The Best of Both Worlds: Cloud + SASE

Prasidh Srikanth, Bitglass
Kenneth G. Hartman, SANS

June 23, 2020

About Me

Kenneth G. Hartman

- BS Electrical Engineering, Michigan Technological University
- MS Information Security Engineering, SANS Technology Institute
- Multiple Security Certifications: CISSP, GIAC Security Expert, etc.
- Certified SANS Instructor – SEC545 Cloud Security Architecture & Operations

The content and opinions in this presentation are my own and do not necessarily reflect the positions, strategies, or opinions of any current or previous employer.

www.kennethghartman.com   **@kennethghartman**

"I help my clients earn and maintain the trust of their customers"

SANS

from the most trusted name in information security

"Identity is the new perimeter" ???

SANS

Examples of Convergence – Network Hardware

IDS

Firewall ⎤ Next Generation Firewall

Access Point

Router SOHO "Router"

Switch

Hub
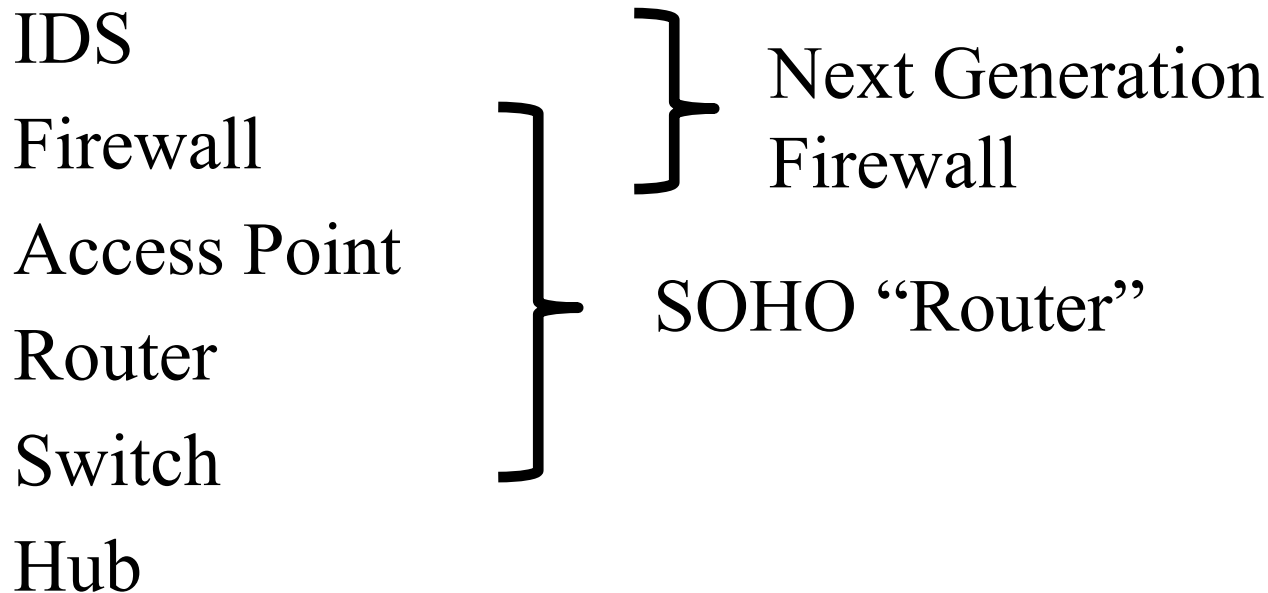
SASE Convergence

Network as a Service

Connect it

Network Security as a Service

Sensitive Data Awareness

Secure it

Threat Detection

Market Convergence

- SD-WAN
- Carriers
- CDN
- WAN Optimization
- Network as a Service
- Bandwidth Aggregators
- Networking Vendors

- Network Security
- CASB
- Cloud SWG
- ZTNA/VPN
- WAAPaaS
- FWaaS
- DNS
- RBI

Secure Access Service Edge

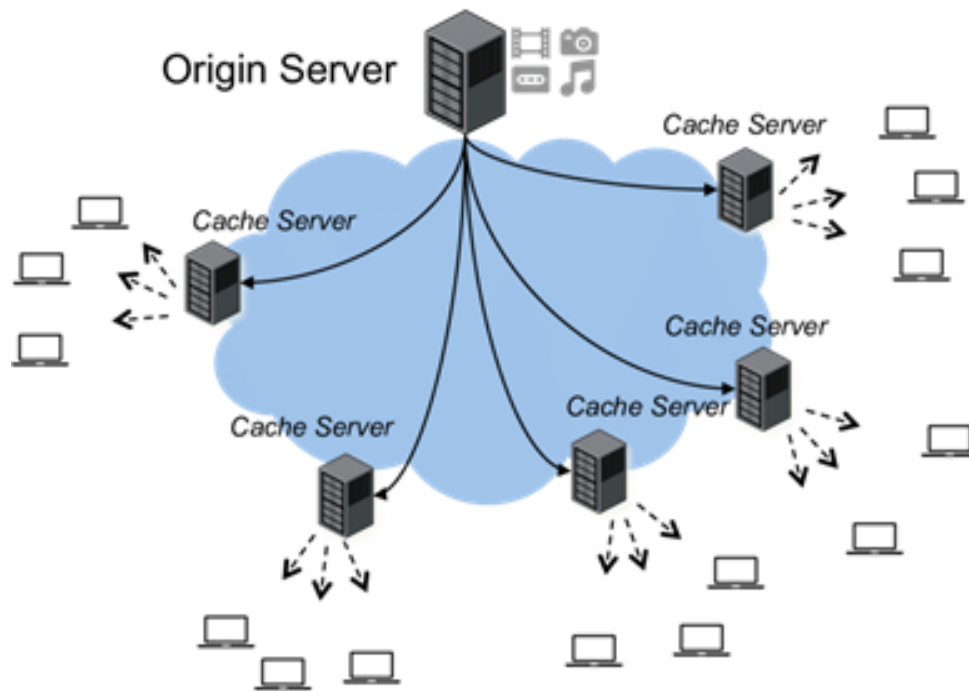Gartner: *The Future of Network Security Is in the Cloud*, ID G00441737

Buzzword Bingo

CDN	FWaaS	WAF	DNS
VPN	CASB	NGFW	RBI
MPLS	IDaaS	SWG	NIDS/NIPS
SD-WAN	ZTNA	WAAPaaS	EDR

from the most trusted name in information security

Content Delivery Network (CDN)

Example CDN Locations
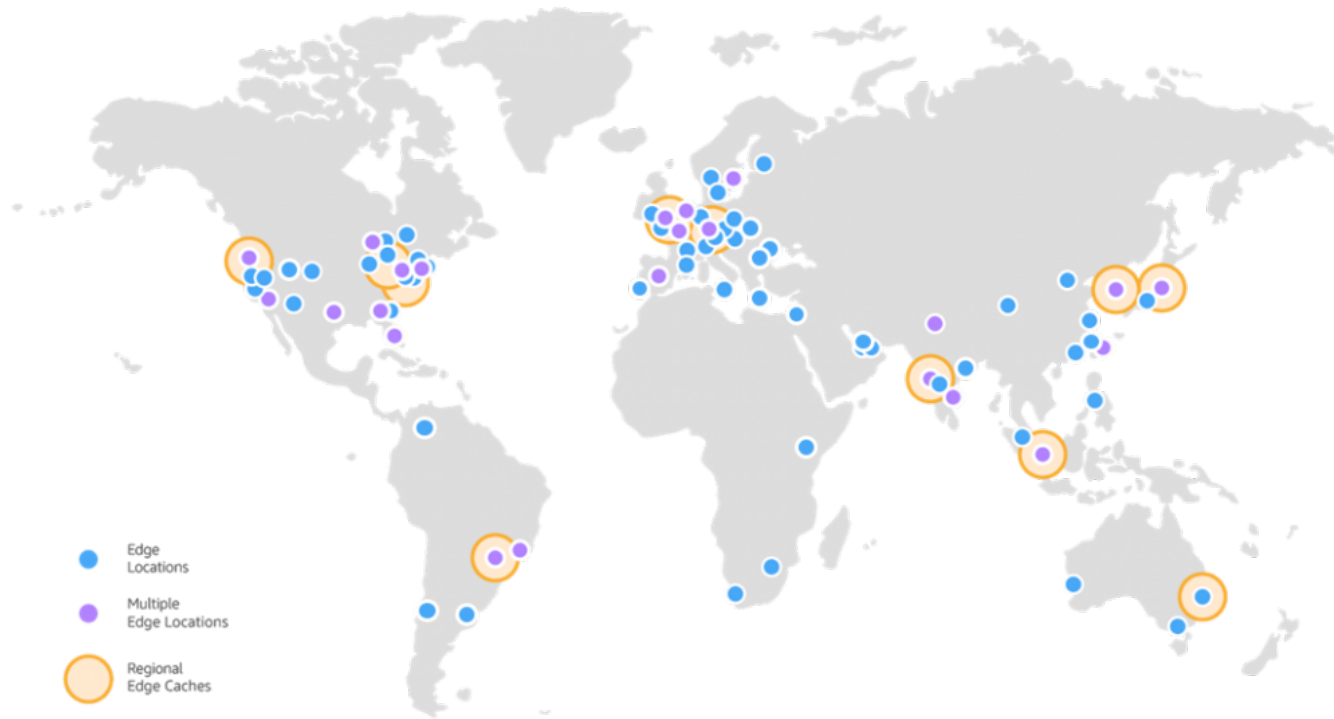
Edge Locations

Multiple Edge Locations

Regional Edge Caches

Buzzword Bingo

CDN	FWaaS	WAF	DNS
VPN	CASB	NGFW	RBI
MPLS	IDaaS	SWG	NIDS/NIPS
SD-WAN	ZTNA	WAAPaaS	EDR

from the most trusted name in information security

Cloud Access Security Broker

1. Managed Devices
Forward Proxy
Device Profiler

SAML Proxy + SSO

Fwd. Proxy

Rev. Proxy

2. Unmanaged Devices
Reverse Proxy + AJAX VM
Selective wipe, device config
No agents/No cert install
Any device

3. API
Data-at-rest/sharing
Centralized control
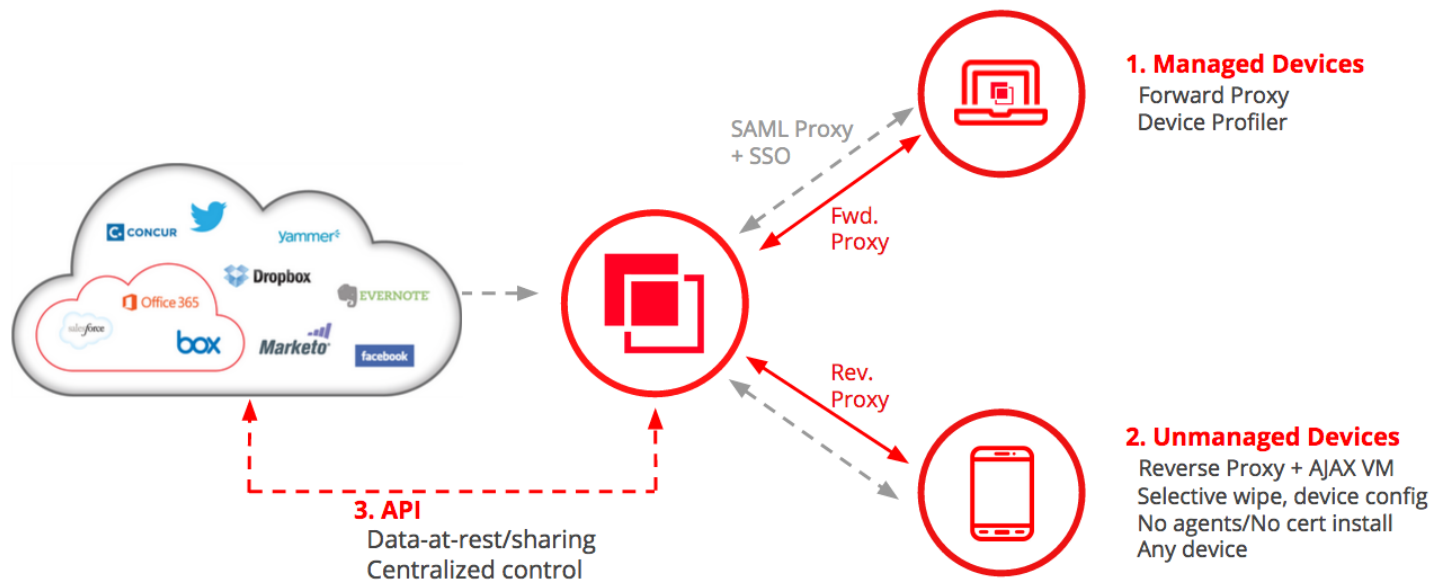
Four core features of cloud access security brokers

VISIBILITY	COMPLIANCE	THREAT PROTECTION	DATA SECURITY
Shadow IT detection	User authentication and authorization	User behavior analysis	Encryption
Cloud services usage tracking	Enforce regulatory requirements	Malware detection	Tokenization
Reporting and logging			Enforce data loss prevention policies
Alerting			

Buzzword Bingo

CDN	FWaaS	WAF	DNS
VPN	CASB	NGFW	RBI
MPLS	IDaaS	SWG	NIDS/NIPS
SD-WAN	ZTNA	WAAPaaS	EDR

from the most trusted name in information security

SANS

Secure Web Gateway

Buzzword Bingo

CDN	FWaaS	WAF	DNS
VPN	CASB	NGFW	RBI
MPLS	IDaaS	SWG	NIDS/NIPS
SD-WAN	ZTNA	WAAPaaS	EDR

from the most trusted name in information security

SANS