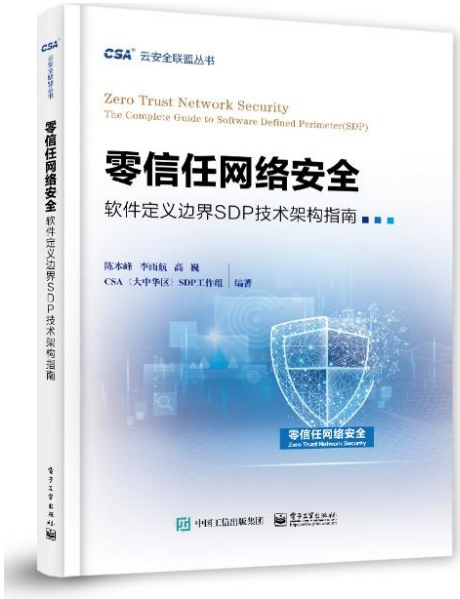
CSA（大中华区）于2019.3成立SDP工作组，2021年升级为零信任工作组

为了提高SDP安全模型在中国的实践和创新，CSA（大中华区）于2019年3月成立SDP工作组，目前已经有100位多专家成员，来自50多个单位。

阿里云、腾讯云、华为、京东云、奇安信、 360、深信服、绿盟科技、天融信、启明星辰、国家电网、中国移动、中国电信、中国联通、中电科、奇安信、中科院、中国信通院、IBM、埃森哲、紫光、云深互联、顺丰科技、安几科技、易安联、联软科技、蔷薇灵动、玉符飞扬、畅思天空、上海云盾、宝信软件、博安科技、漠坦尼科技、鼎赛、深圳CA、蛛语科技、梆梆安全、世平信息、三未信安、上汽乘用车、软通咨询、贝壳、服云、北京邮电大学、缔安科技、筋斗腾云、安永、山石网科、上实龙创、中国金融认证中心、完美世界、中电研、齐安科技、国云科技、国网南瑞、欧喜投资、雅培.....

https://www.c-csa.cn/research/union-detail/i-8.html

电子工业出版社《零信任网络安全—软件定义边界SDP技术指南》今日首发！



零信任落地，从零信任SDP开始！仅限首发日特价！

京东折扣链接

当当折扣链接

CSA GCR cloud security alliance
GREATER CHINA REGION

第二届国际零信任峰会

数字时代：零信任剑行天下

2021 ZERO TRUST SUMMIT

QINGDAO, CHINA
JUNE 25, 2021
中国·青岛
6月25日

Thank You