Aruba SASE Solutions in Federal

Ken Rich and Matthew Gann

October 3, 2023

WHAT'S DRIVING THE JOURNEY TO SASE?

The Challenge of a Dissolving Perimeter has Reached Critical Mass.

Transformation to Cloud

Cloud Native Applications
Hybrid Data Centers

Proliferation of New Sites and Devices

IoT, Mobile, Laptops

Hybrid Workforce

Users Everywhere, Anywhere

Access Has Fundamentally Changed - Work is done from anywhere and Apps now span across hybrid cloud.

3 KEY TRENDS TO WATCH

$4.35 M

Global average cost of a data breach in 2022, up 13% from 2020[1]

$9.2 B

Total worldwide end-user spending on SASE in 2023 is outpacing what was spent in 2022 by a significant margin.[2]

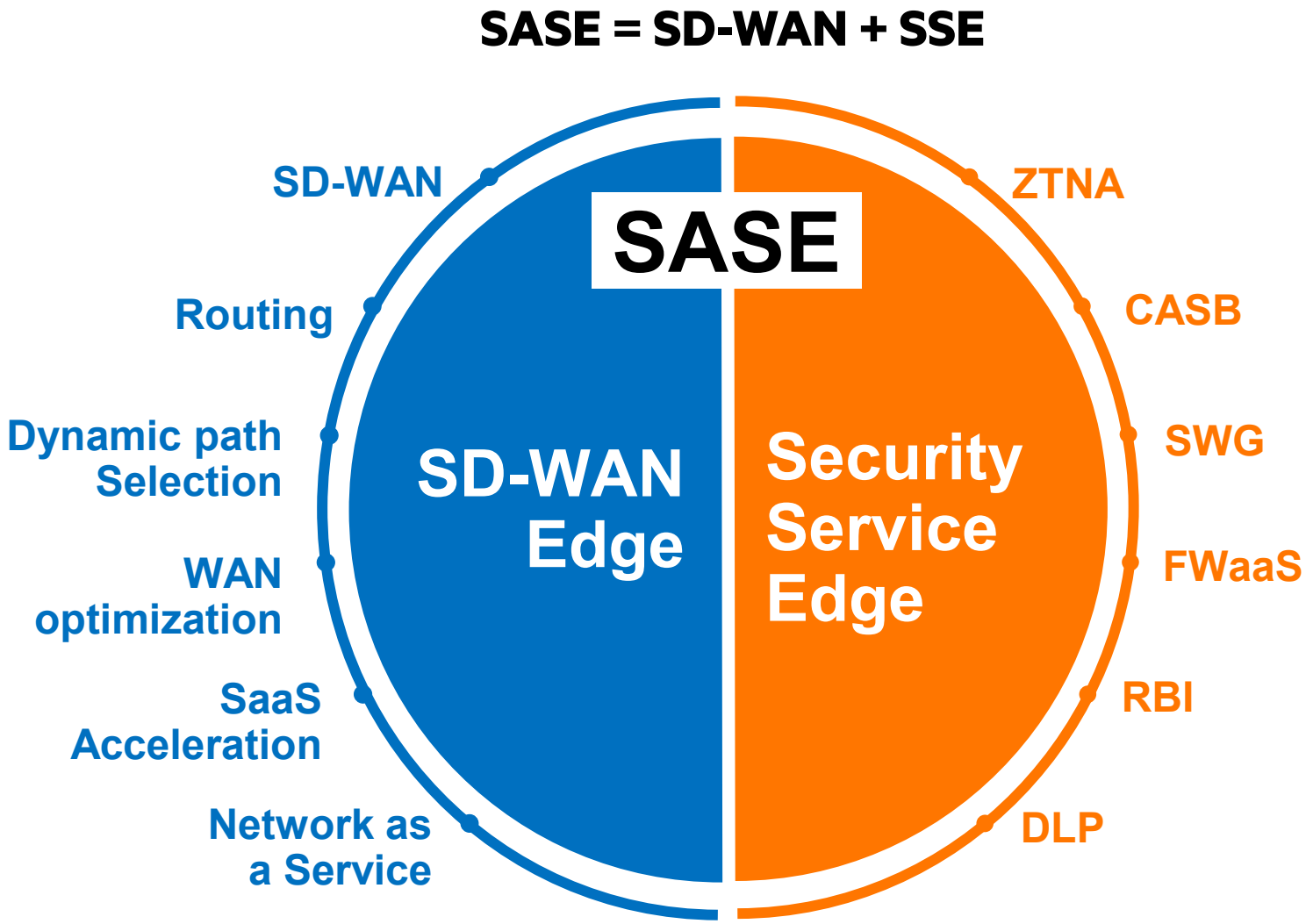
80%

Of SD-WAN deployments will incorporate SSE requirements by 2024[3]

1. IBM study, Cost of a data breach 2022
2. Gartner 2022
3. Gartner 2022

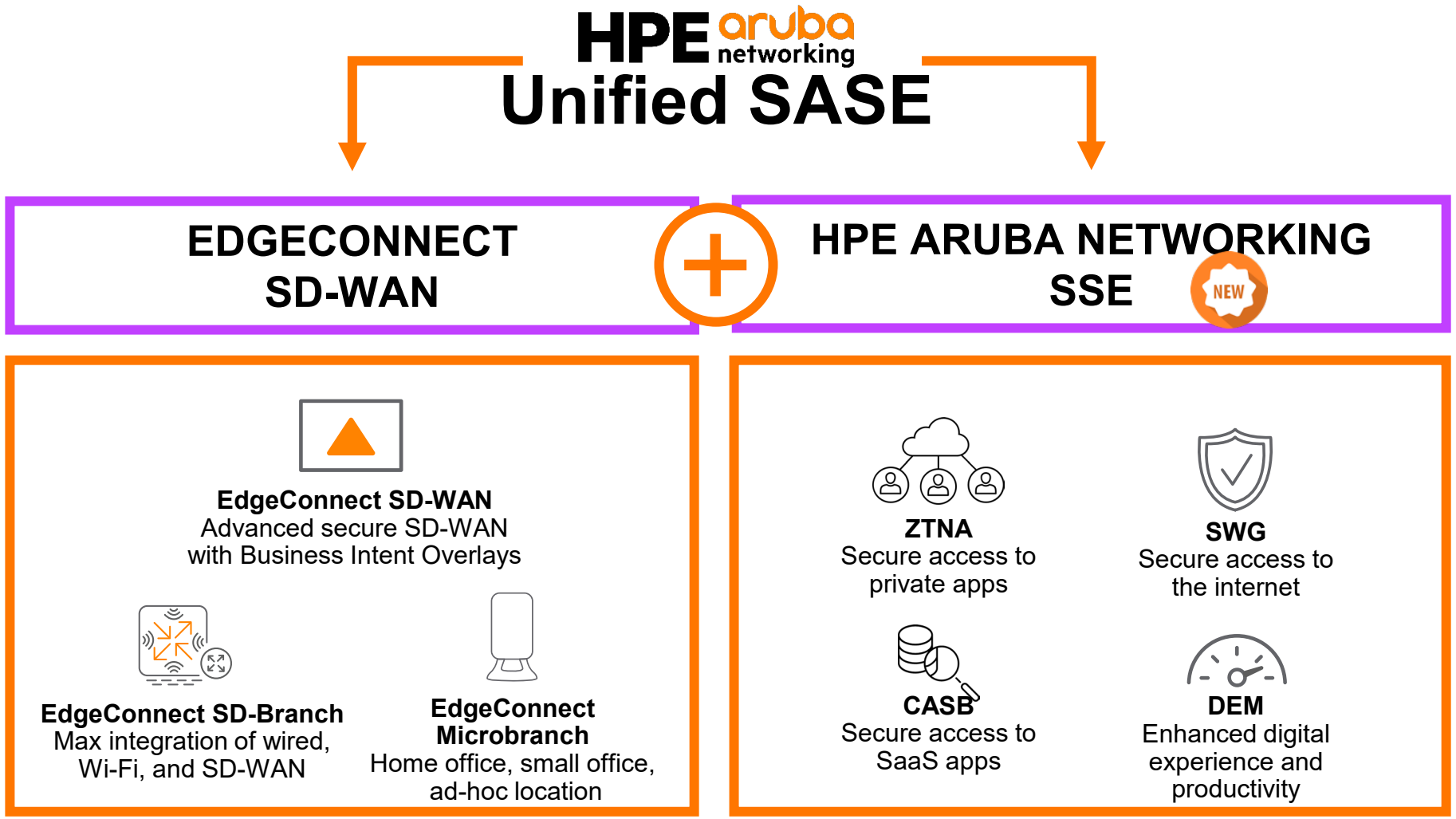
WHAT IS SECURE ACCESS SERVICE EDGE?

As the Security Perimeter is Dissolving, Security Concepts need to Adjust



HPE ARUBA NETWORKING UNIFIED SASE

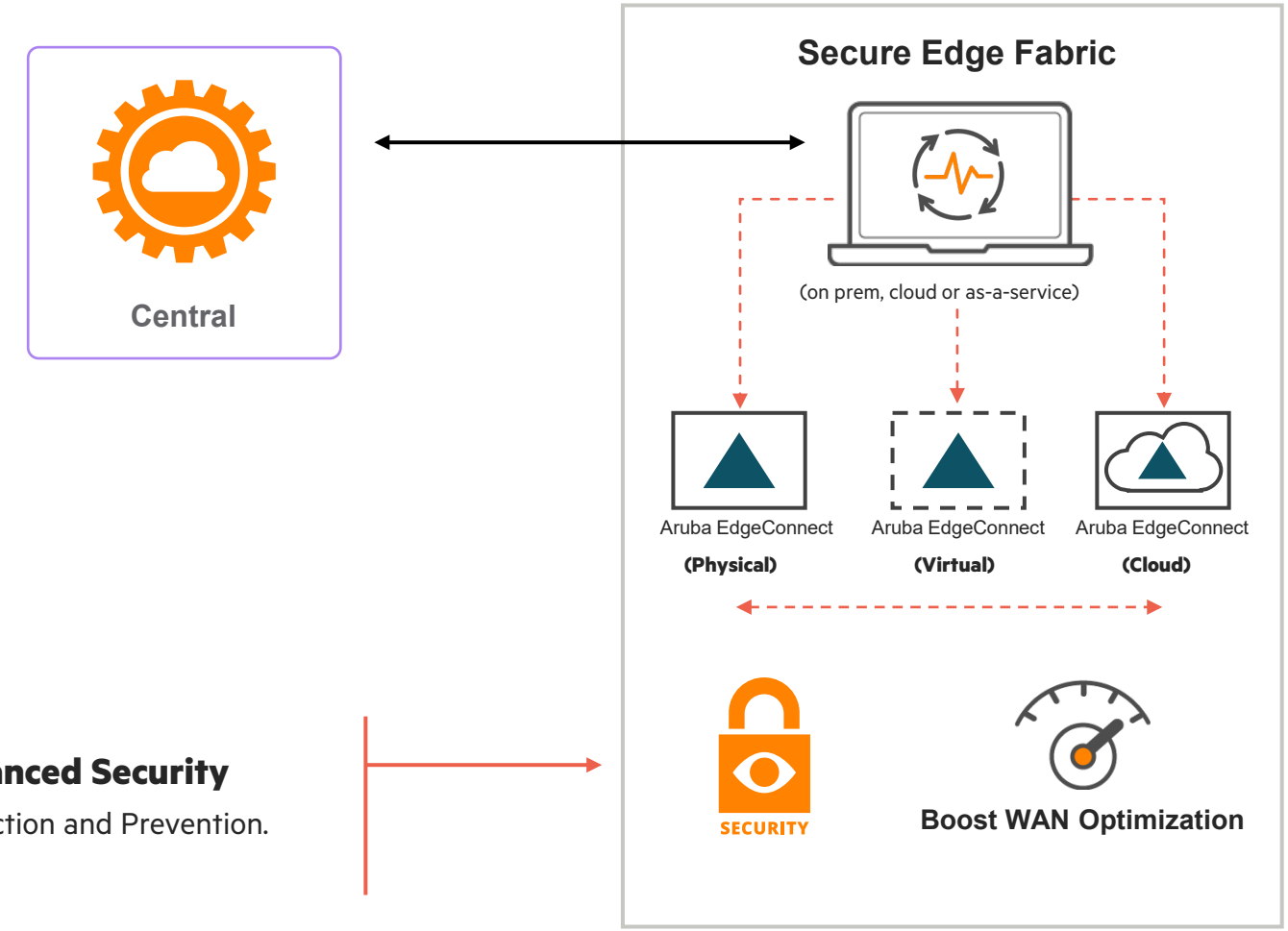
Deploy Industry-leading SD-WAN with the HPE Aruba Networking SSE Platform



Aruba EdgeConnect SD-WAN Solution

Aruba EdgeConnect Secure edge Architecture

Designed for today's cloud-first enterprise



Aruba Orchestrator

Centralized policy orchestration, monitoring and reporting

Aruba EdgeConnect

Unified SD-WAN edge platform: routing, security, SD-WAN and WAN Optimization

Aruba Boost WAN Optimization

On-demand WAN Optimization (Optional)

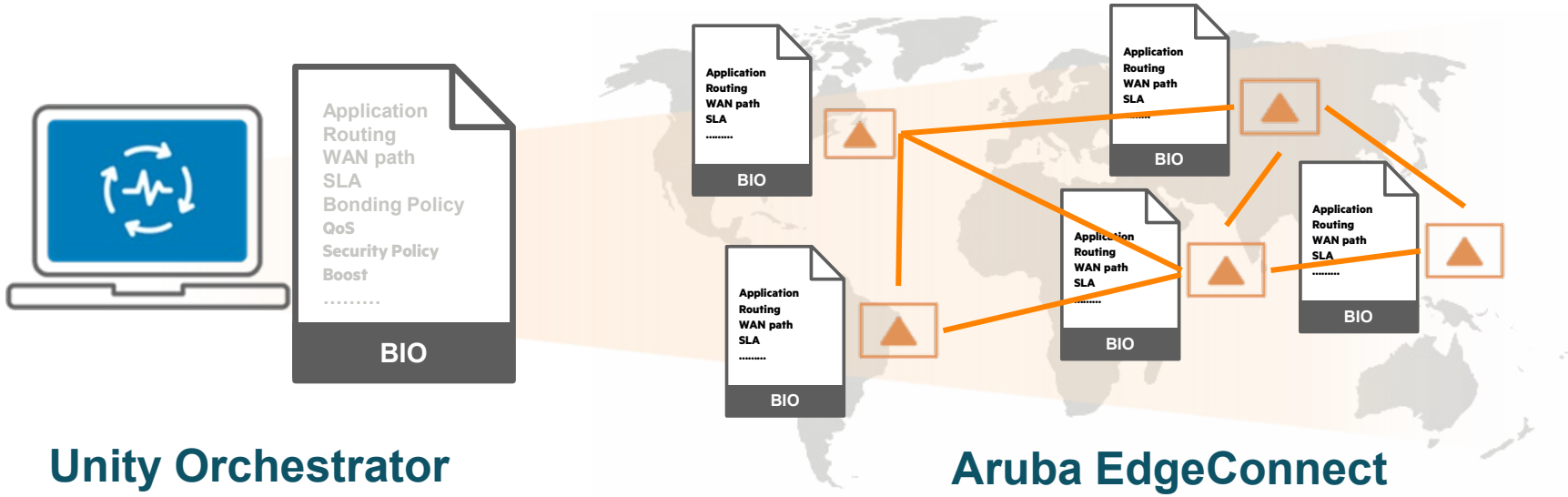
Aruba Advanced Security

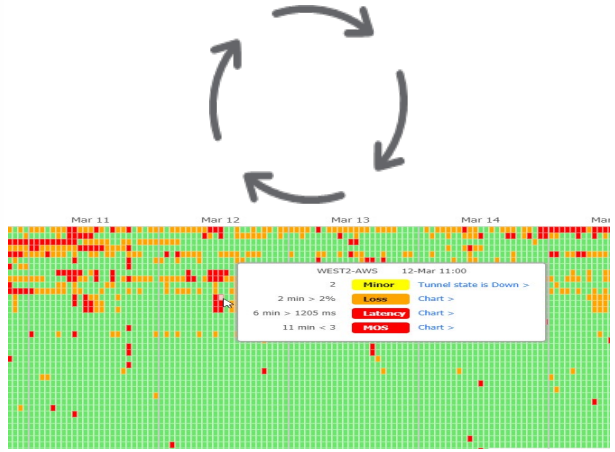
Intrusion Detection and Prevention.

HPE aruba networking

A Completely Automated Approach

Standardize, Templatize & Automate Provisioning





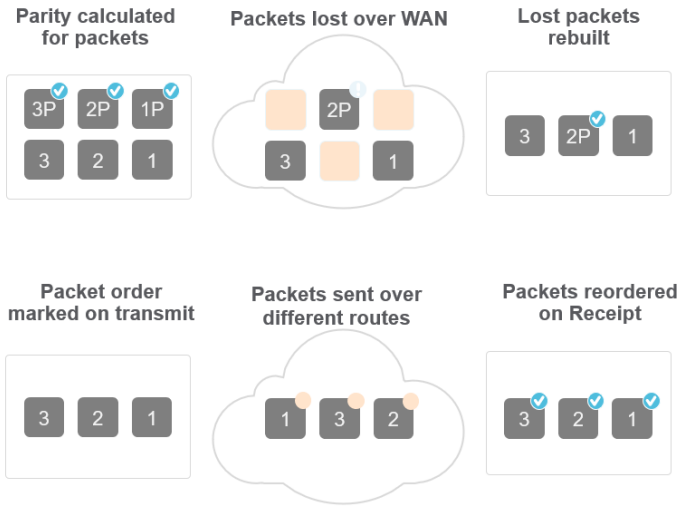
1. Create Business Intent Overlay (BIO)
2. Push and Maintain Policies Globally
3. Continuously Monitored and Updated

BUSINESS INTENT OVERLAYS

Apps, IaaS, PaaS	Circuits	Bonding + SLA	Topology	SaaS, Cloud, Internet Apps	Internet Policy & Firewall, SASE	Overlay Defaults
Real Time Overlay						
	MPLS (Primary) Internet (Primary) LTE (Backup)	**High Availability** Loss: 1% Latency: 400ms Jitter: 200ms	**Mesh**	WebEx, zoom, Ring Central, 8x8	**Best Circuit + Local Firewall** Local Firewall Datacenter (Backup)	**IDS/IPS:** All **FW Zone:** Real Time **QoS:** Real Time **Boost:** Disabled
Enterprise Apps Overlay						
amazon web services, SAP, Azure, ORACLE	MPLS (Primary) Internet (Primary) LTE (Backup)	**High Quality** Loss: 2% Latency: 600ms Jitter: 300ms	**Hub & Spoke**	Office 365, box, salesforce, workday, slack	**Cloud Firewall + Load Balance** zscaler Datacenter (Backup)	**IDS/IPS:** East-West **FW Zone:** Restrict **QoS:** Enterprise **Boost:** Enabled
Default Overlay						
PDF	MPLS (Primary) Internet (Primary) LTE (Backup)	**High Efficiency** Loss: 5% Latency: 800 ms Jitter: 500 ms	**Hub & Spoke**	YouTube	**Cloud Firewall + Load Balance** PRISMA Datacenter (Backup)	**IDS/IPS:** All **FW Zone:** Default **QoS:** Best Effort **Boost:** Disabled

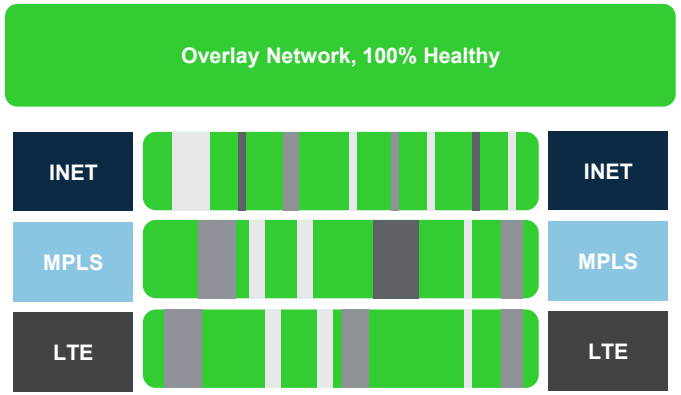
INTERNET QOS, ANY APPLICATION, ANY TRANSPORT

Path Conditioning



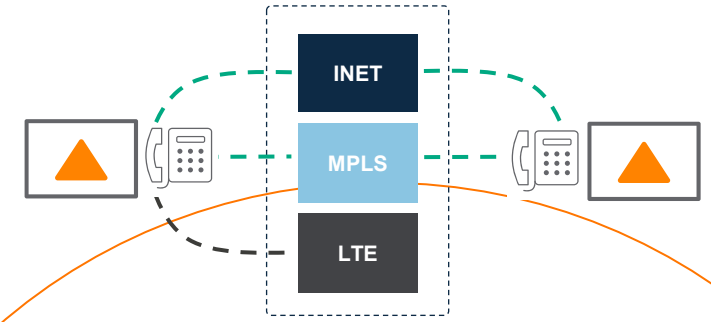
Forward Error Correction (FEC) and Pack Order Correction (POC) fix underlying network issues from impacting application performance.

Overlay Network



Underlying network transports are abstracted allowing for applications to be seamlessly moved between circuits based on load, health or SLA

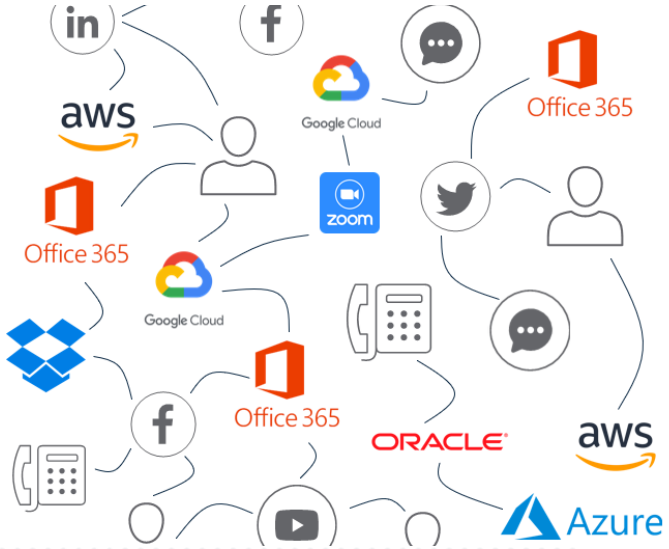
Dynamic Path Selection



Dynamic Path Selection flexibly routes packets across the best possible circuit depending on network health and overlay policy.

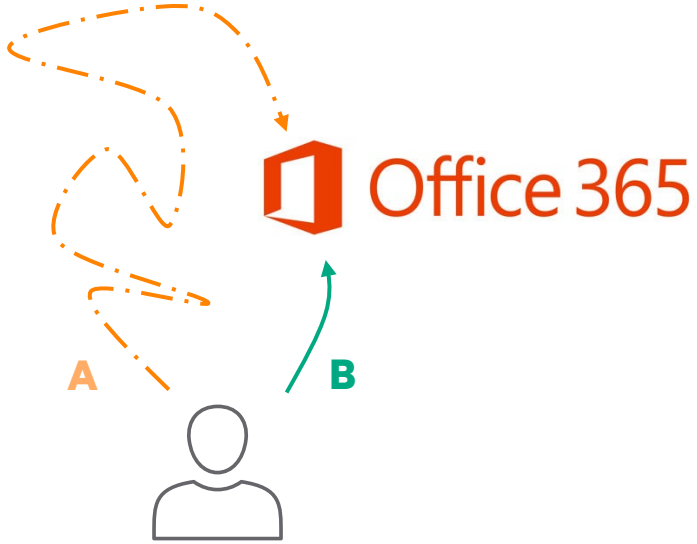
SAAS OPTIMIZATION

Internet Application Map



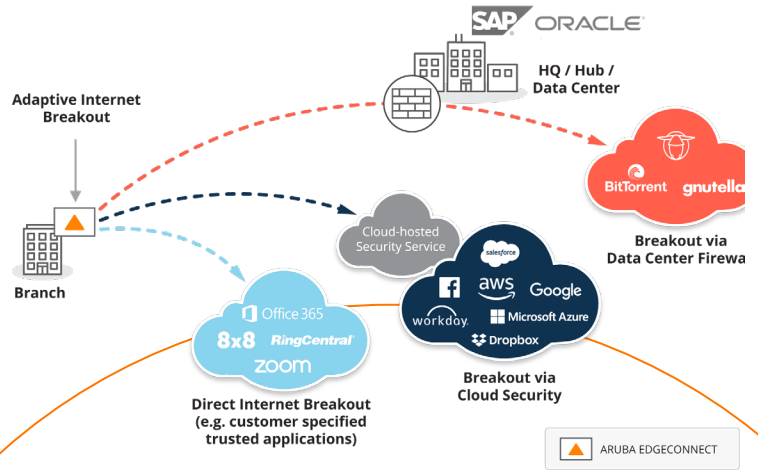
Simple and always up-to-date SaaS application definitions enables optimized routing policies that deliver the highest quality of experience for mission critical apps.

Best SaaS Path



Route SaaS services to their **closest point of presence** using the **best possible path** with advanced network health & performance measurements and **local DNS resolution**.

Secure Local Breakout

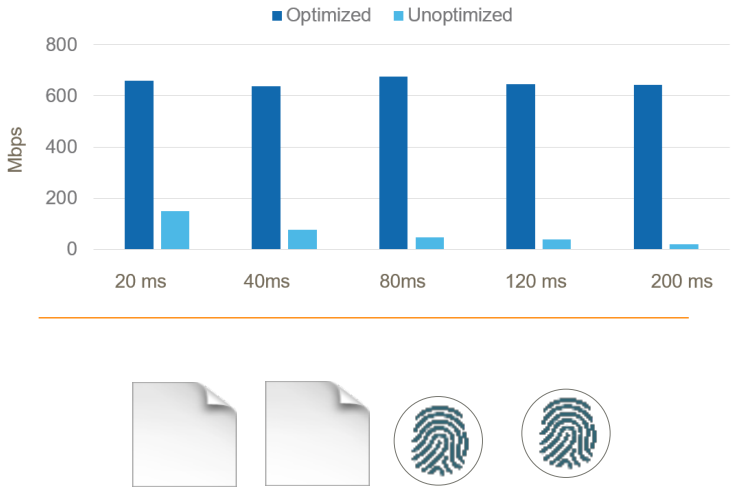


Secure Internet applications without sacrificing performance by leveraging a cloud-first security architecture with intelligent application steering.

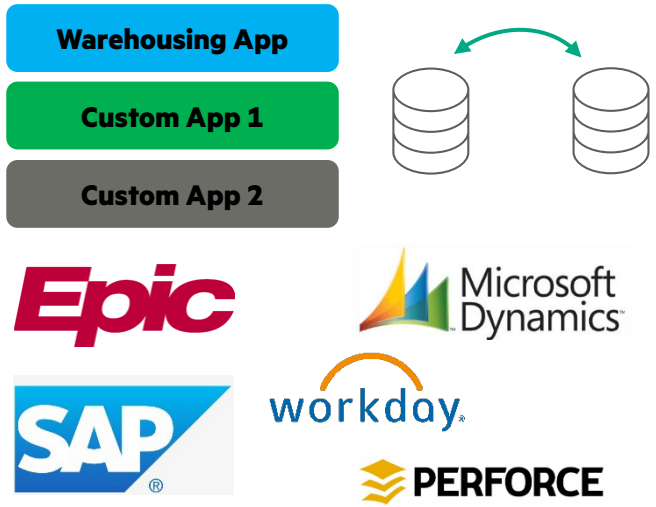
HPE aruba networking

BOOST, ACCELERATE APPLICATION PERFORMANCE

WAN Optimization



Any Application



Applied Anywhere

High Speed TCP and Data Deduplication eliminate the performance impacts of latency and reduces load on the network adding virtual bandwidth.

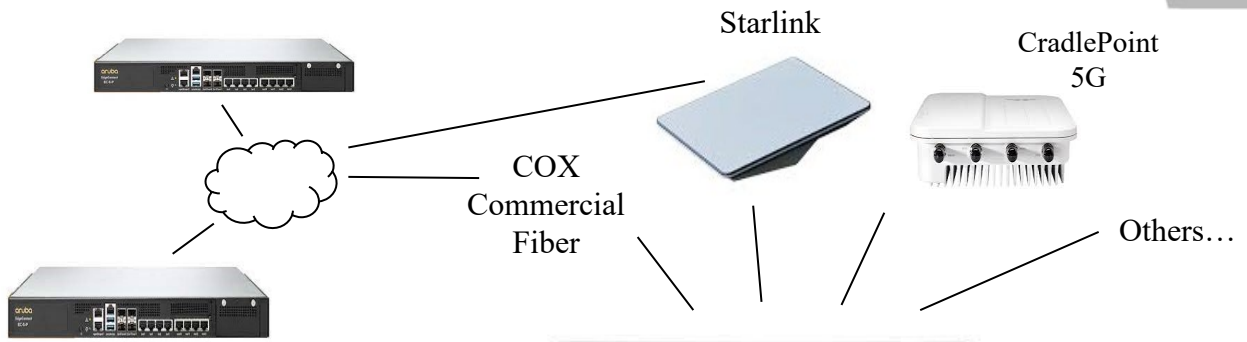
Optimization can be applied towards ANY application where an EdgeConnect appliance is in place between the client and server.

Workloads can be optimized in the branch, datacenter or cloud for mission critical applications, large datasets and custom applications.

MWR WIRELESS

USS Abraham Lincoln (CVN-72)

DEMONSTRATION FOOTPRINT

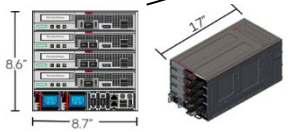


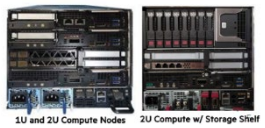
SDN: Aruba Edge Connects

Core Commercial Router:
Netgate 1541

Switching – Aruba 6300M

Tactical
Fleet
Network





QOW: HPE EdgeLine 8000

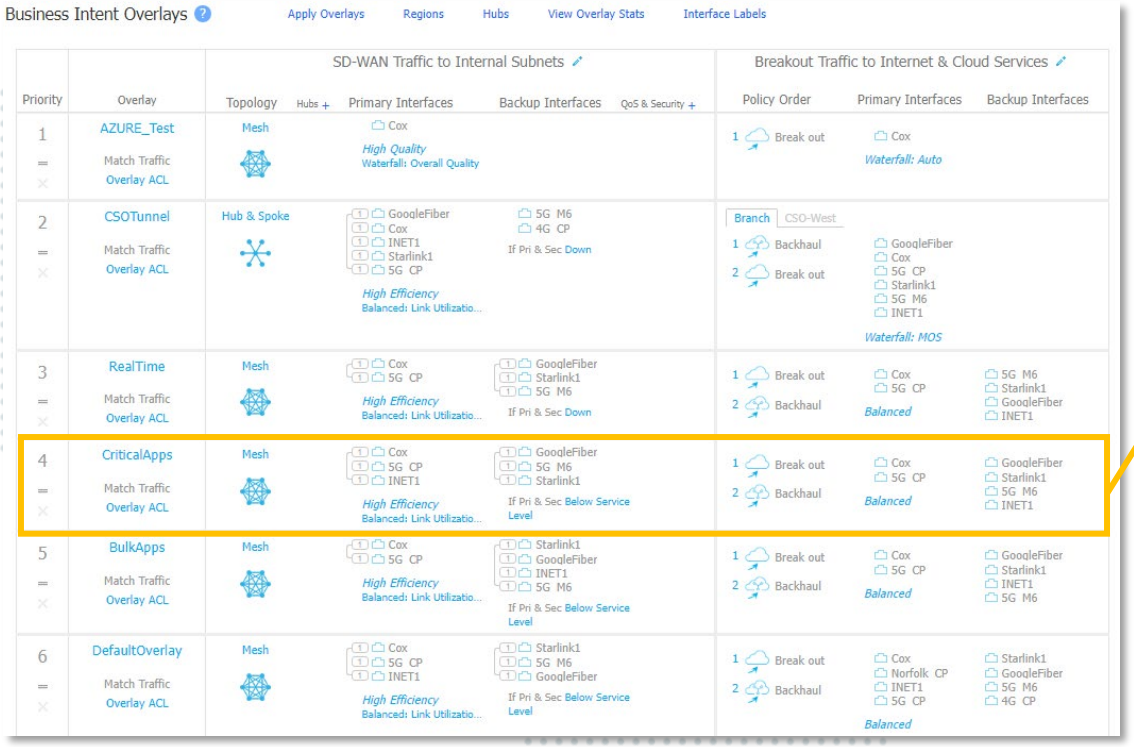
Azure DOD GOV Cloud
extension

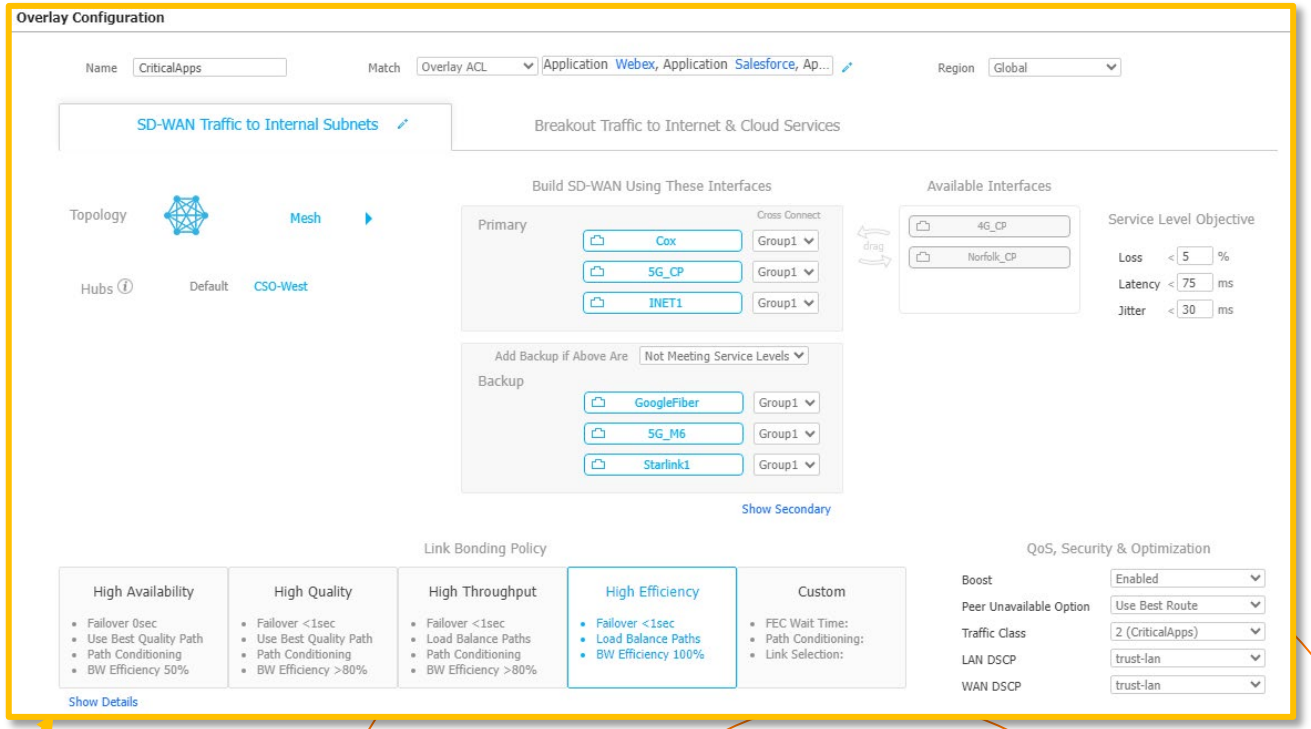
Wireless Controller
– Aruba 7030

User Policy
Manager – Aruba
ClearPass C1000

Wireless Access Points (25) –
Aruba AP-535, 555, 575

CIRCUIT DIVERSITY AND LOAD BALANCING





CIRCUIT DIVERSITY AND LOAD BALANCING

Interface	Inbound Bytes	Outbound Bytes	Inbound Firewall Denies	Outbound Firewall Denies	Inbound Avg BW Util...	Outbound Avg BW Ut...	Inbound Max BW Util...	Outbound Max BW U...
lan0 (Data)	827G	7.4T	0	0	0	0	0	0
wan1 (Cox)	4.8T	542G	161M	0	1.06	0.12	62.68	33.31
wan2 (5G_CP)	2.5T	287G	164M	0	5.61	1.27	100	100
wan0 (Starlink1)	58G	6.5G	5.0M	0	0.05	0.05	67.74	33.98

Interface	Inbound Packets	Outbound Packets	Inbound Firewall Denies	Outbound Fire...	Inbound Avg BW Util...	Outbound Avg BW Ut...	Inbound Max BW Util...	Outbound Max BW U...
lan0 (Data)	2,217,809,688	5,751,174,901	0	0	0	0	0	0
wan1 (Cox)	3,711,745,662	1,341,244,405	2,323,669	0	1.06	0.12	62.68	33.31
wan2 (5G_CP)	2,032,602,793	845,461,200	1,362,617	0	5.61	1.27	100	100
wan0 (Starlink1)	63,034,221	25,490,916	107,312	0	0.05	0.05	67.74	33.98

HPE aruba networking

VISIBILITY

Application Bandwidth

LAN WAN

10 Rows Search

Application	<-- Reduction %	<-- Bytes	Bytes -->	Reduction % -->
Https	0	2.2T	84G	0
Facebook	0	1.0T	29G	0
Youtube	0	990G	14G	0
Apple	0	946G	31G	0
Instagram	0	393G	19G	0
Googleapis	0	136G	239G	0
Netflix	0	327G	4.3G	0
Facetime	0	143G	182G	0
Akamaized	1	255G	2.6G	0
AppleUpdate	0	222G	3.0G	0

Top Talkers

LAN WAN

10 Rows Search

IPs	User	Domain	IP Details	Top Destinations	<-- Bytes	Bytes -->	Flows Star...	Flows Ended...
10.0.51.3 Default					159G	5.3G	188	237
34.104.32.36 Default		prod.gccrunchyroll.com			150G	1.5G	1730	1818
10.0.52.91 Default					133G	537M	1688	1766
10.0.0.152 Default					104G	426M	1898	2020
146.75.94.133 Default		fy.v.vrv.co			86G	697M	214	262
10.0.57.128 Default					75G	215M	110	134
142.251.2.207 Default		gcs-us-00003.content-storage-upload.go...			67G	20G	2108	2216
10.0.63.139 Default					64G	822M	226	252
10.0.25.144 Default					61G	1.5G	623	706
10.0.52.77 Default					58G	2.6G	427	469

Countries	<-- Bytes	Bytes -->
United States of America	4.9T	521G
Sweden	295G	3.2G
Canada	56G	550M
United Kingdom of Great Britain and Northern Ireland	8.8G	374M
Ukraine	8.8G	46M
Netherlands	5.1G	41M
Philippines	1.3G	1.2G
Indonesia	2.0G	20M
Brazil	1.5G	101M
Guam	464M	910M
France	1.1G	13M
Germany	951M	7.0M
Australia	863M	14M
Portugal	488M	344M
Japan	696M	31M
New Zealand	456M	3.6M
Mexico	18M	347M
Puerto Rico	131M	126M
Singapore	117M	110M
Belize	185M	2.3M

HPE aruba networking

VISIBILITY

Flow details for IP1: 10.0.62.254 Port1: 55582 IP2: 34.104.32.36 and Port2: 443

General | Optimization | TCP | NAT | AVC/DNS | Internet | App Perf | IP1 | IP2

Route

Map Name	map1
Priority in Map (ACL)	20008 (ACL: 1210)
Overlay	RealTime
Configured Tx Action	Passthrough_Cox_RealTime
Tx Action	Passthrough_Cox_RealTime
Rx Action	Passthrough_Cox_RealTime
Tx Reason	primary
Application	Https (port-protocol)
Application Group	Encrypted,Network_Services
Traffic Category	Video_Streaming
Protocol	tcp
Using Stale Map Entry	No
Flow Direction	Outbound
Ingress interface	lan0
Egress interface	wan1
Flow Redirected From	
Auto-opt Transit Node	
LAN-side VLAN	None
Subnet	0.0.0.0/0 (50) (Non-Local)
Internet flow	Yes
WAN routing	Passthrough_Cox_RealTime (nexthop_72.203.224.0_wan1-40904100205 2023)
LAN routing	nexthop_10.3.204.46_lan0-1949381408052023

Stats

Outbound Ratio	1.00
Inbound Ratio	1.00
Outbound LAN bytes	7,065,454
Outbound WAN bytes	7,065,454
Inbound LAN bytes	2,306,161,758
Inbound WAN bytes	2,306,161,758
Outbound LAN pkts	128,801
Outbound WAN pkts	128,801
Inbound LAN pkts	1,548,035
Inbound WAN pkts	1,548,035
Inbound WAN lost	0
Inbound WAN average jitter	0.00 milli sec
Flow Up Time	27m 59.843s
Flow ID	161422
Active	Yes
TCP Flow Context	161422
Is Flow Queued For Reset	No
Web Proxy Detected	No
Source IP	10.0.62.254
Dest IP	34.104.32.36
Last Policy Change	4838672302
Last Policy Lookup	4842679784

Start Time...	Uptime	Overlay	User Name...	Protoc...	Application	IP1	Port1	IP2	Port2	*Inbound Bytes*	Outbound B...	Inbound Tunn...	Outbound Tu...	User...	Role...
09:14:15	7m 3s	RealTime	N/A	tcp	Https	10.0.62.254	55582	prod.gccru...	443	620M	2.0M	Passthrough_...	Passthrough...		
10-Aug-23...	48d 19h ...	CSOTunnel	N/A	gre	Gre	10.73.73.12	0	192.168.13...	0	600M		to_CSO-West...	to_CSO-West...		
08:58:18	23m	DefaultOverl...	N/A	udp	Youtube	10.0.60.237	58891	rr4---sn-a5...	443	398M	2.5M	Passthrough_...	Passthrough...		
10-Aug-23...	48d 19h ...	CSOTunnel	N/A	gre	Gre	10.3.200.2	0	192.168.13...	0	530M		to_CSO-West...	to_CSO-West...		
27-Sept-2...	15h 38m...	AZURE_Test	N/A	udp	Ipsec-nat-trave...	192.168.23.2	4500	52.245.235...	4500	337M	3	Passthrough_...	Passthrough...		
09:11:33	5m 22s	DefaultOverl...	N/A	tcp	Netflix	10.0.56.127	41534	ipv6-c003-...	443	314M	3.8M	Passthrough_...	Passthrough...		
09:14:58	2m 57s	DefaultOverl...	N/A	tcp	Netflix	10.0.56.127	59916	ipv6-c002-...	443	184M	2.1M	Passthrough_...	Passthrough...		
09:15:31	5m 47s	RealTime	N/A	tcp	Https	10.0.63.108	52406	edge-041.u...	443	180M	3.4M	Passthrough_...	Passthrough...		

HPE aruba networking

RESILIENCY

Inbound Pre-POC Out Of Order	**15.5 %**
Inbound Post-POC Out Of Order	**3.8 %**
Outbound Pre-POC Out Of Order	**7.82 %**
Outbound Post-POC Out Of Order	**0.12 %**

Out of Order Packets

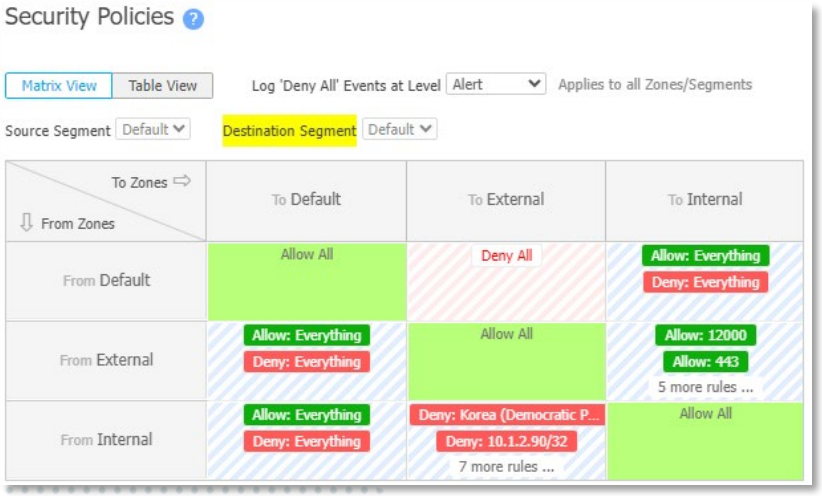
Pre-POC Out Of Order Post-POC Out Of Order

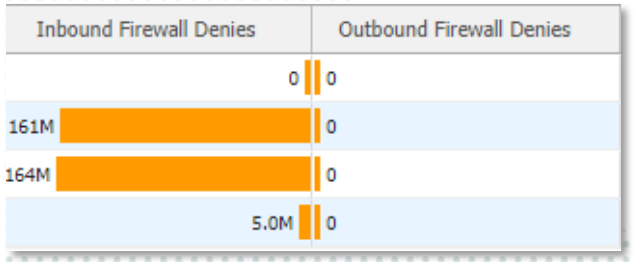
8 Rows Search

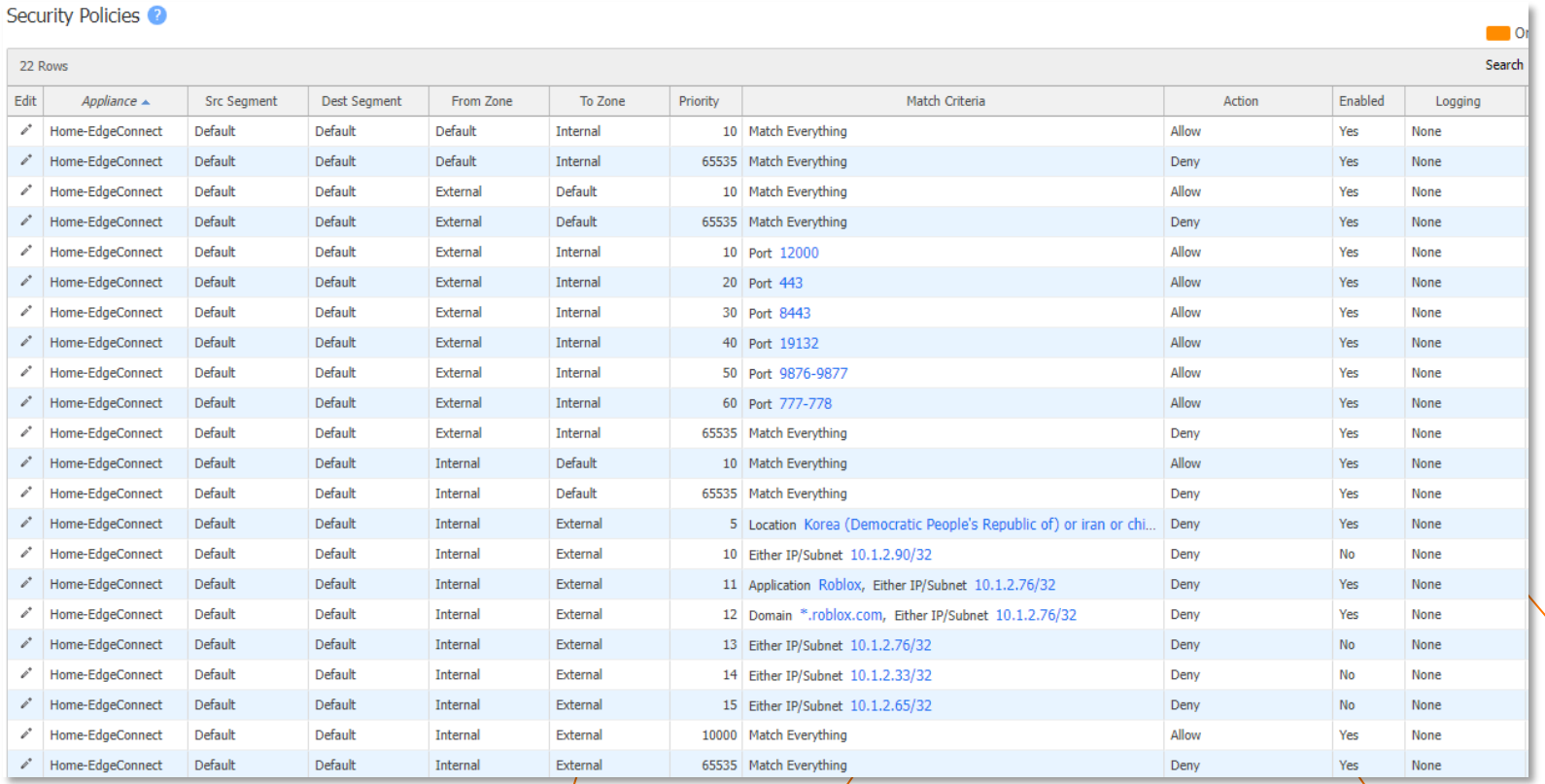
Appliance	Tunnel	<-- Avg Out Of Order %	Avg Out Of Order % -->	Remote Tunnel	Remote Appliance
Abe-EC	to_CSO-West_CSOTunnel	23	0.01 9.04	to_Abe-EC_CSOTunnel	CSO-West
Abe-EC	to_CSO-West_RealTime	15.5 3.8	0.12 7.82	to_Abe-EC_RealTime	CSO-West
Abe-EC	to_CSO-West_DefaultOverlay	13.2 1.5	0.29 14.88	to_Abe-EC_DefaultOverlay	CSO-West
Abe-EC	to_Chet-East_CriticalApps	1.1	1.13	to_Abe-EC_CriticalApps	Chet-East
Abe-EC	to_Chet-East_BulkApps	0	0	to_Abe-EC_BulkApps	Chet-East
Abe-EC	to_Chet-East_DefaultOverlay	0	0	to_Abe-EC_DefaultOverlay	Chet-East
Abe-EC	to_CSO-West_BulkApps	0	0 14.59	to_Abe-EC_BulkApps	CSO-West
Abe-EC	to_CSO-West_CriticalApps	0	1.32 25.57	to_Abe-EC_CriticalApps	CSO-West

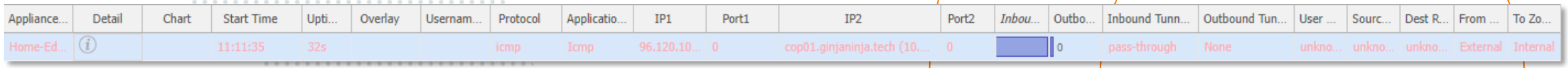
HPE aruba networking

SECURITY POLICIES – FIREWALL









SECURITY - IDS

Status	IDS/IPS State	Profile	Eligible	Licensed	Signature Version	Inspected pkts/sec (l...	Threats detected (last...	IPS Flow Drops (Cum...	Events	Stats
Protecting Traffic	IPS Enabled	Default	Yes	Yes	10421	0	0	0		

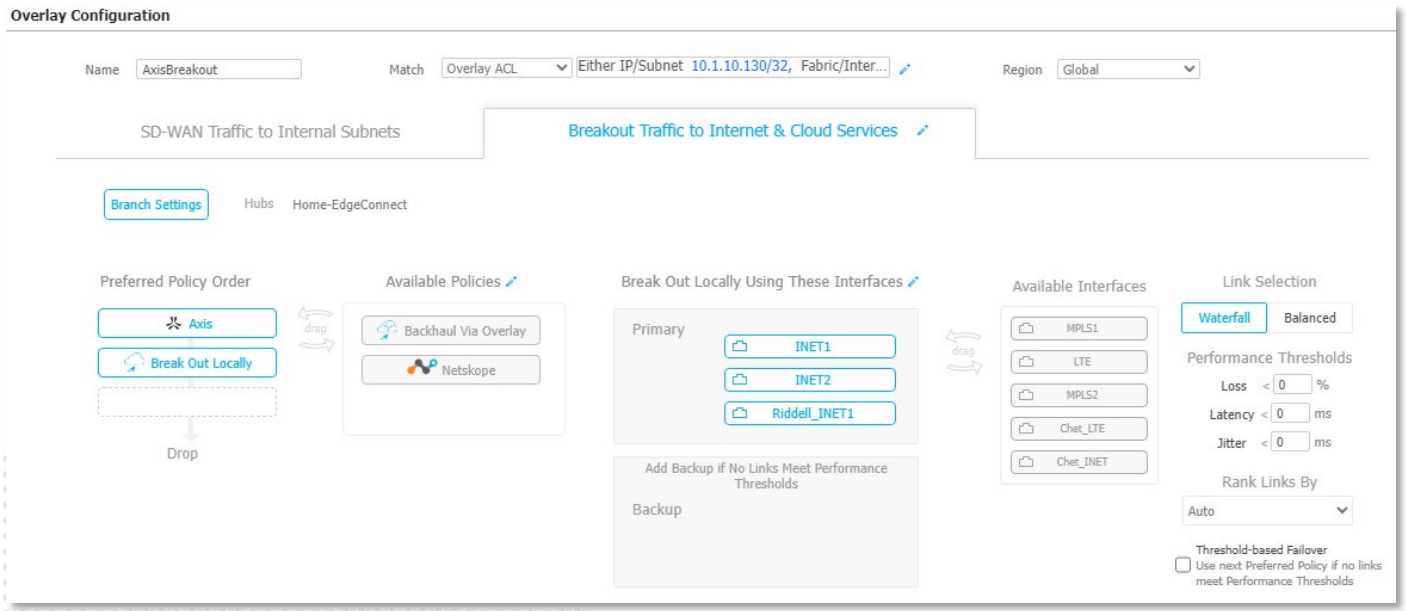
101 Rows

Search

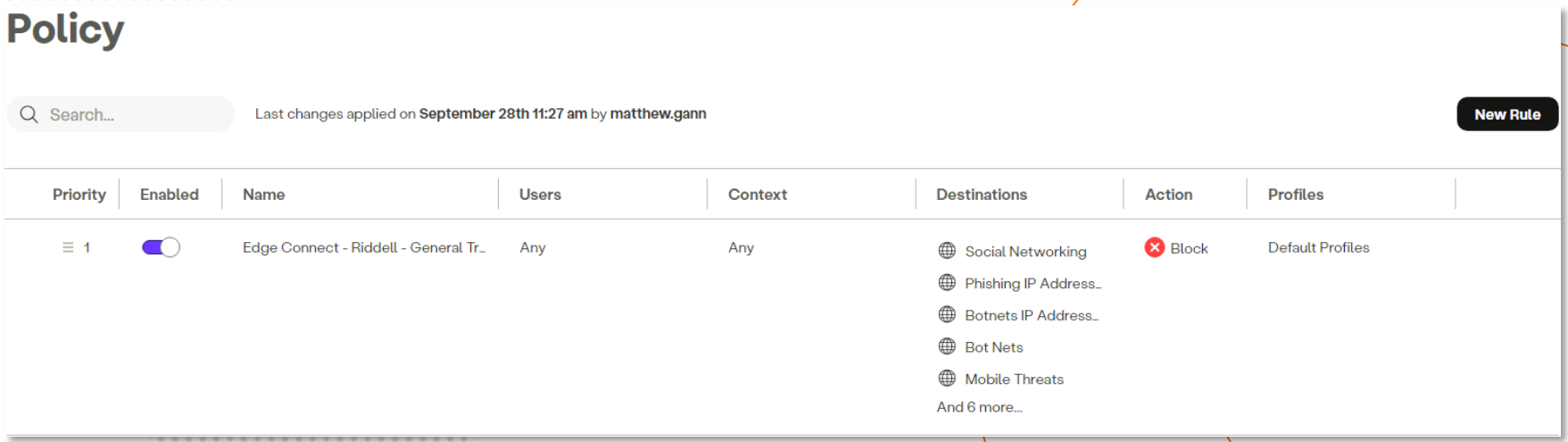
Date	Rule ID	Message
Jul 3 09:47:17 2023	1:2027758:3	ET DNS Query for .cc TLD [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 10.1.6.69:52320 -> 1.1.1.1:53
Jul 3 09:46:44 2023	1:2027758:3	ET DNS Query for .cc TLD [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 10.1.6.69:53535 -> 8.8.8.8:53
Jul 3 09:46:48 2023	1:2027758:3	ET DNS Query for .cc TLD [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 10.1.6.69:53535 -> 208.67.222.222:53
Jul 3 09:46:41 2023	1:2027758:3	ET DNS Query for .cc TLD [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 10.1.6.69:53535 -> 1.1.1.1:53
Jul 3 09:46:08 2023	1:2027758:3	ET DNS Query for .cc TLD [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 10.1.6.69:52127 -> 8.8.8.8:53
Jul 3 09:46:12 2023	1:2027758:3	ET DNS Query for .cc TLD [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 10.1.6.69:52127 -> 208.67.222.222:53
Jul 3 09:46:05 2023	1:2027758:3	ET DNS Query for .cc TLD [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 10.1.6.69:52127 -> 1.1.1.1:53
Jul 3 09:45:37 2023	1:2016150:3	ET INFO Session Traversal Utilities for NAT (STUN Binding Response) [Classification: Misc activity] [Priority: 3] {UDP} 52.115.223.157:3478 -> 10.1...
Jul 3 09:45:36 2023	1:2027758:3	ET DNS Query for .cc TLD [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 10.1.6.69:51592 -> 8.8.8.8:53
Jul 3 09:45:32 2023	1:2027758:3	ET DNS Query for .cc TLD [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 10.1.6.69:51592 -> 208.67.220.220:53
Jul 3 09:45:32 2023	1:2016150:3	ET INFO Session Traversal Utilities for NAT (STUN Binding Response) [Classification: Misc activity] [Priority: 3] {UDP} 52.115.223.157:3478 -> 10.1...
Jul 3 09:45:31 2023	1:2016150:3	ET INFO Session Traversal Utilities for NAT (STUN Binding Response) [Classification: Misc activity] [Priority: 3] {UDP} 52.115.223.157:3478 -> 10.1...
Jul 3 09:45:29 2023	1:2027758:3	ET DNS Query for .cc TLD [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 10.1.6.69:51592 -> 1.1.1.1:53
Jul 3 09:45:00 2023	1:2027758:3	ET DNS Query for .cc TLD [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 10.1.6.69:51446 -> 8.8.8.8:53
Jul 3 09:45:01 2023	1:2016150:3	ET INFO Session Traversal Utilities for NAT (STUN Binding Response) [Classification: Misc activity] [Priority: 3] {UDP} 52.115.223.157:3478 -> 10.1...
Jul 3 09:44:56 2023	1:2016150:3	ET INFO Session Traversal Utilities for NAT (STUN Binding Response) [Classification: Misc activity] [Priority: 3] {UDP} 52.115.223.157:3478 -> 10.1...
Jul 3 09:44:56 2023	1:2027758:3	ET DNS Query for .cc TLD [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 10.1.6.69:51446 -> 208.67.220.220:53
Jul 3 09:44:53 2023	1:2016150:3	ET INFO Session Traversal Utilities for NAT (STUN Binding Response) [Classification: Misc activity] [Priority: 3] {UDP} 52.115.223.157:3478 -> 10.1...
Jul 3 09:44:53 2023	1:2027758:3	ET DNS Query for .cc TLD [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 10.1.6.69:51446 -> 1.1.1.1:53
Jul 3 09:44:52 2023	1:2016150:3	ET INFO Session Traversal Utilities for NAT (STUN Binding Response) [Classification: Misc activity] [Priority: 3] {UDP} 52.115.223.157:3478 -> 10.1...
Jul 3 09:44:21 2023	1:2027758:3	ET DNS Query for .cc TLD [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 10.1.6.69:53177 -> 8.8.4.4:53
Jul 3 09:44:25 2023	1:2027758:3	ET DNS Query for .cc TLD [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 10.1.6.69:53177 -> 208.67.220.220:53

HPE aruba networking

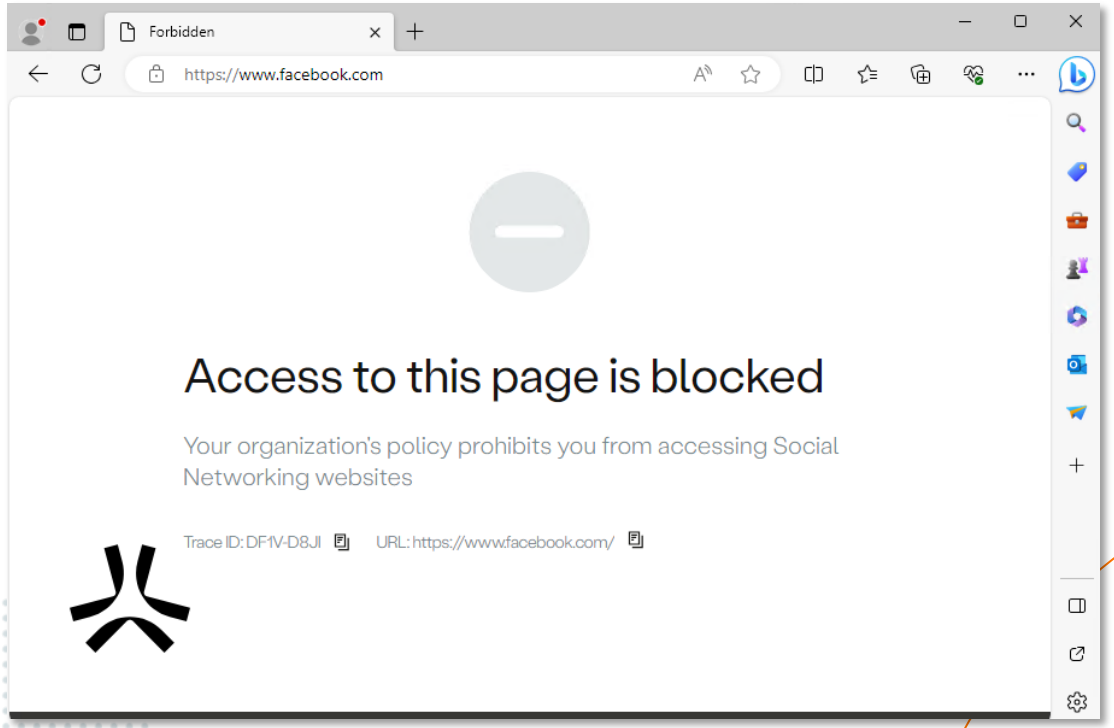
SECURITY – SECURE WEB GATEWAY (SWG)

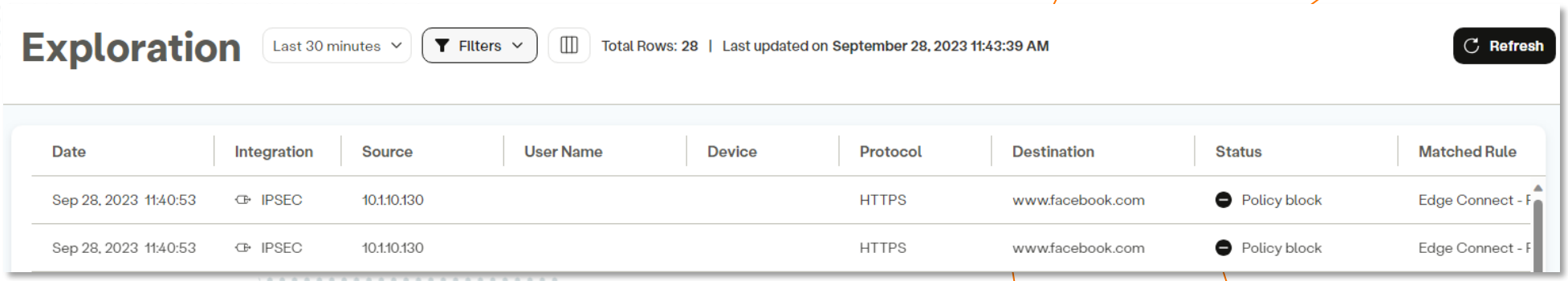


Primary Tunnel Remote Identifier	Connection Status
ipsec-geo.axisapps.io	Up - Active
ipsec-geo-secondary.axisapps.io	Up - Active



SECURITY – SECURE WEB GATEWAY (SWG)





HPE ARUBA NETWORKING SSE SOLUTION

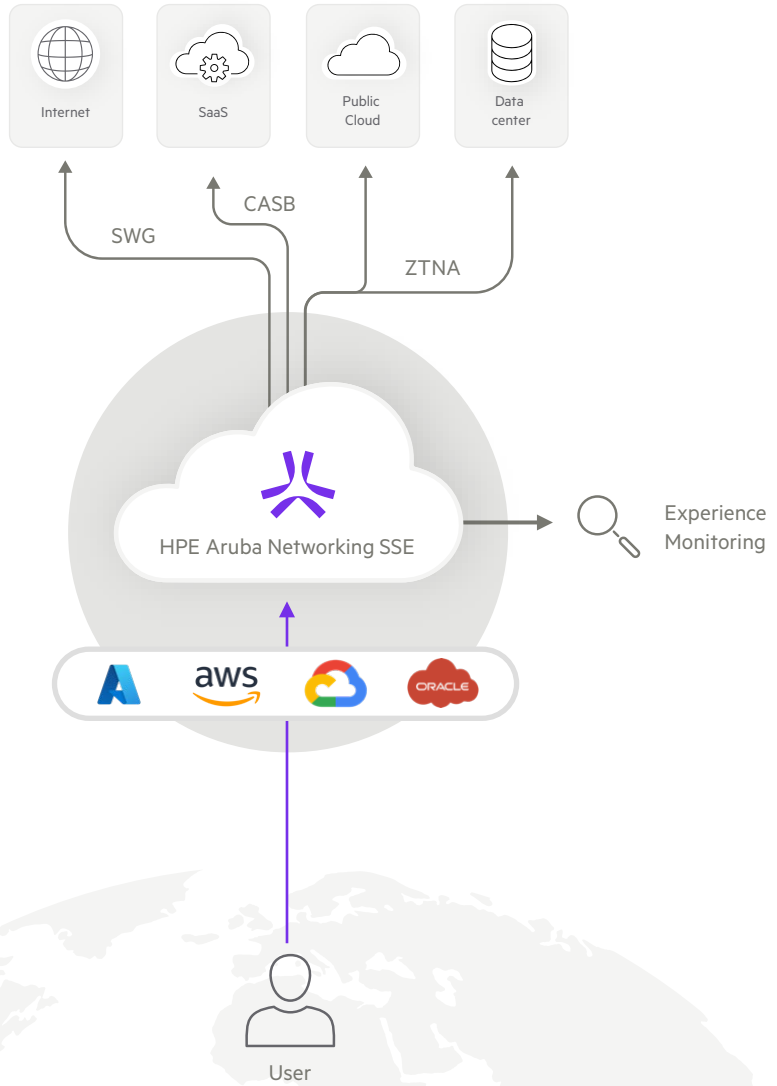
What's So Different About HPE Aruba Networking SSE

Focus is on unification of capability. One UI, one policy, one platform (ZTNA, SWG, CASB, DEM)

Goal is to **simplify policy & inspect any traffic** for Internet, SaaS, and legacy apps (SSH, RDP, VOIP, AS400, ICMP etc.)

Ability to **harmonize access across the world** via smart routing and a cloud-backbone on AWS, Azure, Google, and Oracle

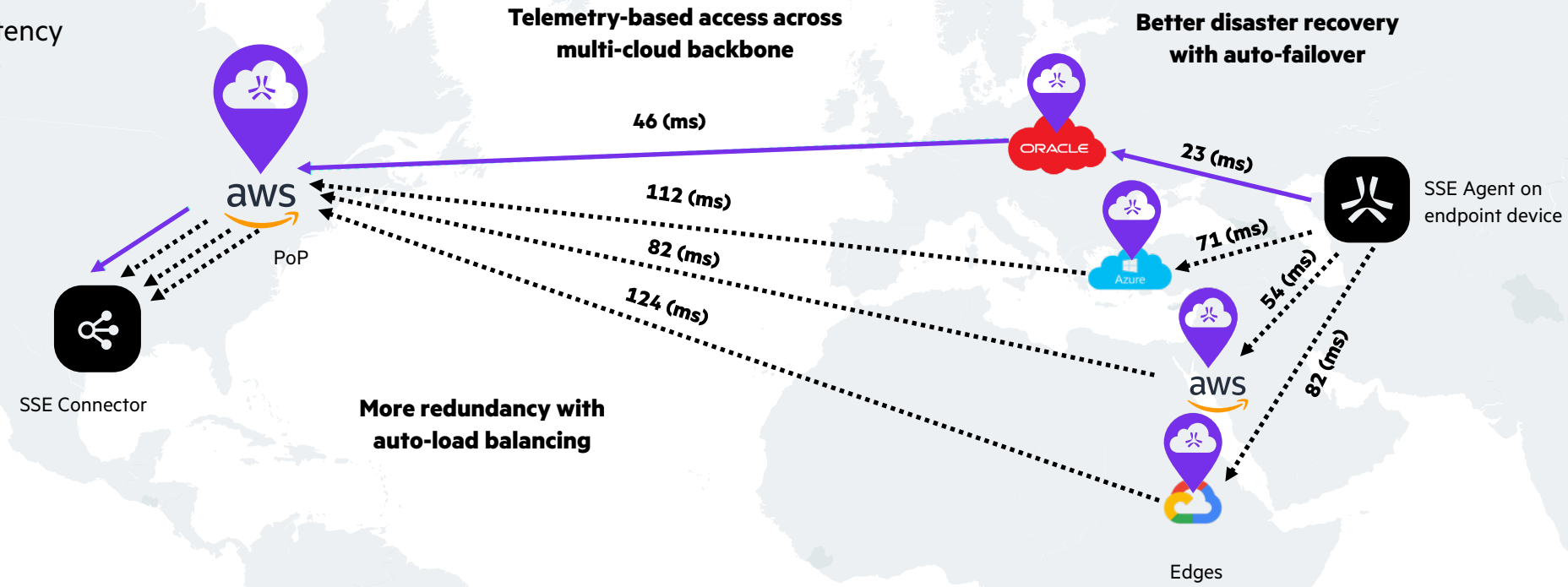
Purposely designed to enable users to access resources **with or without an agent**



Cloud-Backbone for Hyper-Resiliency and Speed During Remote Work

Network-as-a-Service

- Geo-proximity routing
- Smart routing based on latency
- Extremely high availability



HPE ARUBA NETWORKING SSE KEY CAPABILITIES

ZTNA
(Zero Trust Network Access)

Secure access to web apps

Least privilege access

Agent or agentless

VPN replacement

CASB
(Cloud Access Security Broker)

Mediates connectivity to SaaS applications

Ensures sensitive Data remains protected

Reduces the opportunity for cyber attack

SWG
(Secure Web Gateway)

Protects against malicious web traffic

SSL Inspection, URL filtering, sandboxing, malware scanning, DNS filtering

DEM
(Digital Experience Monitoring)

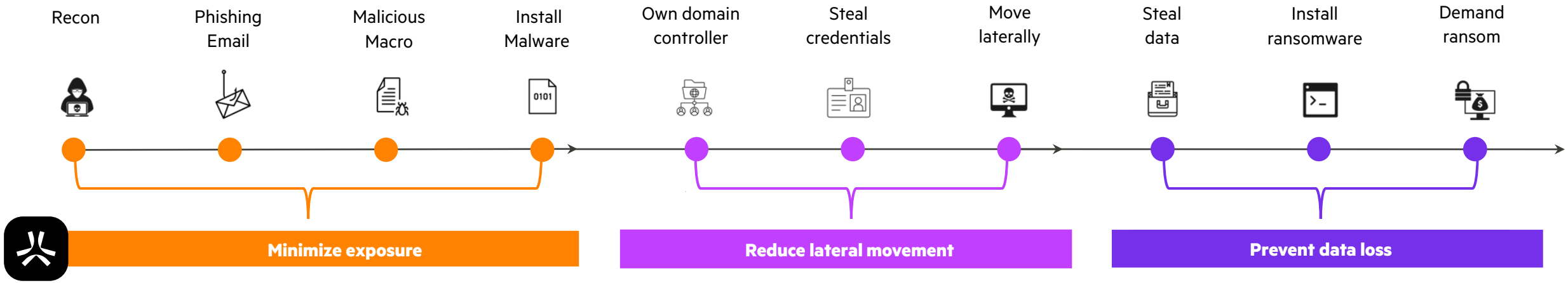
Ensure user productivity by measuring hop-by-hop metrics

Monitor app and network performance

Visibility into End User Devices

DISRUPT THE CYBER KILL CHAIN WITH ZTNA, SWG, AND CASB COMBINED

71% of orgs worldwide were affected by **ransomware** in 2022



Eliminate the attack surface
Prevent applications from being discovered by placing them behind HPE Aruba Networking SSE – RDP protected, no VPN

Inline content inspection
Content inspection for visibility into user activity and for threat detection

Least-privileged user access
Securely connect authorized users to specific apps, without placing them on the corporate network - no ACLs needed

Server-to-Server segmentation
Enable least privilege server-to-server communications to protect networks from ransomware

DLP for Traffic
Inline controls enforce disable download, copy & paste etc. policies for users and servers

Visibility into malicious activity
View employee and third-party user activity, file downloads, protocols used, and SSH commands

Unified SASE Benefits

STREAMLINE SASE DEPLOYMENT WITH CONSOLIDATED NETWORKING AND SECURITY

HPE aruba networking

Unified SASE

EDGECONNECT SD-WAN + **HPE ARUBA NETWORKING SSE**

Unified Security Posture

Apply universal security policies and centralized access controls **across all traffic and locations**

Reduced Complexity

Streamline network and security management and deployment

Eliminate the need for multiple point solutions and hardware appliances

Optimized User Experience

Guarantee a secure, high-performance, low-latency connection to applications and resources

Reduce the need for backhauling traffic to the data center

HPE aruba networking

Thank You

Questions and Answers