

What is this Zero Trust to which you refer?

- SDP: The Most Advanced Zero Trust Architecture

Cloud Security Alliance

CloudBytes Connect “Birds of a Feather”

February 2, 2021

Cloud Security Alliance CSA

The Cloud Security Alliance (CSA) is the world's leading organization dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment. CSA harnesses the subject matter expertise of industry practitioners, associations, governments, and its corporate and individual members to offer cloud security-specific research, education, certification, events and products. CSA's activities, knowledge and extensive network benefit the entire community impacted by cloud — from providers and customers, to governments, entrepreneurs and the assurance industry — and provide a forum through which diverse parties can work together to create and maintain a trusted cloud ecosystem.

CSA operates the most popular cloud security provider certification program, the CSA Security, Trust & Assurance Registry (STAR), a three-tiered provider assurance program of self-assessment, 3rd-party audit and continuous monitoring. CSA also manages the CSA Global Consulting Program, a professional program it developed that allows cloud users to work with a network of trusted security professionals and organizations that offer qualified professional services based on CSA best practices.

In 2009, CSA released the Security Guidance for Critical Areas of Focus In Cloud Computing, providing a practical, actionable road map to managers wanting to adopt the cloud paradigm safely and securely. The following year, CSA launched the industry's first cloud security user certification, the Certificate of Cloud Security Knowledge (CCSK), the benchmark for professional competency in cloud computing security, along with the Cloud Controls Matrix (CCM), the world's only meta-framework of cloud-specific security controls mapped to leading standards, best practices and regulations. By way of follow up, in 2015 together with (ISC)², CSA debuted the Certified Cloud Security Professional (CCSP) certification, representing the advanced skills required to secure the cloud.

CSA's comprehensive research program works in collaboration with industry, higher education and government on a global basis. CSA research prides itself on vendor neutrality, agility and integrity of results. CSA has a presence in every continent except Antarctica. With our own offices, partnerships, member organizations and chapters, there are always CSA experts near you. CSA holds dozens of high quality educational events around the world and online. Please check out our events page for more information.

Topics

What is Zero Trust?

Secondary discussions (including, but not limited to)

- 1) Why Zero Trust
- 2) What Zero Trust Addresses
- 3) Implementing Zero Trust
- 4) How SDP Implements Zero Trust
- 5) Benefits of SDP

Special guest speaker: Juanita Koilpillai

- CEO of USG DoD Consultancy
- CSA's SDP Zero Trust WG Technical Advisor
- Next steps – Join the SDP Zero Trust Working Group (WG)



- **Juanita Koilpillai, Waverley Labs**

-
- jkoilpillai@waverleylabs.com

www.waverleylabs.com/publications/

Special guest speaker: Junaid Islam

- Co-founder of SDP
- CSA's SDP Zero Trust WG co-chair
- Next steps – Join the SDP Zero Trust Working Group (WG)



- **Junaid Islam, National Spectrum Consortium**
-

- junaid@xqmsg.com

<https://www.nationalspectrumconsortium.org/about-us-2/leadership/>



What is Zero Trust

Allowing access to the network changes with “Zero Trust”; as the name implies - users aren’t allowed access to anything until they authenticate who they are.

A network security architecture that withholds access until a user, device or even an individual packet has been thoroughly inspected and authenticated.


Specifically, the least amount of necessary access is granted.

Continuous monitoring of suspicious user activity

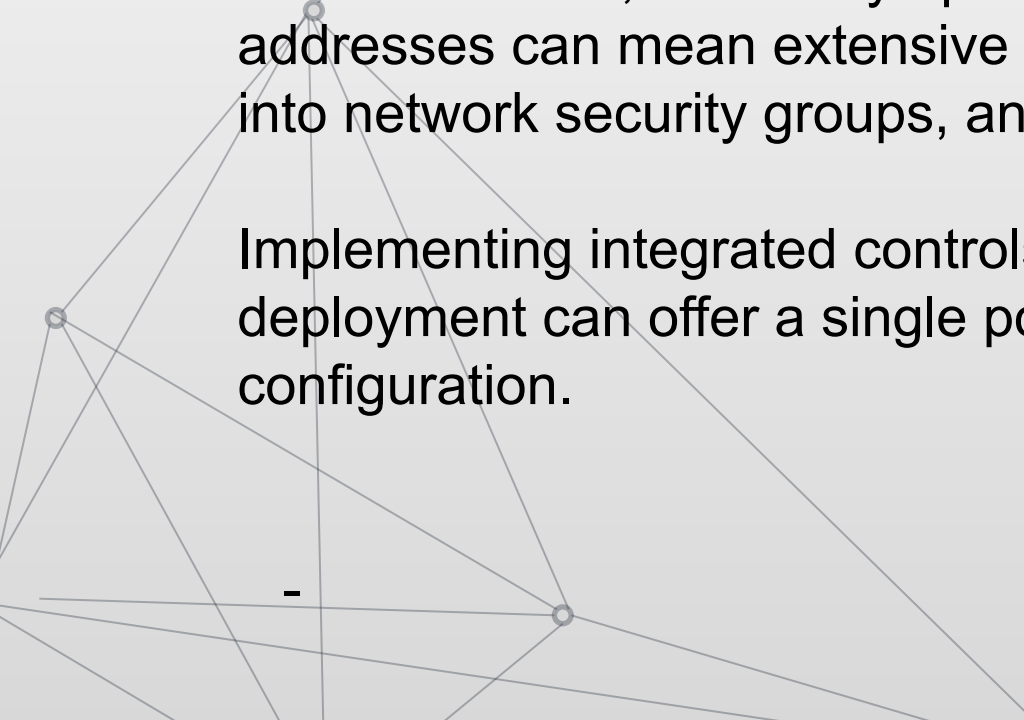


Why Zero Trust

Changing Perimeter - fixed network perimeter problematic for mobile devices




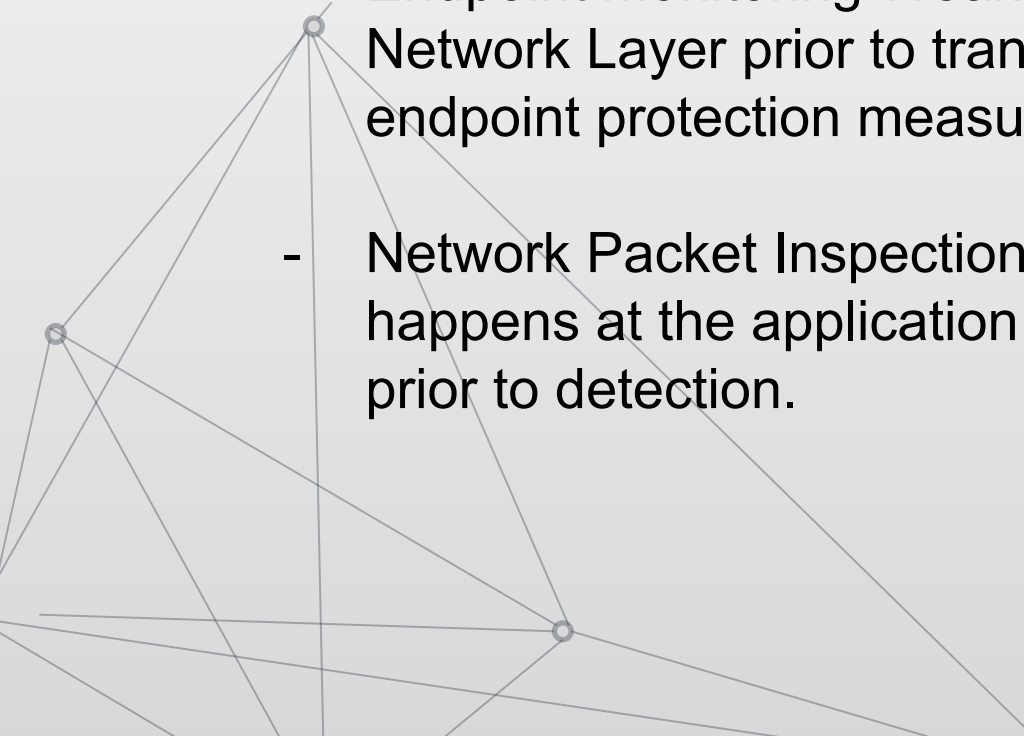
IP address conundrum – IP addresses simply provides connectivity; no user context; inherently open to compromises. Changes to IP addresses can mean extensive configuration, and errors creeping into network security groups, and network access control lists.



Implementing integrated controls can be a challenge. An SDP deployment can offer a single point for network layer firewall configuration.



What Zero Trust Addresses

- Access Control Vulnerabilities - access control mechanisms with current authentication and authorization protocols have weaknesses that are being exploited or bypassed
 - Endpoint monitoring Weaknesses - Vulnerabilities at the Network Layer prior to transport and application protocol and endpoint protection measures.
 - Network Packet Inspection Limitations - Packet analysis happens at the application layer, so incursions can happen prior to detection.
- 
- 

Implementing Zero Trust

Requires authentication before access

- implicitly requires separate control and data planes
- immediate authentication

Requires ability to limit network connectivity and exposure

- drop network connections if authentication fails.

Requires granular trust mechanism

- unlike VPNs that do not have fine-grained access control
- implicitly requires authorization as well as authentication and access

Requires monitoring for suspicious activity

- implicitly requires instant knowledge of connectivity and use of services



How SDP Implements Zero Trust

Hide Assets

- enables deny-all gateway until users/devices are proven

Single Packet Authorization

- enables integrated controls for authentication and authorization
- 



Authenticate BEFORE Access

- Implements a separate control and data channel
- Validation prior to TLS/TCP handshakes
- Fine-grained access control implicit in this design
- Two-way mutually encrypted communications enforced

Benefits of SDP

Reduced attack surface


- enhanced protection for cloud applications
- gives more centralized control to business/system owners
- gain visibility to all authorized connections from whom, where, when, what
- monitored instantly because controls are integrated

Reduced cost of ownership

- reduce costs for endpoint prevention/detection
- reduce cost for incident response
- reduce complexity for integrating controls

Open Specification

- vetted by community
- hackathons



Join the SDP Zero Trust Working Group

The SDP Zero Trust working group launched with the goal to develop a solution to stop network attacks against application infrastructure. With the adoption of cloud services the threat of network attacks against application infrastructure increases since servers can not be protected with traditional perimeter defense techniques.

This is where SDP comes in. Join now and see why SDP truly is the optimal engine for Zero Trust

CSA Working Groups are the go-to source for best practices, research and tools for providing security assurance and privacy in the cloud. CSA's diverse membership of industry practitioners and corporate members has converged and continuously cycled through researching, analyzing, formulating and delivering arguably the most advanced research and tools available across the cloud security spectrum.

Next Meeting

SDP Monthly call

Wednesday, Feb 17th

Other WG calls

SDP DNS paper (subgroup)

Friday, Feb 5th

SDP Zero Trust Specification v2 (subgroup)

Wednesday, Feb 10th

Working Groups

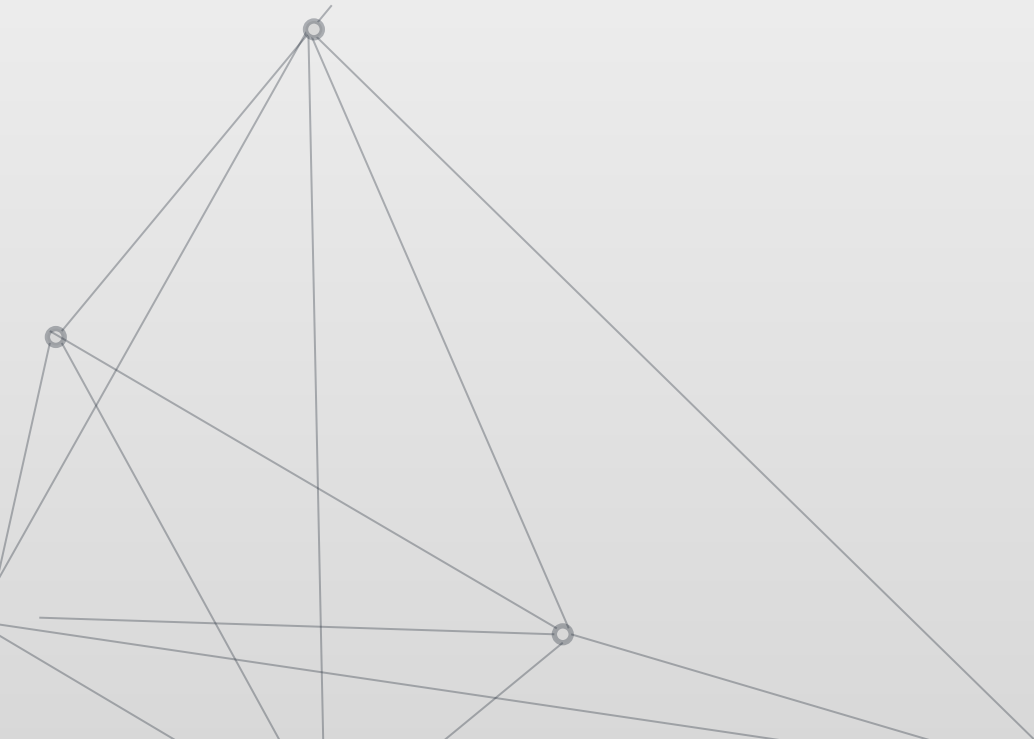
- <https://cloudsecurityalliance.org/research/>





Supplemental slides

More details about SDP Zero Trust
WG



SDP References

Cloud Security Alliance Initiatives

- SDP Architecture version 2.0 published May 2019
- SDP as a DDoS Defense Mechanism published October 2019
- SDP and Zero Trust published May 2020
- Specification 2.0 in March 2021 - In progress

Market Awareness and Adoption Overview

- Cloud Security Alliance [The State of SDP Survey: A Summary](#)

Open Source Reference Implementation (funded by DHS)

- <http://sdpcenter.com/test-sdp/>

SDP Working Group

SDP Co-Chair

Bob Flores

Jason Garbis

Junaid Islam

SDP Technical Advisor

Juanita Koilpillai

CSA Research Analysts


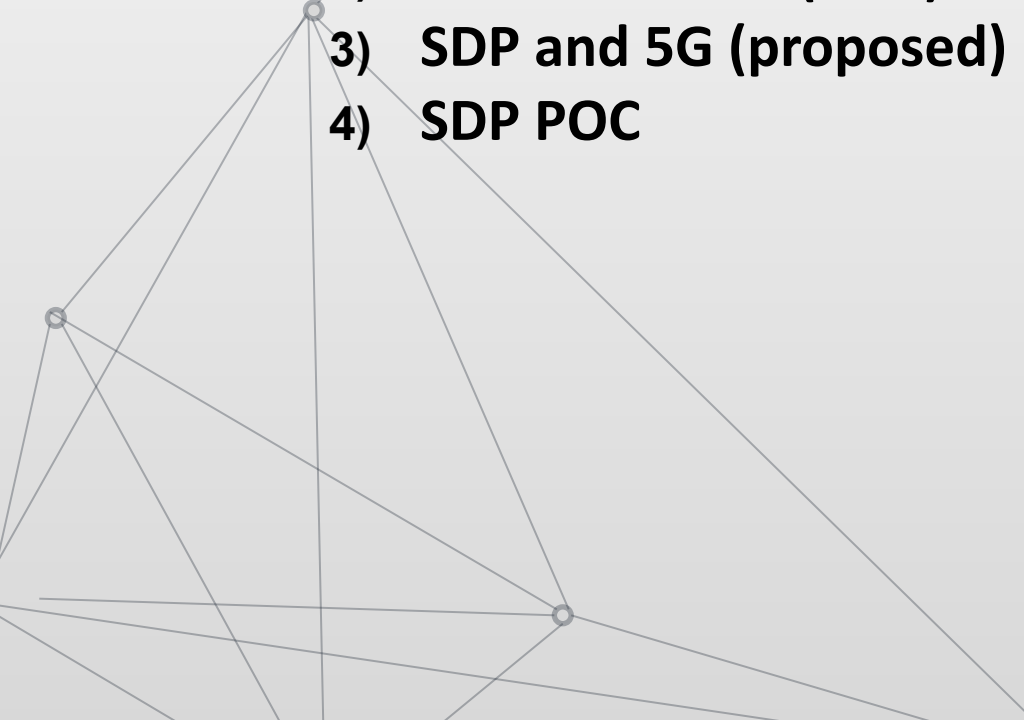
Shamun Mahmud





SDP Working Group Initiatives proposed

Status: Ongoing

- 1) SDP and DNS
 - 2) SDP and DDoS (v2.0)
 - 3) SDP and 5G (proposed)
 - 4) SDP POC
- 
- 

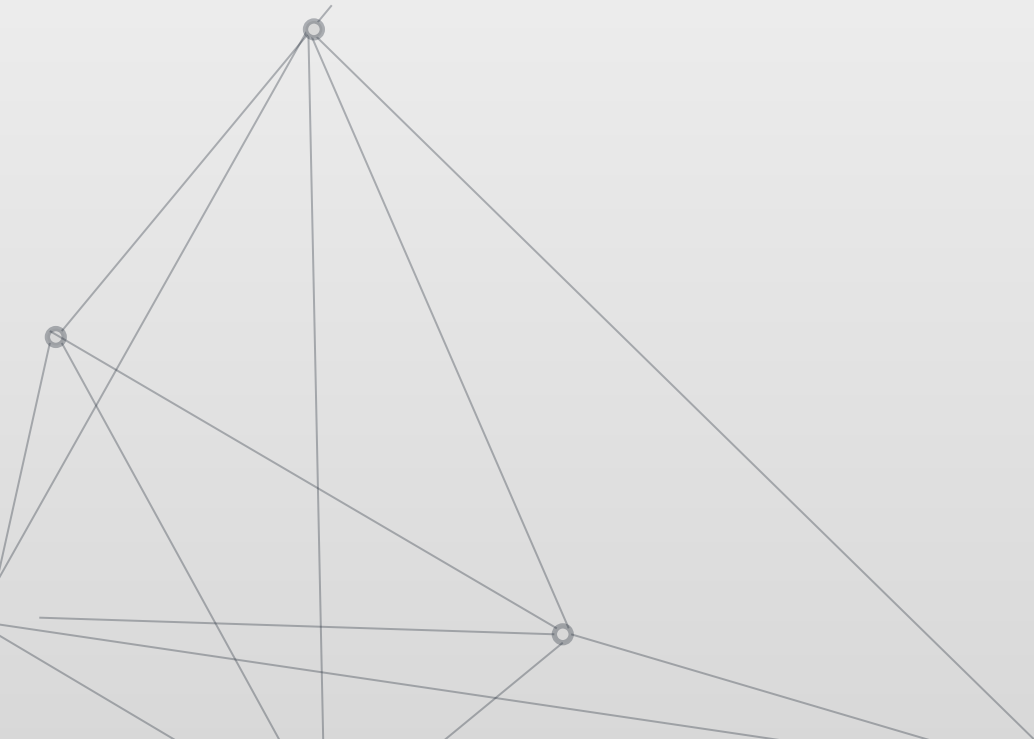


SDP Working Group Initiatives explained

Status: Ongoing. Briefings: Currently Available

1) **Open Source DDoS Initiative**

- 1) **Objective:** Research SDP as a high speed Internet-based packet filter
- 2) **Application:** Enable access to mission critical sites during DDoS attacks

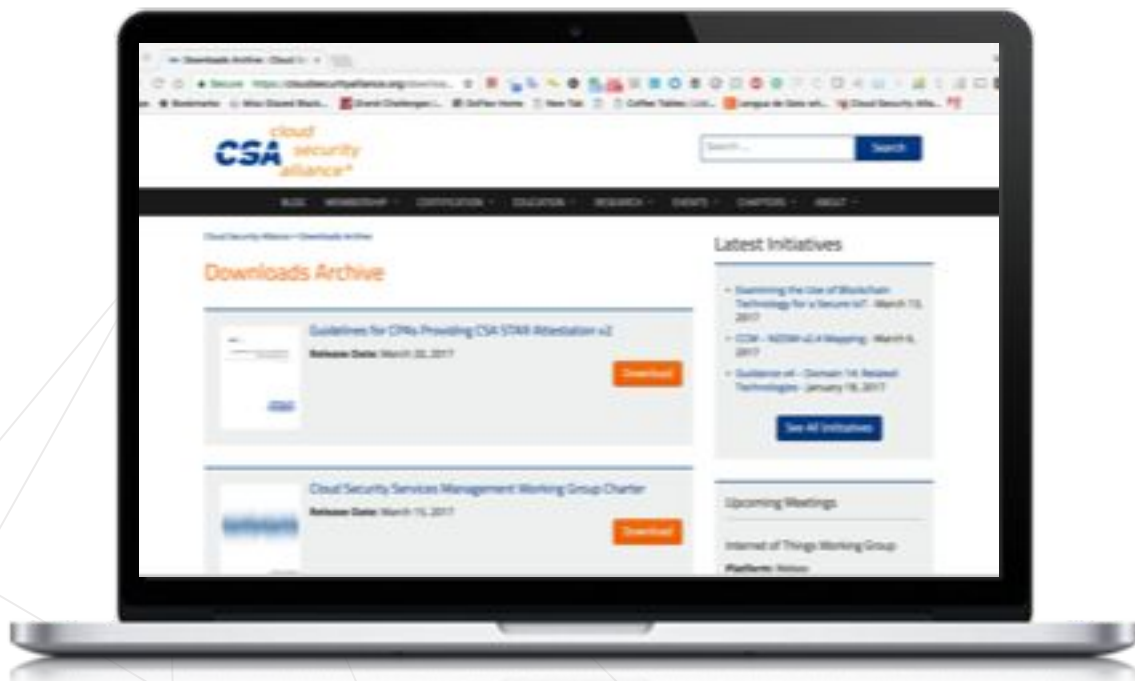


SDP Working Group Initiatives **solicited**

Status: **Ongoing.**

1) **Call for Topics**

- 1) **Objective:** Research future areas where SDP could help. Should be aimed at reinforcing Zero Trust security postures. Filter to a reference implementation
- 2) **Application:** POCs and Use cases.



Contact CSA Research

Email: research@cloudsecurityalliance.org

Twitter: [@CloudSA](https://twitter.com/CloudSA)

Overview: www.cloudsecurityalliance.org/research

Learn: www.cloudsecurityalliance.org/research/cloudbytes

Download: www.cloudsecurityalliance.org/download

