

atmosphere'23

BELGIUM



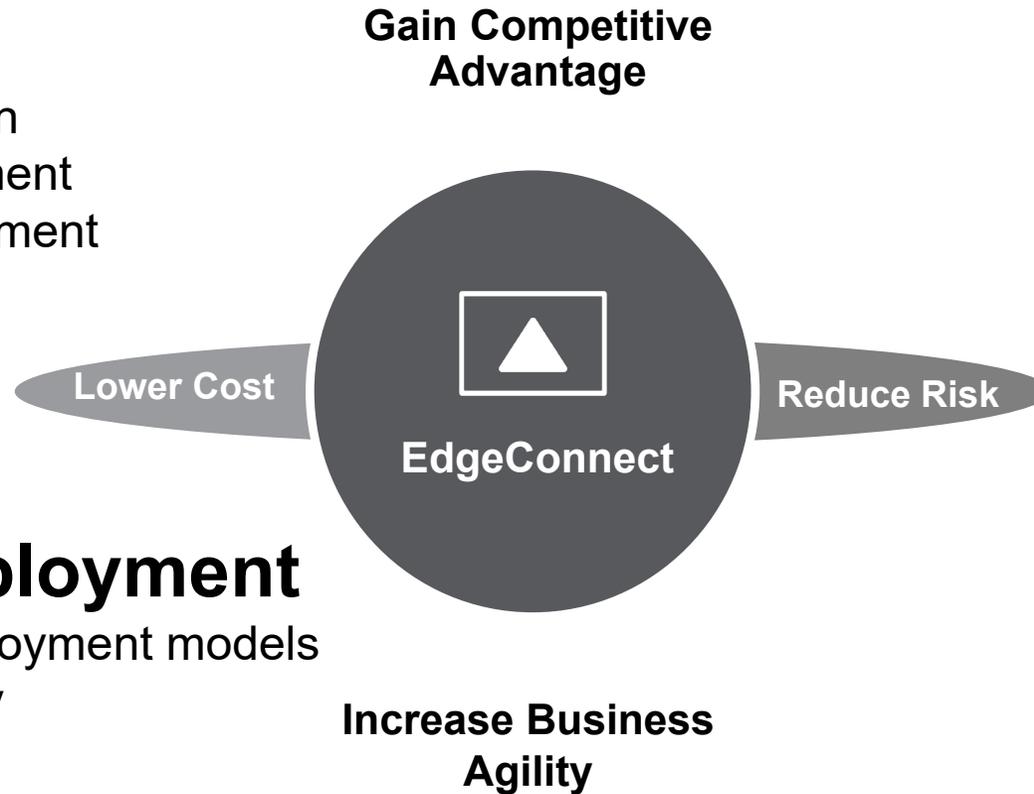
Building a secure Edge

Jan-Willem Keinke
Sales Engineer SASE Benelux
Email: jwk@hpe.com

ADVANTAGES OF AN APPLICATION DRIVEN WAN

Savings

- WAN cost savings
- Automation savings
- Cloud security integration
- Eliminate branch equipment
- Simplified edge management



100x Faster Deployment

- Simple and flexible deployment models
- Comprehensive visibility

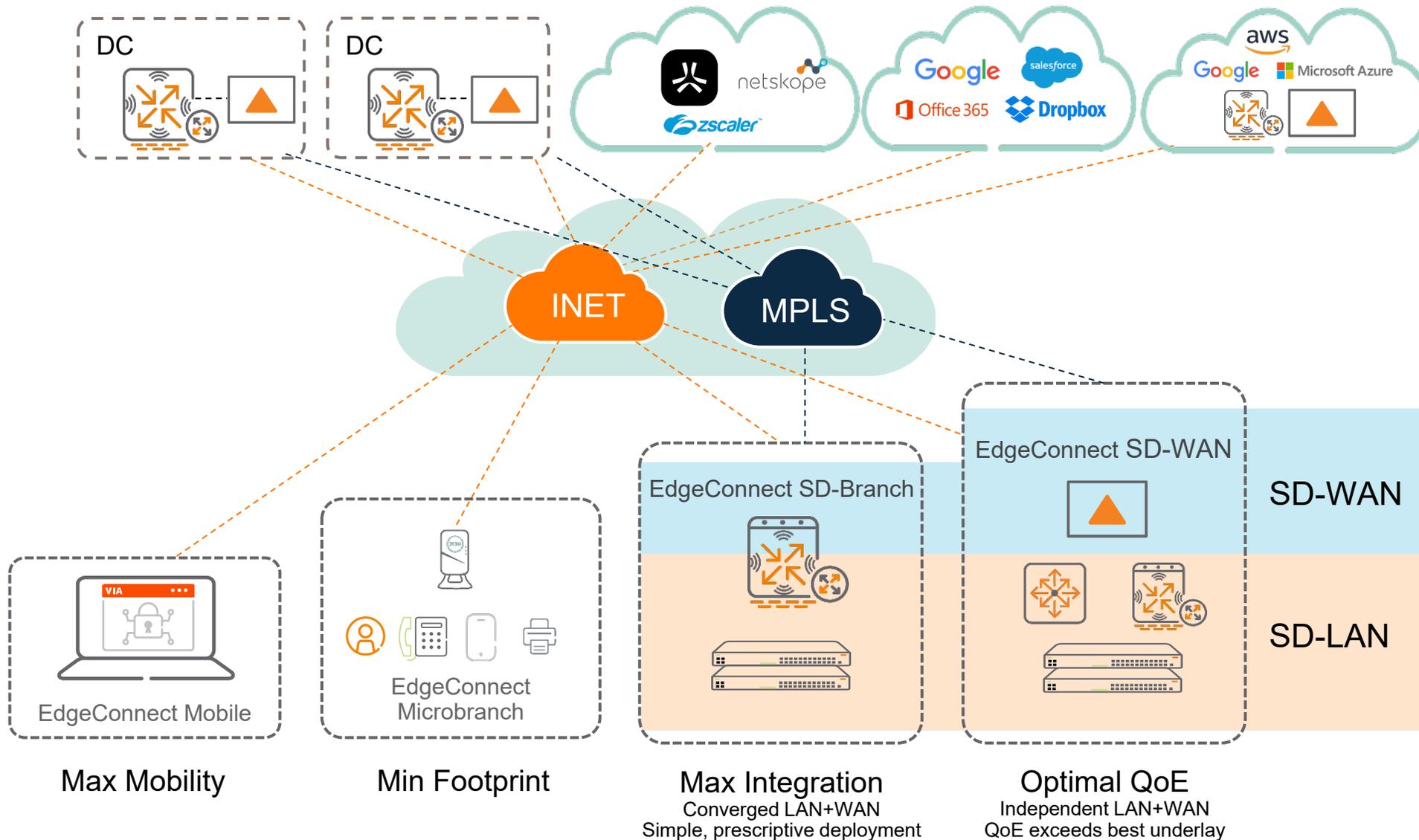
Performance

- Sub second session failover
- 10 x faster applications
- Performance Improvement for SaaS/IaaS
- Add / remove branches instantly
- Uptime during blackouts

Security

- Segment your apps
- Automated policies
- UTM features
- ZBF within VRFs
- Cloud Security Integration

HPE Aruba's secure edge portfolio



Integration opportunities

Converged management

Aruba Central
w/ EdgeConnect site view

Silver Peak Orchestrator
w/Aruba WAN view

Cross portfolio security

Clear Pass: Role based policy

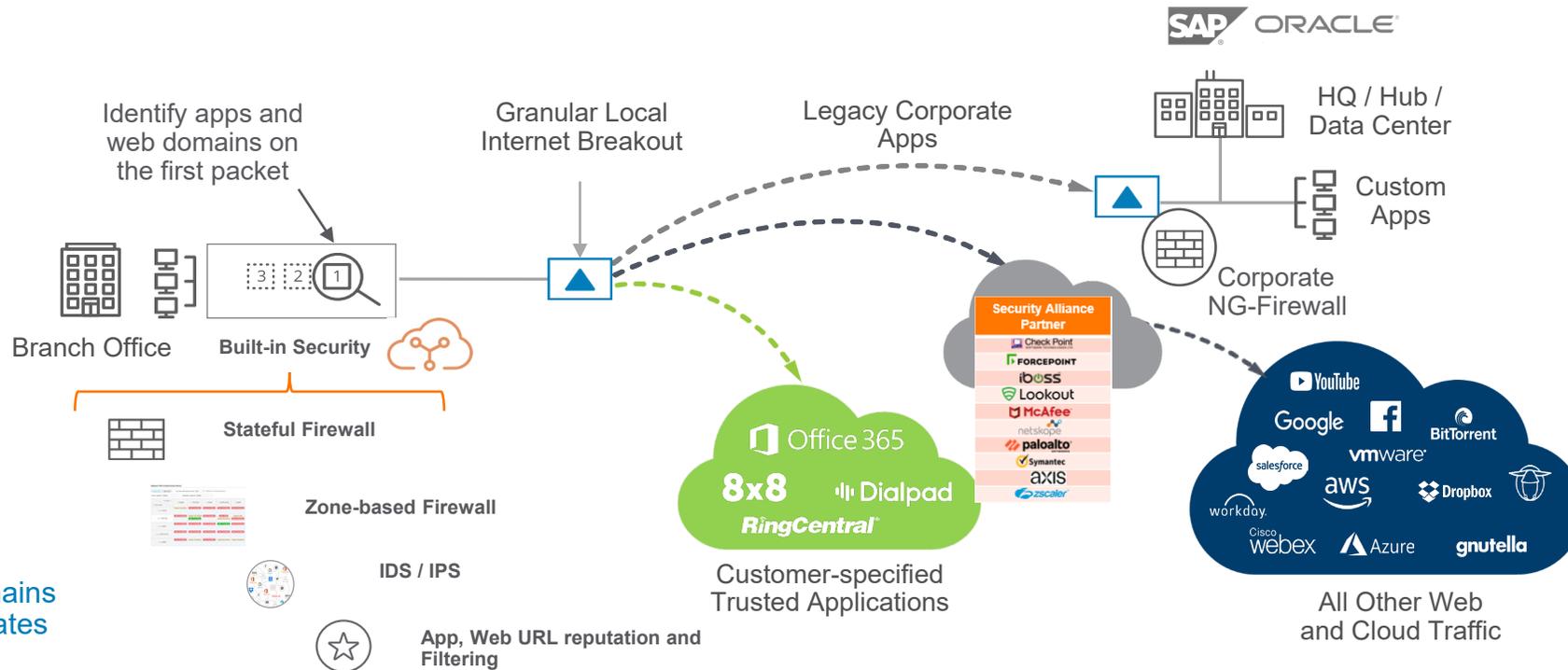
Dynamic segmentation

Unified threat management

Cloud security partners

Secure, adaptive internet breakout

– First-packet iQ™ enables application visibility and control



10,000+ Apps
300 Million+ Web Domains
Automated Daily Updates

Steer Apps Intelligently

Granular, intelligent breakout of SaaS and trusted internet-bound traffic directly from the branch

Improve App Response Time

Avoid added latency through direct access to where the app resides

Reduce Backhaul

Backhaul only untrusted traffic to corporate FW

Save Valuable WAN Bandwidth

Avoid consumption of expensive MPLS circuits where not necessary

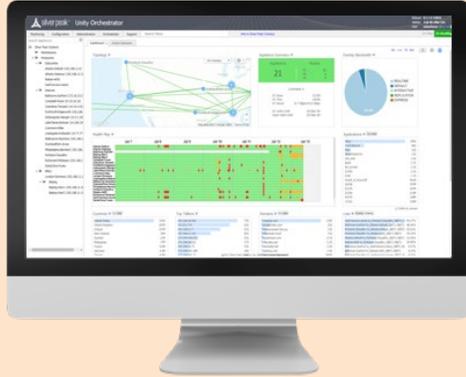


EdgeConnect Orchestrator

Your SD-WAN control center



What is EdgeConnect Orchestrator?



EdgeConnect Orchestrator

Orchestrate application policies across thousands of appliances, through a single pane of glass, driven by simple business intent policies.

Align **application policies** (QoS, security) with **business intent**

Secure, centralized visibility, control and administration of SD-WAN across thousands of sites

Extensive analytics, application & network performance measurements, & troubleshooting.

Automates & simplifies lifecycle management of SD-WAN

Orchestrates **end-to-end service chains** through partner APIs.

Business Intent Based Overlays

Dashboard		Zscaler Internet Access		Business Intent Overlays ×				
Business Intent Overlays ?								
Apply Overlays Regions Hubs View Overlay Stats Interface Labels								
Priority	Overlay	Region	Topology	Primary Interfaces	Backup Interfaces	Policy Order	Primary Interfaces	Backup Interfaces
1	GUEST Match Traffic GUEST	Global Regions ▶	Regional Hub & Spoke 	<i>High Quality</i> Waterfall: Overall Quality		1 Zscaler Cloud 2 Break out	INETA INETB INETC <i>Waterfall: Fixed Order</i>	
2	REALTIME Match Traffic REALTIME	Global Regions ▶	Regional Hub & Spoke 	1 TRANSIT1 2 INETA 2 INETB 2 INETC 6 INETA v6 6 INETB v6 <i>High Availability</i> Waterfall: Overall Quality	2 LTEA 2 LTEB 2 SAT1 If Pri & Sec Down	Branch CENTRAL1-Azure 1 Backhaul 2 Break out	INETA INETB INETC <i>Waterfall: MOS</i>	
3	BATCH Match Traffic BESTEFFORT	Global Regions ▶	Regional Hub & Spoke 	2 INETA 2 INETB 2 INETC <i>High Quality</i> Waterfall: Overall Quality	2 LTEA 2 LTEB 2 SAT1 If Pri & Sec Down	Branch CENTRAL1-Azure 1 Prisma 2 Backhaul 3 Break out	INETA INETB INETC <i>Balanced</i>	
4	RECREATIONAL Match Traffic RECREATIONAL	Global Regions ▶	Regional Hub & Spoke 	2 INETA 2 INETB 2 INETC <i>High Quality</i> Waterfall: Overall Quality	2 LTEA 2 LTEB 2 SAT1 If Pri & Sec Down	Branch CENTRAL1-Azure 1 Break out 2 Backhaul	INETA INETB INETC <i>Waterfall: Auto</i>	
5	BUSINESS Match Traffic BUSINESS	Global Regions ▶	Regional Hub & Spoke 	1 TRANSIT1 2 INETB 2 INETA 2 INETC 6 INETA v6 6 INETB v6 <i>High Quality</i> Waterfall: Overall Quality	2 LTEA 2 LTEB 2 SAT1 If Pri & Sec Down	Branch CENTRAL1-Azure 1 Break out 2 Backhaul 3 Zscaler Cloud	INETA INETB INETC <i>Waterfall: Auto</i>	

Search tags, appliances

- 84 Appliances
- 6 -- HUB -- 13
- 1 -- APJ & AUS -- 4
- 4 -- EMEA -- 9
 - Hamburg-Pady
 - Ripponden-Collier
 - Edinburgh-Moir 2
 - Edinburgh1-Moir
 - Edinburgh2-Moir
 - Pamplin 3
 - Dublin-Pamplin
 - Sussex2-Pamplin
 - WRH-TEST-Pamplin2
 - Reading-Cook 2
 - Reading1-Cook
 - Reading2-Cook
- 1 -- US CENTRAL -- 20
- 1 -- US EAST -- 25
- 1 -- US WEST -- 12
- MAINTENANCE 1
 - silverpeak 123708
- OFFLINE 0

Dashboard Business Intent Overlays Access Lists Flows Topology

Appliance Licenses

Appliances		Models	
84		EC-XS	28
		EC-V	42
		EC-US	14

EC Licenses			
Base	39/50	1 Gbps	3/100
Plus	13/50	2 Gbps	3/100
50 Mbps	7/100	Unlimited	5/110
200 Mbps	17/100	Boost	56.1% of 10.0 Gbps
500 Mbps	10/100		

Valid Until	
EC	01-Aug-23 08:00
EC Boost	01-Aug-23 08:00

Topology



Overlay Bandwidth



Top Talkers

10.100.0.199 Default	41G
192.168.14.24 Default	41G
10.41.71.253 Default	3.4G
192.168.11.85 Default	2.9G
10.50.21.245 Default	1.4G
192.168.11.167 Default	1.2G
192.168.11.120 Default	1.1G
14.73.173.170 Default	1.1G
40.97.120.66 Default	951M
192.168.17.7 Default	937M
192.168.23.102 Powers	937M
89.164.9.116 Default	929M
52.96.91.66 Default	814M
14.153.79.12 Default	769M
192.168.23.106 Powers	715M

Domains

ffivetuple.net	51G
fdropcam.com	5.8G
fgooglevideo.com	3.0G
ffoffice365.com	2.2G
falv-cdn.net	929M
fsilverpeak.cloud	559M
fgvtL.com	355M
fscalerthree.net	345M
*akamaihd.net	269M
*microsoft.com	237M
*yimg.com	164M
*nai.com	152M
*windows.net	80M
*cloudfront.net	65M
dns.google	60M

Applications

Clk_Lamb	41G
Next_AwareVideo	5.8G
YouTube	3.6G
Office365Exchange	2.2G
Synlog	1.4G
Https	1.3G
Rtp	941M
Emp	938M
Netflow	872M
udp:11131	856M
PingPlotter-icmp	525M
SilverPeakOrch	423M
Akamaihd	269M
Http	239M
others	2.0G

Countries

United States	16G
United Kingdom	235M
Singapore	84M
Japan	42M
Germany	21M
Hong Kong	16M
Australia	12M
Netherlands	11M
Canada	6.5M
Denmark	2.2M
France	1.4M
Belgium	1.2M
Ireland	430K
Taiwan Province of China	63K
India	48K

Health Map



Ports

445 TCP (Microsoft-ds)	41G
61609 TCP	24G
61649 TCP	17G
443 TCP (Https)	11G
0 ICMP	4.4G
443 UDP (Https)	2.8G
514 UDP (Syslog)	2.8G
11131 UDP	1.6G
61660 TCP	1.1G
554 TCP (Rtp)	941M
51905 TCP	937M
2055 UDP (Netflow)	783M
89143 TCP	719M

Security policy matrix

Security Policies ?

Matrix View Table View

Merge Replace

To Zones ⇄ From Zones ↓	To Default	To POS	To WAN	To Guest_Wifi	To InternetBreakout	To Business_Overlay
From Default	Allow All	Allow: Everything Deny: Everything	Allow: Everything Deny: Everything	Allow: Everything	Allow: Everything Deny: Everything	Allow: Everything
From POS	Deny All	Allow All	Allow: Everything	Allow: ACL Printer Deny: Everything	Deny All	Allow: Everything
From WAN	Deny All	Deny: Vnc Allow: Everything	Allow All	Allow: Everything	Deny All	Deny All
From Guest_Wifi	Deny All	Deny All	Allow: Everything	Allow All	Deny: Social_Network Deny: Games 1 more rule ...	Deny All
From InternetBreakout	Deny All	Deny All	Deny All	Deny All	Allow All	Deny All
From Business_Overlay	Deny All	Allow: ACL_BusinessCritical Deny: Vnc	Deny All	Deny All	Deny All	Allow All

Edit Rules: Guest_Wifi to InternetBreakout ✕

Add Rule

4 Rows Search

Priority ▲	Match Criteria	Action	Enabled	Tag	Comment	
1001	Application group Social_Network	deny	<input checked="" type="checkbox"/>			✕
1002	Application group Games	deny	<input checked="" type="checkbox"/>			✕
1004	ACL Internet_Traffic	allow	<input checked="" type="checkbox"/>			✕
65535	Match Everything	deny	<input checked="" type="checkbox"/>			✕

EdgeConnect SD-WAN IDS Highlights

- Built-in signature-based intrusion detection
- Utilizes common Aruba UTM framework
 - Automated threat feeds (from Aruba Central)
 - Threat logging to centralized collector/SIEM
 - Threat logging to Central (future)
- Integrated with zone-based firewall enabling application-level selection for inspection
 - Allow, Deny, Allow & Inspect
 - e.g., “inspect all flows on Internet link”
- Add-on “Advanced Security” license

The screenshot displays the Aruba EdgeConnect SD-WAN management interface. At the top, there are navigation tabs: Dashboard, Security Policies, Routing Segmentation (VRF), and Intrusion Detection System. The main heading is "Intrusion Detection System". Below this, there are two buttons: "IDS Configuration" and "Enable IDS on Appliances".

A table titled "3 Rows" shows the configuration for three appliances:

Edit	Appliance	Status	Config File	Signatures	Schedule
	bkutty3-ecvb	Enabled	user_config.yaml	https://rules.emergingthreats.net/open/suricata-4.0/emerging.rules.zip	Every day at 8:59 starting 14-Dec-20 8:57 PST
	bkutty3-ecva	Enabled	user_config.yaml	https://rules.emergingthreats.net/open/suricata-4.0/emerging.rules.zip	Every day at 8:59 starting 14-Dec-20 8:57 PST
	bkutty3-ecvc	Enabled	user_config.yaml	https://rules.emergingthreats.net/open/suricata-4.0/emerging.rules.zip	Every day at 8:59 starting 14-Dec-20 8:57 PST

Below the table is a modal window titled "Segment (VRF) Firewall Zones Policies". It has tabs for "Matrix View" and "Table View". The "Log 'Deny All' Events at Level" is set to "Alert". It applies to all Zones/Segments. The "Source Segment" is set to "Default" and the "Destination Segment" is set to "Default".

The matrix shows the following policies:

To Zones	To Default	To TRUSTED	To GUEST	To UNTRUSTED	To MGMT
From Default	Inspect: Everything	Deny: Everything	Deny: Everything	Deny: Everything	Deny: Everything
From TRUSTED	Deny: Everything	Inspect: ACL Finance Allow: Everything	Deny: Everything	Deny: Adult Inspect: Everything	Inspect: icmp Deny: Everything
From GUEST	Deny: Everything	Deny: Everything	Deny: Everything	Allow: Everything	Deny: Everything
From UNTRUSTED	Deny: Everything	Deny: Everything	Deny: Everything	Deny: Everything	Deny: Everything
From MGMT	Deny: Everything	Inspect: Everything	Deny: Everything	Inspect: Everything	Inspect: Everything

At the bottom of the modal window are "Save" and "Cancel" buttons.

Summary: Benefits of SD-WAN

- Complete control and visibility of WAN infrastructure
- Route application traffic, not packets, based on:
 - Business importance
 - Security requirements
- Built in Firewall, end-to-end segmentation and IPS/IDS security
- Automated integration with Cloud infrastructures and Secure Service Edge providers

Best-of-breed SASE architecture

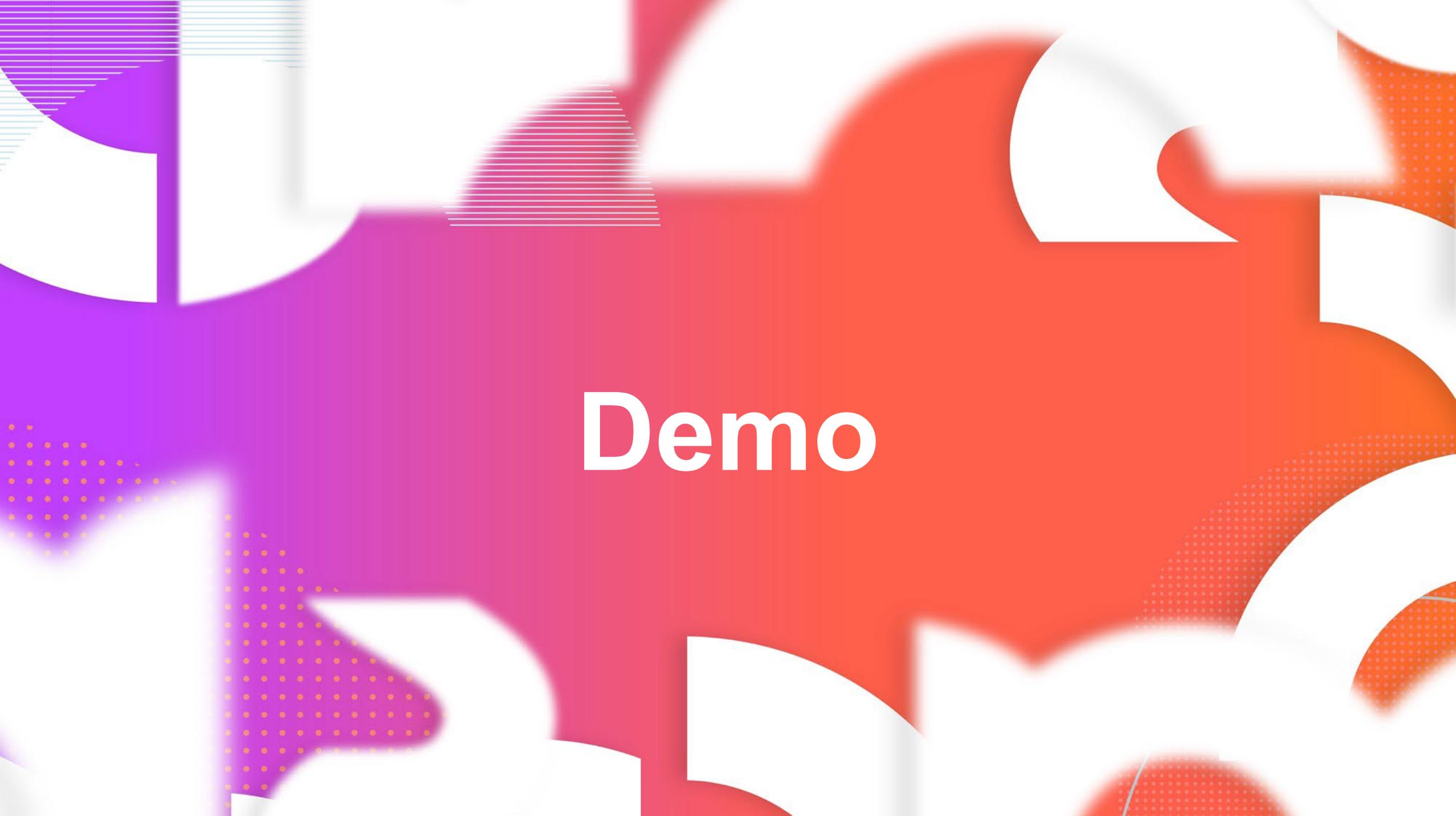
Secure SD-WAN

- SaaS Acceleration
- WAN Optimization
- Tunnel Bonding
- Zero-Touch Provisioning
- Data Encryption
- Next-generation Firewall
- Granular Segmentation
- IDS/IPS and DDoS Protection



Security Service Edge (SSE)

- Zero Trust Network Access
- Cloud Access Security Broker
- Secure Web Gateway
- Firewall as a Service
- Remote Browser Isolation
- Data Loss Prevention
- Sandboxing

The background features a complex, abstract design with overlapping organic shapes. The color palette includes vibrant purple, bright red, and warm orange. Some areas are filled with fine horizontal lines, while others have a dotted pattern. The overall effect is dynamic and modern.

Demo

Thank you.