RSACONFERENCE2014
ASIA PACIFIC & JAPAN

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

Software Defined Perimeter: Securing the Cloud to the Internet of Things

SESSION ID: CDS-T08

Jim Reavis

Chief Executive Officer
Cloud Security Alliance
@cloudsa

#RSAC

About Cloud Security Alliance

- Global, not-for-profit organization
- Building security best practices for next generation IT
- Research and Educational Programs
- Cloud Provider Certification – CSA STAR
- User Certification - CCSK
- The globally authoritative source for Trust in the Cloud

"To promote the use of best practices for providing security assurance within Cloud Computing, and provide education on the uses of Cloud Computing to help secure all other forms of computing."

Cloud Security Alliance Fast Facts

- Founded in 2009
- Membership stats as of July 2014
  - 57,000 individual members, 75 chapters globally
  - 250 corporate members
- Offices in Seattle USA, Singapore, Greece, Beijing (2014)
- Over 30 research projects in 25 working groups
- Strategic partnerships with governments, research institutions, professional associations and industry
- www.cloudsecurityalliance.org

Software Defined Perimeter

- Architecture for creating highly secure and trusted end-to-end networks
  - BYOD and Internet of Things
  - Secure virtual private clouds
  - Make network “dark” until entity is authenticated
  - Create dynamic perimeters around clients, applications and hosts
- Complementary to Software Defined Networks (SDN)

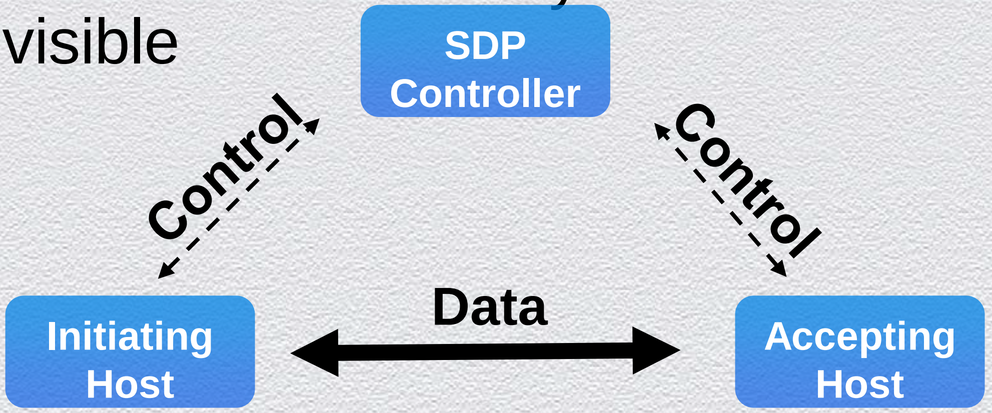
SDP™ Software Defined Perimeter Working Group

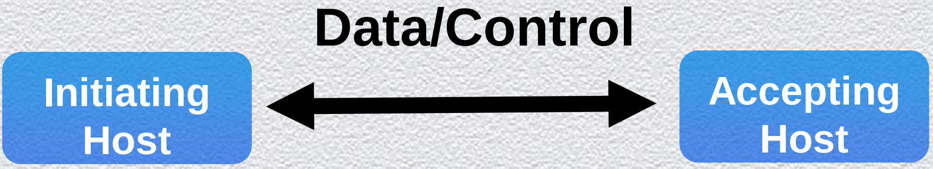
What's different?

- Standardization of "Need-to-know" access model
  - Deployed with Classified, “Top Secret” networks for many years but rarely seen in the commercial world
- Substantial portions of Internet must be made “Dark”
- Integrates latest ideas from NIST & other experts
  - Mutual TLS DHE, Device attestation, identity-based access
- Public domain project
  - Integrates existing standards & best practices into an industry standard

What's different?

- We have separated Control communications from Data communications
- Servers do not accept inbound connections by default – effectively making them invisible
- Controller maintains authorized clients

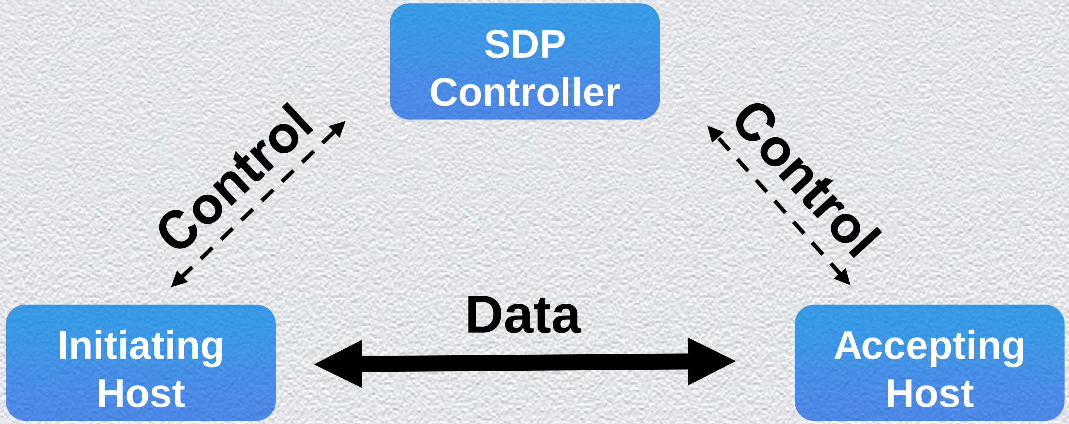




Internet of Today

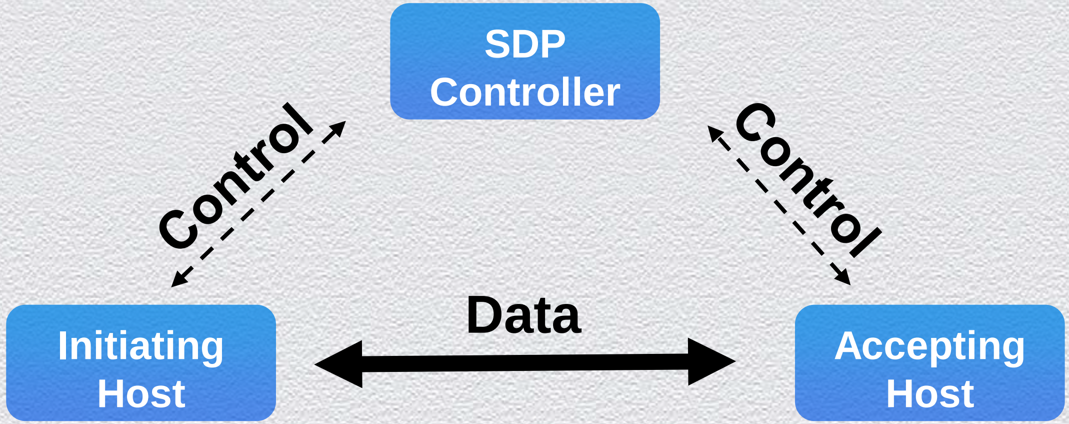
SDP Applications

- Enterprise Application Isolation
- Infrastructure as a Service (Virtual Private Cloud)
- Software as a Service
- Platform as a Service
- Cloud-based VDI
- BYOD, Mobile
- Internet-of-Things



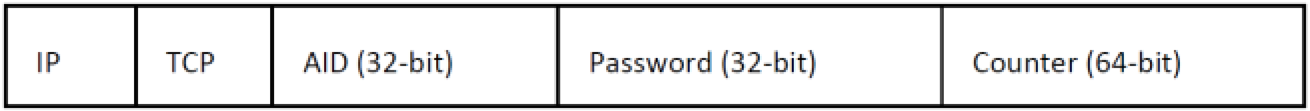
Five Layers of Security Controls

- Single Packet Authorization (SPA)
- Mutual Transport Layer Security (mTLS)
- Device Validation
- Dynamic Firewalls
- Application Binding



Single Packet Authorization (SPA)

- Single Packet Authorization One-Time Password
  - Makes server invisible
  - Mitigates DoS attacks, simplifies attack detection
- Based on RFC 4226 (HMAC-Based One-Time Password Algorithm)
  - Seed: secret 32 bit signed integer for communication pairs
  - Counter: 64 bit unsigned integer for synchronizing communications between pairs
  - Password: generated by the RFC 4226 algorithm



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

Mutual Transport Layer Security (mTLS)

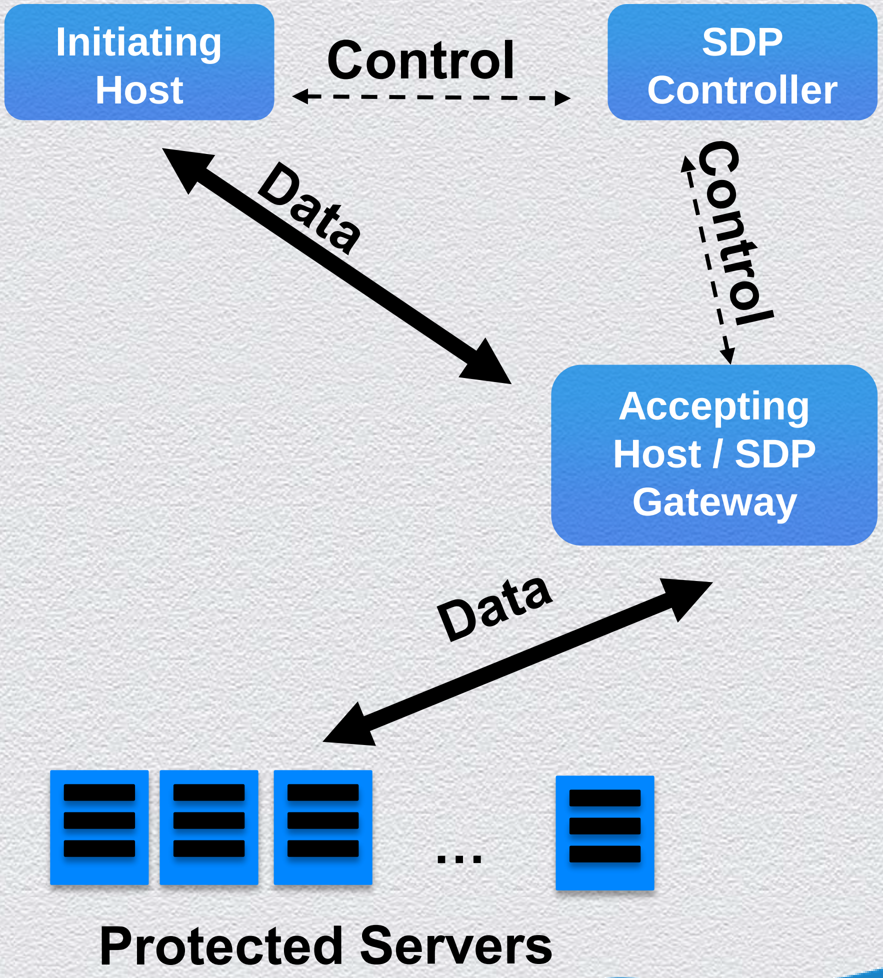
- TLS typically only authenticates servers, not clients
- Mutual TLS is bi-directional authenticates clients
- Validates both entities as part of the SDP
- Root certificate must be known valid root
- Avoid “Root CA explosion” in common browsers
- How root certificate is installed outside of SDP specification
  - Cloud orchestration tools may be used

Device Validation

- Validates that the proper device holds the private key
- Proves that the key is not stolen
- Not included in version 1.0 specification
- Common endpoints have many of elements of uniqueness
- Many methods of device validation in the market

Dynamic Firewalls / SDP Gateways

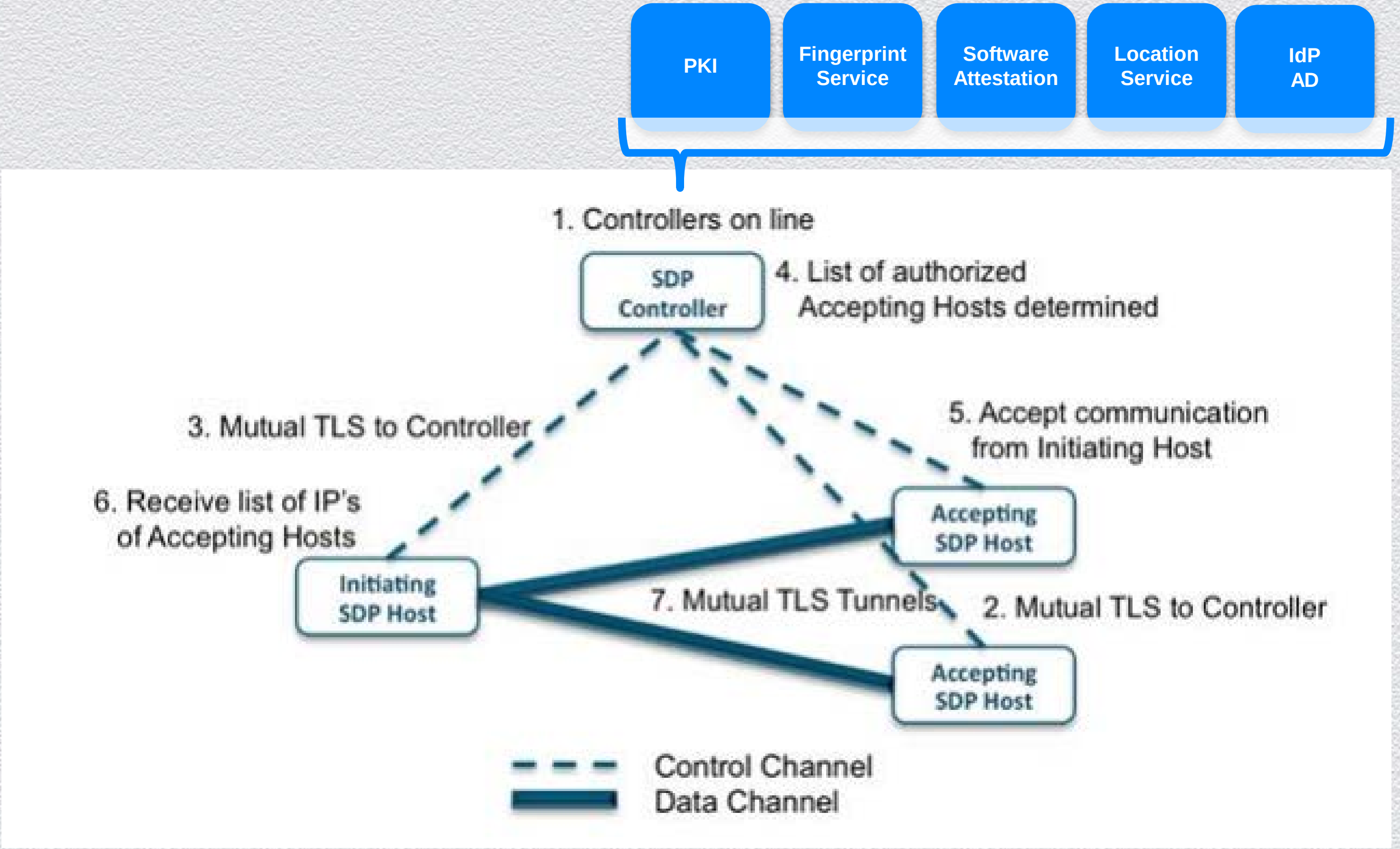
- SDP Gateway: special version of Accepting Host that protects servers
- One initial rule: Deny All
- Dynamically adds a “Permit” rule for Initiating Host to Protected Server as instructed by SDP Controller



Application Binding

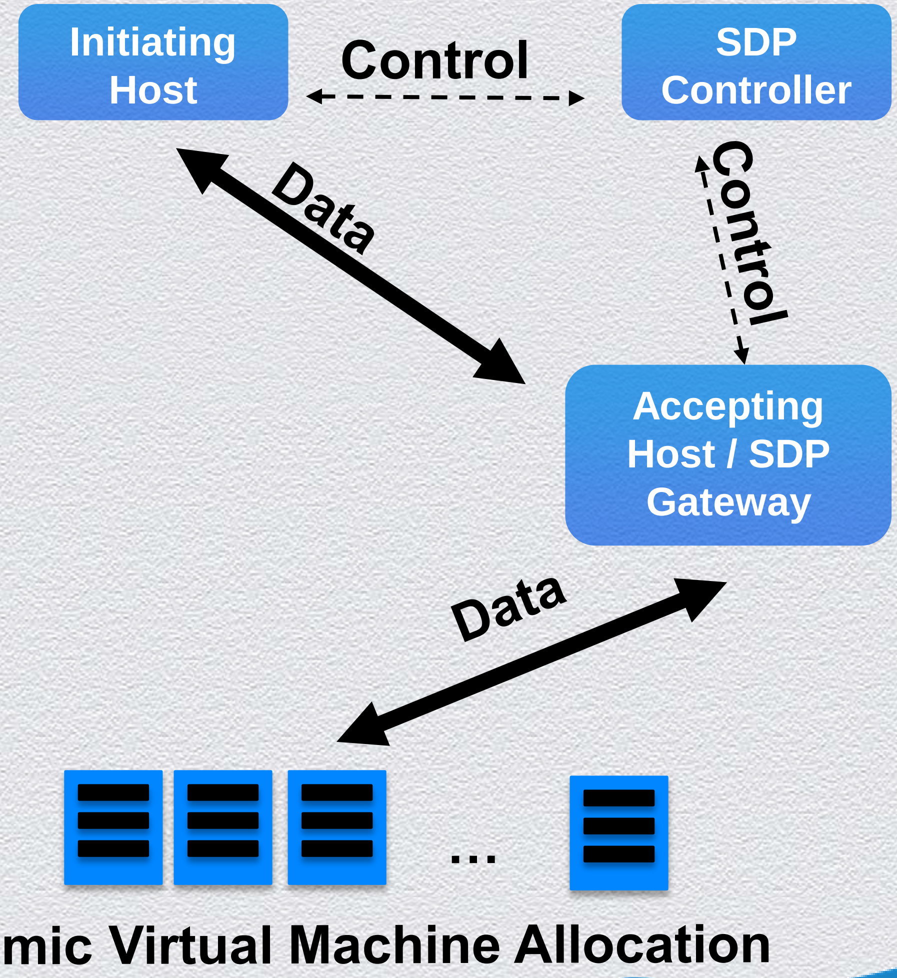
- After authenticating and authorizing both the device and the user, the software defined perimeter creates encrypted TLS tunnels to the protected applications
- Application binding constrains authorized applications so they can only communicate through those encrypted tunnels
- SDP simultaneously blocks all other applications from using those tunnels
- Malware resident on device cannot access encrypted tunnel

Basic Workflow



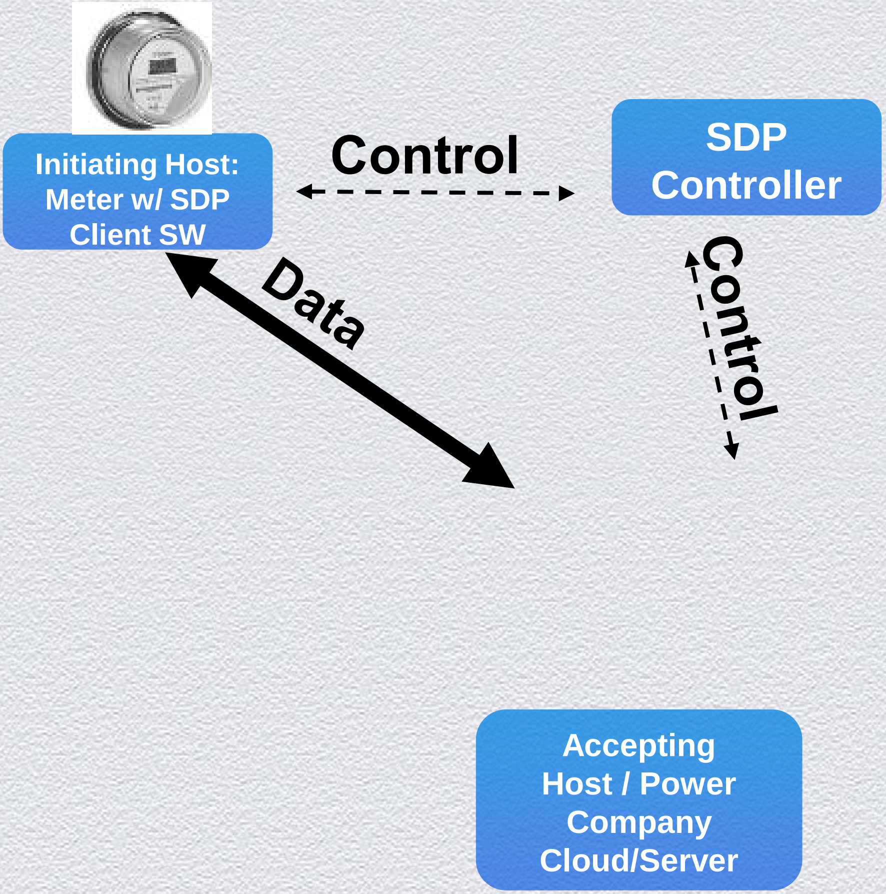
SDP Virtual Private Cloud Use Case

- One or more Accepting Host(s) acting as SDP Gateway
- Locked Down Virtual Machine template
- Dynamic expansion via common cloud orchestration tools
- Dark cloud inside of a public cloud


Initiating Host
Control
SDP Controller
Data
Control
Accepting Host / SDP Gateway
Data
...
Dynamic Virtual Machine Allocation

SDP Internet of Things Use Case

- Smart Power Meter with SDP client acts as an Initiating Host
  - Metering S/W bound to Dynamic VPN according to SDP Controller policy
  - SDP client can be quite small - 50k or less
- SDP Controller provides authorized Power Meter list to Power Company's Servers or Cloud VMs
  - Can use multiple of the Authentication sources, including geolocation
- Power Meter sends data only to intended destination


Initiating Host: Meter w/ SDP Client SW
Control
SDP Controller
Data
Control
Accepting Host / Power Company Cloud/Server

Dynamic Virtual Machine Allocation

SDP Activities

- SDP Hackathon @ RSA Conference 2014 Whitepaper
  - Conducted in popular public IaaS
  - 10 billion packets – no one got past SPA
- SDP Specification 1.0
  - Complete protocol specification
  - Foundation for cloud-based applications
- Download both at https://cloudsecurityalliance.org/research/sdp/#_downloads
- Pilots/prototypes at large enterprises
- Next hacking contest & workshop at CSA Congress US
  - Sept 17-19, San Jose, https://cloudsecurityalliance.org/events/

RSA CONFERENCE 2014
ASIA PACIFIC & JAPAN

#RSAC