Firewall „Następnej Generacji”

Chwyt marketingowy, czy jednak codzienność?

MBUM #6

Michal Zalewski
Sales Engineer, CEE
mzalewski@barracuda.com

Barracuda
Your journey, secured.

18 lat w branży IT

Od 2014 roku w obszarze Cyber/InfoSec

CEH/CEI/MTCNA/MTCRE/MTCSE/MTCUME/RHCE

Trener: EC-Council | HackerU | Barracuda

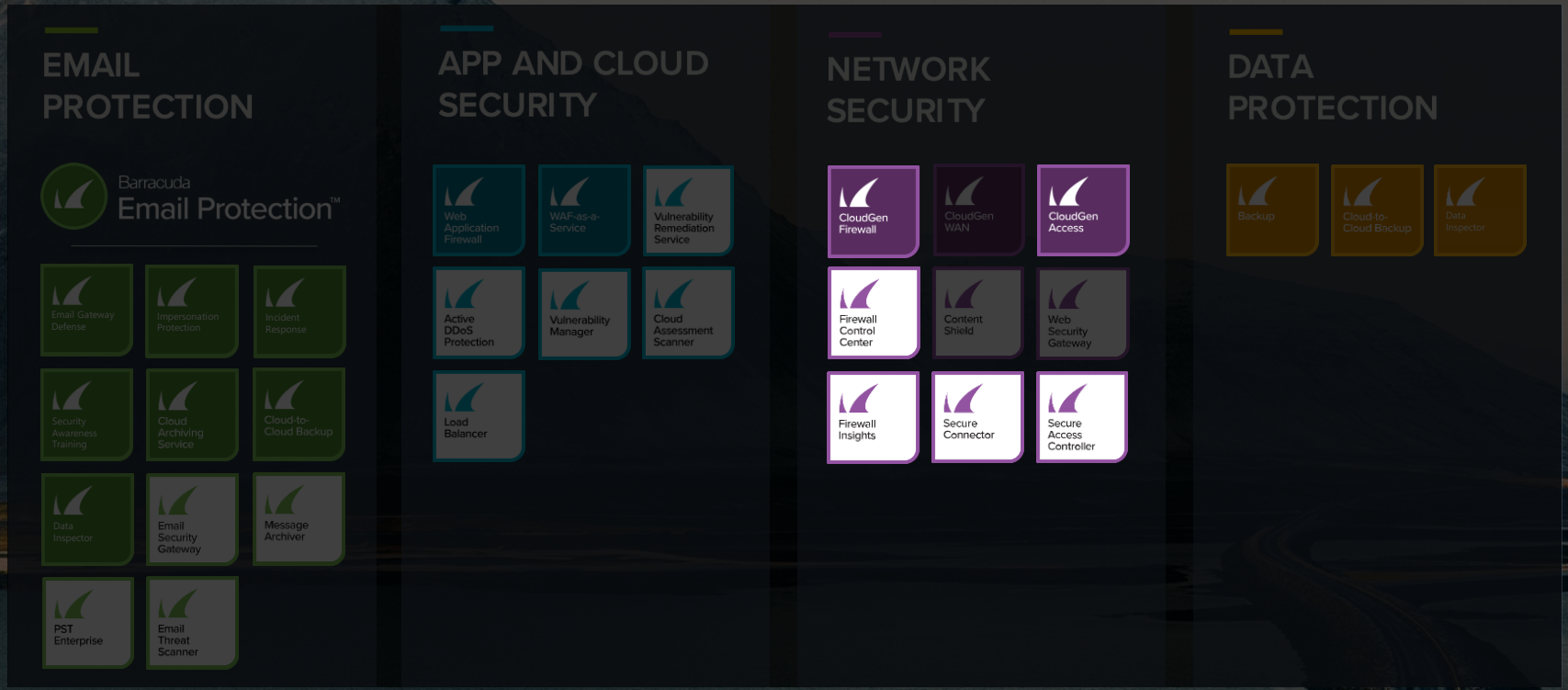
Obecnie: Sales Engineer CEE (17 krajów)

michal@zalewski.cloud

in/michal-a-zalewski


Barracuda protects the people, data, apps, and networks of more than 225,000 organizations worldwide by providing cloud-first security solutions that are easy to buy, deploy, and use

Network Security– portfolio



Krótka historia produktu CloudGen Firewall

Firewalle Barracuda w chmurach

2014

First Firewall with Microsoft Azure Certification

2015

Launch of Barracuda NextGen Firewalls

2016

Launch of first IoT/ICS Solutions

Microsoft Partner of the Year 2016

Adding Google Cloud Platform to the Cloud Portfolio

2017

First Firewall with AWS Security Competency

2018

Launch of Barracuda CloudGen Firewalls

Barracuda CloudGen Firewall

Bezpieczeństwo, dostęp, niezawodność w epoce chmury

Barracuda

Barracuda CloudGen Firewall – skąd pochodzi

Development and Engineering
Innsbruck, Austria
Vienna, Austria
Nottingham, United Kingdom

Manufacturing
San Jose, United States

Sales and Support
Worldwide

Datacenters
North America
Europe
Asia

Barracuda CloudGen Product Portfolio

Wide range of hardware appliances, ranging from 1.0 Gbps (F18) to 40 Gbps (F1000) firewall throughput. Various sub-models offer flexibility in terms of supported interfaces. Optional subscription allow the creation of tailor-made solutions.

CloudGen Firewall – urządzenia typu appliance

Samodzielne firewalle serii F:

- Zarządzanie uproszczone (za pomocą interfejsu Webowego)
- Zarządzanie pełne (za pomocą aplikacji GUI)
- Zarządzanie scentralizowane: z Control Center (maszyna wirtualna z systemem zarządzania)
- Modele F12, F18, F80, F180, F280, F380, F400, F600, F800, F900, F1000

CloudGen Firewall – urządzenia typu appliance

Urządzenia Secure Connetor:

- Zbieranie i tunelowanie ruchu do Access Controllera
- Zarządzane ze wspólnego z CGF Control Center
- Z możliwością uruchomienia własnego oprogramowania (kontener Linux LXC na mini-aplikację klienta)
- SC1, SC2 (wbudowany modem komórkowy, WiFi)

Flexible Deployment Options

Physical

- Hardware

Virtual

- Hyper-V
- VMware
- XEN
- KVM

Cloud

- Azure
- AWS
- GCP

Hardware – Entry level / branch offices

	F12	F18	F80	F82.DSLA	F82.DSLB	F180	F183	F183R	F280
Firewall throughput	1.2 Gbps	1.0 Gbps	1.5 Gbps	1.5 Gbps	1.5 Gbps	1.7 Gbps	2.0 Gbps	2.1 Gbps	3.7 Gbps
VPN throughput	220 Mbps	190 Mbps	240 Mbps	240 Mbps	240 Mbps	300 Mbps	300 Mbps	320 Mbps	1.1 Gbps
IPS throughput	400 Mbps	400 Mbps	400 Mbps	400 Mbps	400 Mbps	500 Mbps	580 Mbps	790 Mbps	1.2 Gbps
NGFW throughput	250 Mbps	340 Mbps	400 Mbps	400 Mbps	400 Mbps	550 Mbps	700 Mbps	800 Mbps	1.0 Gbps
Threat Prot. throughput	230 Mbps	320 Mbps	380 Mbps	380 Mbps	380 Mbps	480 Mbps	600 Mbps	700 Mbps	900 Mbps
Concurrent sessions	80,000	80,000	80,000	80,000	80,000	100,000	100,000	100,000	250,000
New sessions per sec.	8,000	8,000	8,000	8,000	8,000	9,000	9,000	9,000	10,000
Form factor	Desktop	Desktop	Desktop	Desktop	Desktop	Desktop	Desktop	Compact	Desktop
1 GbE copper	5x	4x	4x	4x	4x	6x	6x	5x	6x
1 GbE fiber SFP	-	-	-	1x	1x	-	2x	2x	-
10 GbE fiber SFP+	-	-	-	-	-	-	-	-	-
Integrated switch	-	-	-	-	-	8-port	-	-	8-port
Integrated modem	-	-	-	A, RJ11	B, RJ45	-	-	-	-

Hardware – Mid level

	F380	F400 .STD	F400 .F20	F600 .C10	F600 .C20	F600 .F10	F600 .F20	F600 .E20
Firewall throughput	5.2 Gbps	7.1 Gbps	9.0 Gbps	11 Gbps	11 Gbps	11 Gbps	11 Gbps	20 Gbps
VPN throughput	1.4 Gbps	2.3 Gbps	2.3 Gbps	3.1 Gbps	3.1 Gbps	3.1 Gbps	3.1 Gbps	5.6 Gbps
IPS throughput	2.0 Gbps	2.8 Gbps	3.0 Gbps	4,6 Gbps	4,6 Gbps	4,6 Gbps	4,6 Gbps	8.0 Gbps
NGFW throughput	1.4 Gbps	2.2 Gbps	3.0 Gbps	4.2 Gbps	4.2 Gbps	4.2 Gbps	4.2 Gbps	6.4 Gbps
Threat protection throughput	1.2 Gbps	2.0 Gbps	2.7 Gbps	4,0 Gbps	4,0 Gbps	4,0 Gbps	4,0 Gbps	5.8 Gbps
Concurrent sessions	400,000	500,000	500,000	2,100,000	2,100,000	2,100,000	2,100,000	2,100,000
New sessions per sec.	15,000	20,000	20,000	115,000	115,000	115,000	115,000	115,000
Form factor	1U rack	1U rack	1U rack	1U rack	1U rack	1U rack	1U rack	1U rack
1 GbE copper	8x	8x	8x	12x	12x	8x	8x	8x
1 GbE fiber SFP	-	-	4x	-	-	4x	4x	-
10 GbE fiber SFP+	-	-	-	-	-	-	-	2x
Power supply	Single	Single	Dual	Single	Dual	Single	Dual	Dual

Hardware – High level

	F800			F900				F1000			
	.CCC	.CCF	.CCE	.CCC	.CCE	.CFE	.CFEQ	.CE0	.CE2	.CFE	.CFEQ
Firewall throughput	30 Gbps	30 Gbps	30 Gbps	35 Gbps	35 Gbps	35 Gbps	45 Gbps	40 Gbps	40 Gbps	40 Gbps	46 Gbps
VPN throughput	7.5 Gbps	7.5 Gbps	7.5 Gbps	9.3 Gbps	9.3 Gbps	9.3 Gbps	13.5 Gbps	10 Gbps	10 Gbps	10 Gbps	10.3 Gbps
IPS throughput	8.3 Gbps	8.3 Gbps	8.3 Gbps	11.3 Gbps	11.3 Gbps	11.3 Gbps	13 Gbps	13 Gbps	13 Gbps	13 Gbps	14 Gbps
NGFW throughput	7.7 Gbps	7.0 Gbps	7.0 Gbps	8.0 Gbps	8.0 Gbps	8.0 Gbps	12 Gbps	10.2 Gbps	10.2 Gbps	10.2 Gbps	13 Gbps
Threat prot. Throughput	7.6 Gbps	7.6 Gbps	7.6 Gbps	11.5 Gbps	11.5 Gbps	11.5 Gbps	11.5 Gbps	4.0 Gbps	4.0 Gbps	4.0 Gbps	12 Gbps
Concurrent sessions	2,500,000	2,500,000	2,500,000	4,000,000	4,000,000	4,000,000	4,000,000	10,000,000	10,000,000	10,000,000	10,000,000
New sessions per sec.	180,000	180,000	180,000	190,000	190,000	190,000	190,000	250,000	250,000	250,000	250,000
Form factor	1U Rack	1U Rack	1U Rack	1U Rack	1U Rack	1U Rack	1U Rack	2U Rack	2U Rack	2U Rack	2U Rack
1 GbE copper	24x	16x	16x	32x	16x	8x	8x	16x	32x	16x	16x
1 GbE fiber SFP	-	8x	-	-	-	8x	8x	-	-	16x	16x
10 GbE fiber SFP+	-	-	4x	-	8x	8x	4x	4x	8x	8x	6x
40 GbE fiber QSFP+	-	-	-	-	-	-	2x	-	-	-	2x
Power supply	Dual	Dual	Dual	Dual	Dual	Dual	Dual	Dual	Dual	Dual	Dual

Virtual deployment

	VF10	VF25	VF50	VF100	VF250	VF500	VF1000	VF2000	VF4000	VF8000
# of protected IPs	10	25	50	100	250	500	unlimited	unlimited	unlimited	unlimited
Allowed cores	1	2	2	2	2	2	2	4	8	16

vmware®

Microsoft Hyper-V

KVM

CITRIX® XenServer

6 obszarów kluczowych CGF

Advanced Security

Secure SD-WAN

Central Management

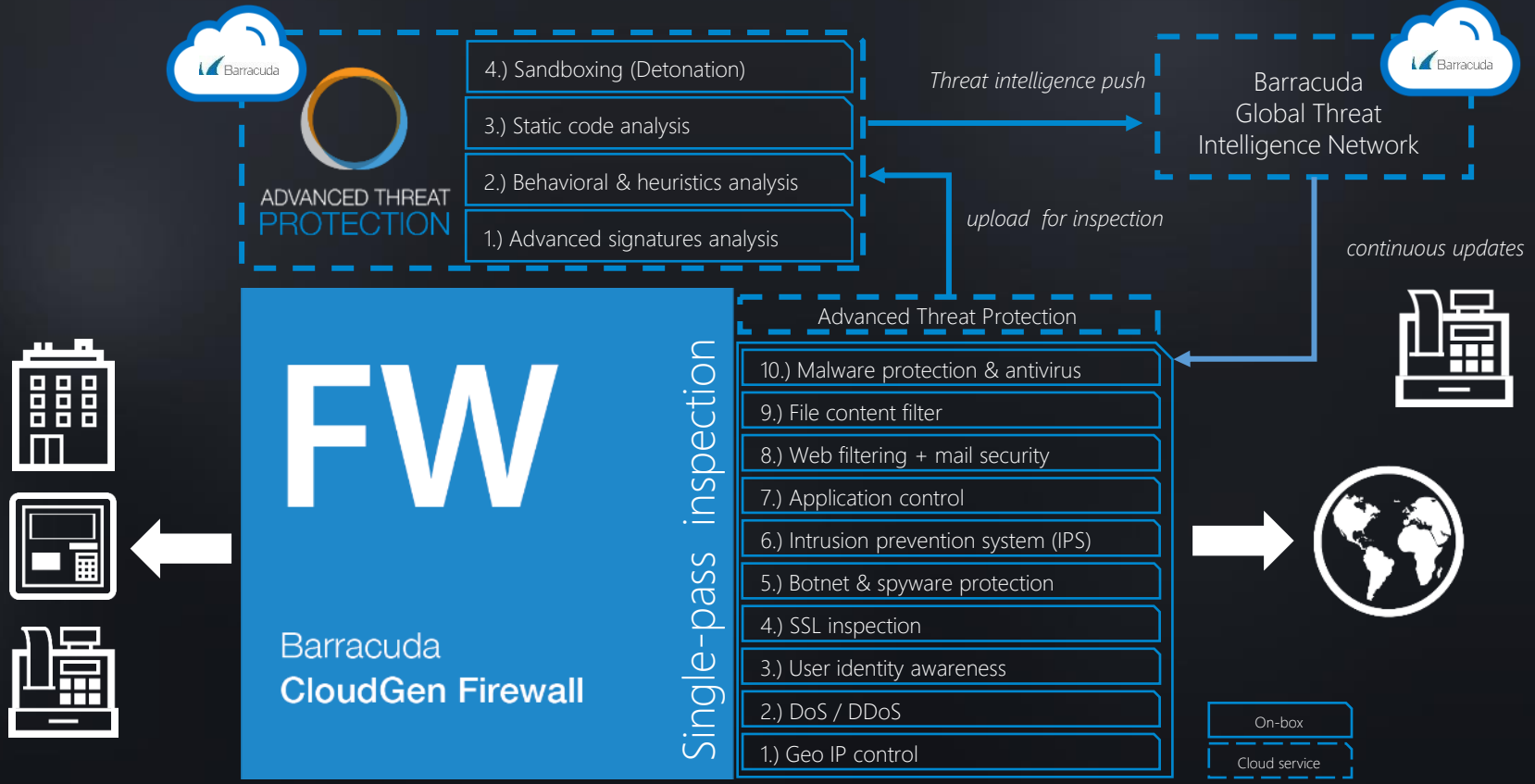
Advanced Remote Access

Public Cloud Integration

Internet of Things and ICS

Barracuda CloudGen Firewall: Security

Full next-generation security



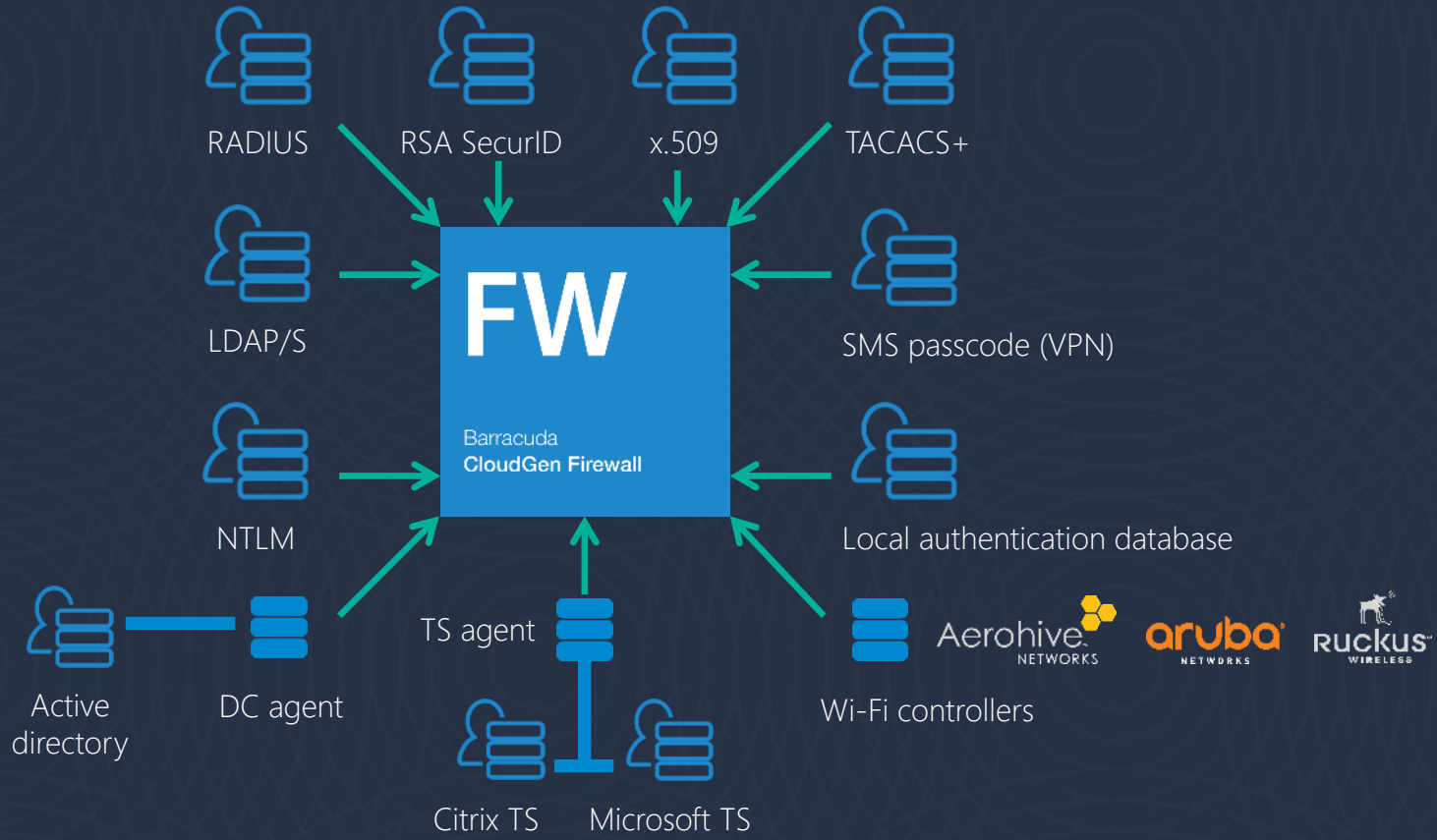
Kontrola aplikacji- „protect the business"

- Kontroluj / akceleruj zezwolony ruch
- Zachowuj pasmo / przyspiesz aplikacje krytyczne biznesowo

Application Rules

	Action	Name	Application	User	URL Filter Policy	QoS	Protocol	Schedule	Source	Destination
0		**P2P**	P2P 4 Risk Bandwidth Consuming File Sharing P2P	Any	N.A.	N.A.	Any	Always	Any 0.0.0.0/0	Any 0.0.0.0/0
1		**Lunch-Break**	Facebook Chat Facebook Photos Facebook Post Twitter Base Twitter Compose Tweet Twitter Receive Tweet	Any	None	Low (ID 3)	Any	LunchBreak	Any 0.0.0.0/0	Any 0.0.0.0/0
2		**Social-Networking**	Social Time/Productivity Consuming Social Networking	Any	N.A.	N.A.	Any	Always	Any 0.0.0.0/0	Any 0.0.0.0/0
3		**Management**	Any	Management groups=OU=Man...	Management Allow all but: (...	NoDelay (ID 4)	Any	Always	Private 10 10.0.0.0/8	Any 0.0.0.0/0
4		**Streaming**	Streaming Bandwidth Consuming Time/Productivity Consuming Media Streaming	Any	None	Low (ID 3)	Any	Always	Any 0.0.0.0/0	Any 0.0.0.0/0
5		**Updates**	Updates Adobe Update Apple Update Avira AV Update Microsoft Update	Any	None	System (ID 1)	Any	Always	Any 0.0.0.0/0	Any 0.0.0.0/0
6		**Salesforce**	Salesforce	Sales groups=OU=Sales	None	NoDelay (ID 4)	HTTP-HTTPS All HTTP protocols	Always	Any 0.0.0.0/0	Any 0.0.0.0/0
7		**Surf-Strict**	Web browsing	Employees groups=OU=Users	Employees Allow all but: (...	Bulk (ID 2)	HTTP-HTTPS All HTTP protocols	Always	Any 0.0.0.0/0	Any 0.0.0.0/0
8		**All-Apps**	Any	Any	None	Bulk (ID 2)	Any	Always	Any 0.0.0.0/0	Any 0.0.0.0/0

User awareness

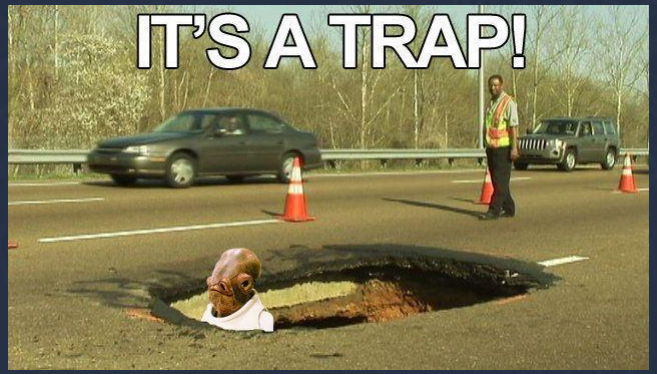


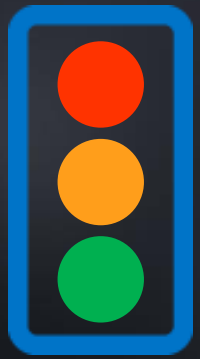
POKAZ PRAKTYCZNY

Barracuda
Your journey, secured.

Elementy

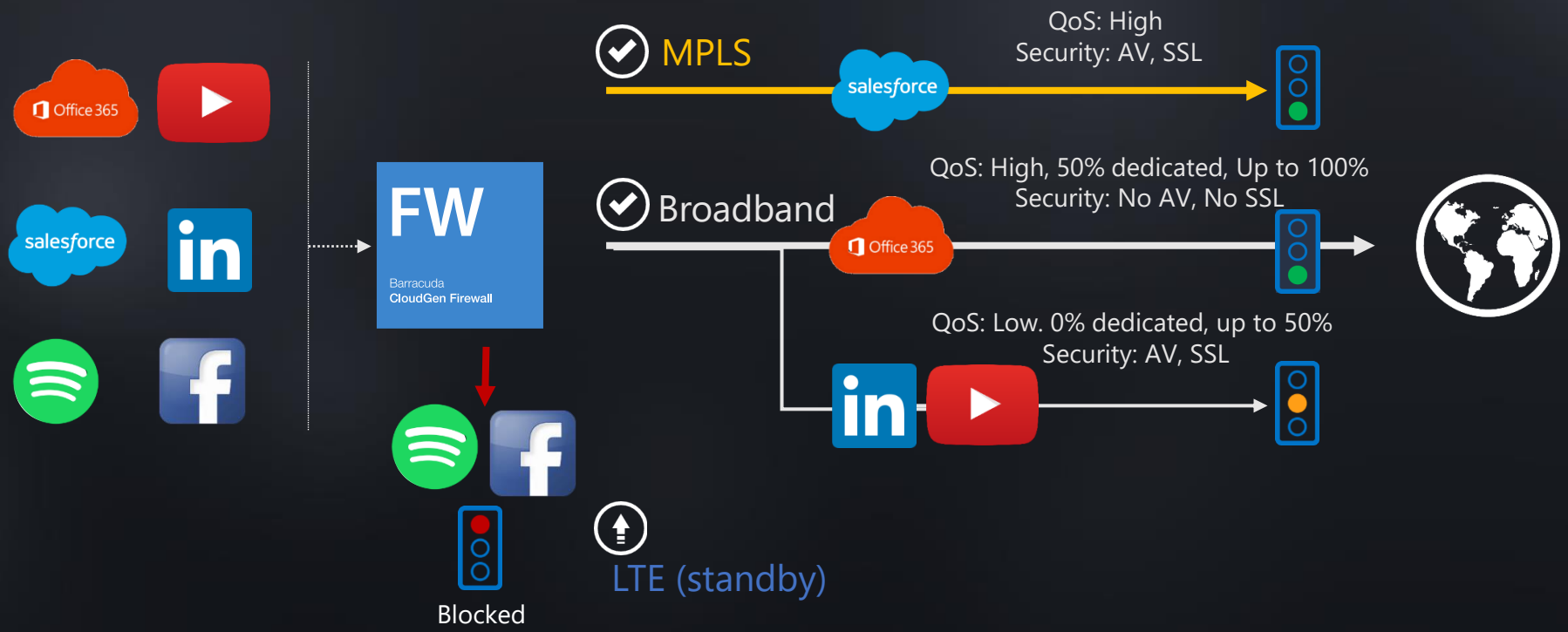
- **SSL Inspection**
- **Kontrola aplikacji + URL filtering**
- **Skaner AV + Sandboxing**
- **DNS Interception + Sinkholing***



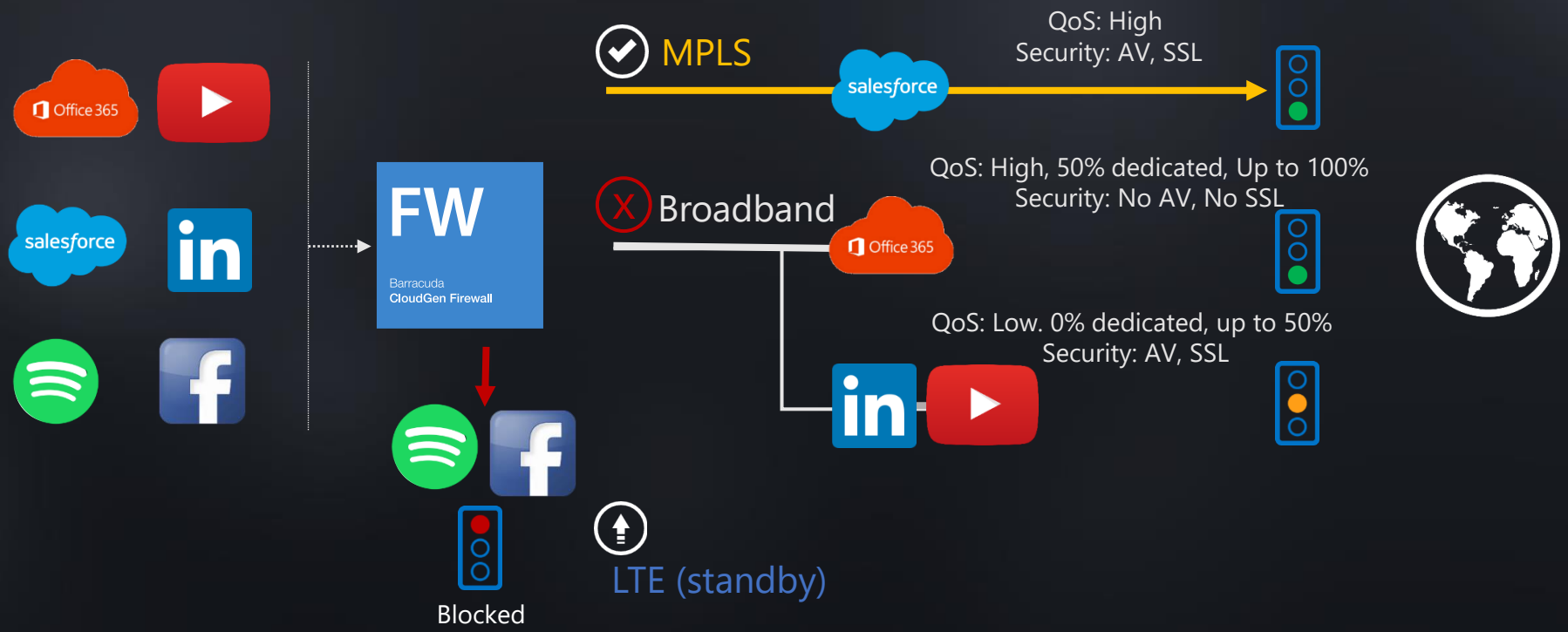


Inteligentne zarządzanie pasmem

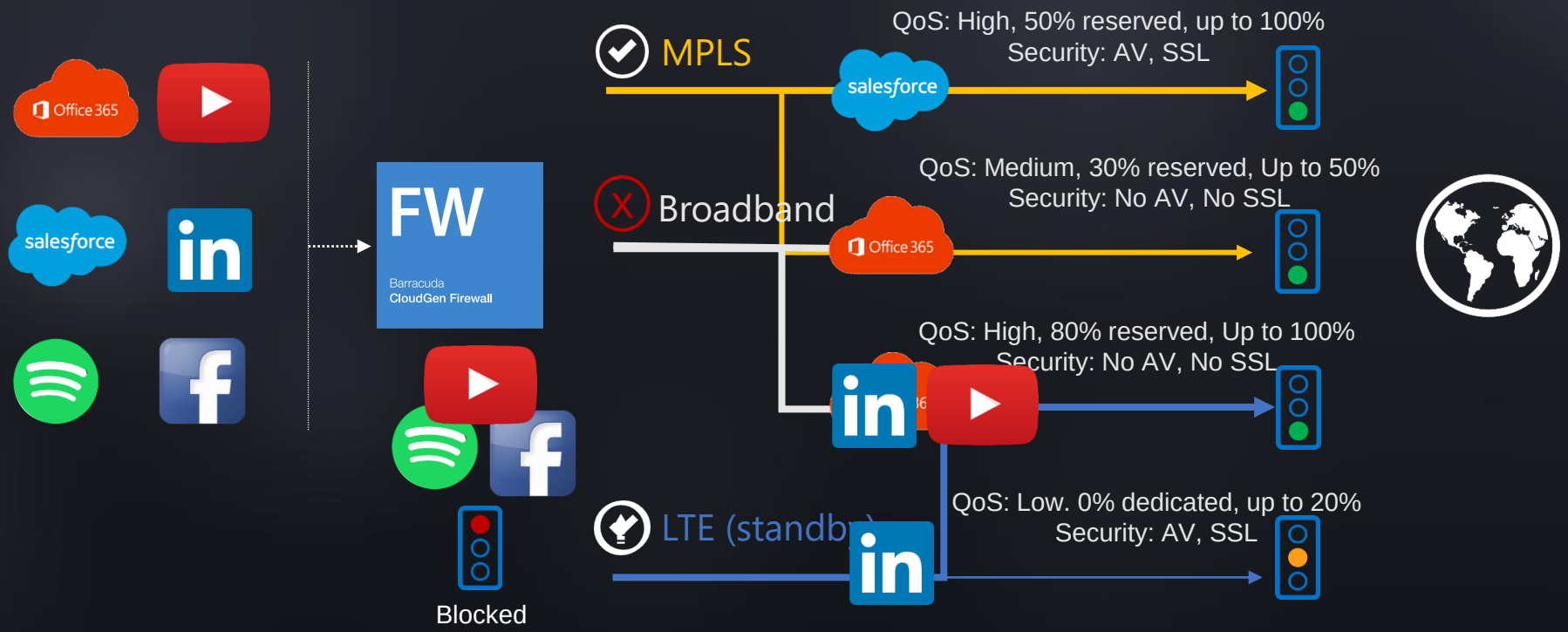
Barracuda CGF: Traffic Intelligence



Barracuda CGF: Traffic Intelligence



Barracuda CGF: Traffic Intelligence



Barracuda CloudGen Firewall: SD-WAN

Link Management
Bandwidth Optimization

Cloud Generation SD-WAN

Agregacja połączeń:

- Do 24 „fizycznych” uplinków per logiczne połączenie VPN

ExpressRoute / Direct Connect
Cloud Interconnect

Broadband

3G / 4G

Cloud Generation SD-WAN

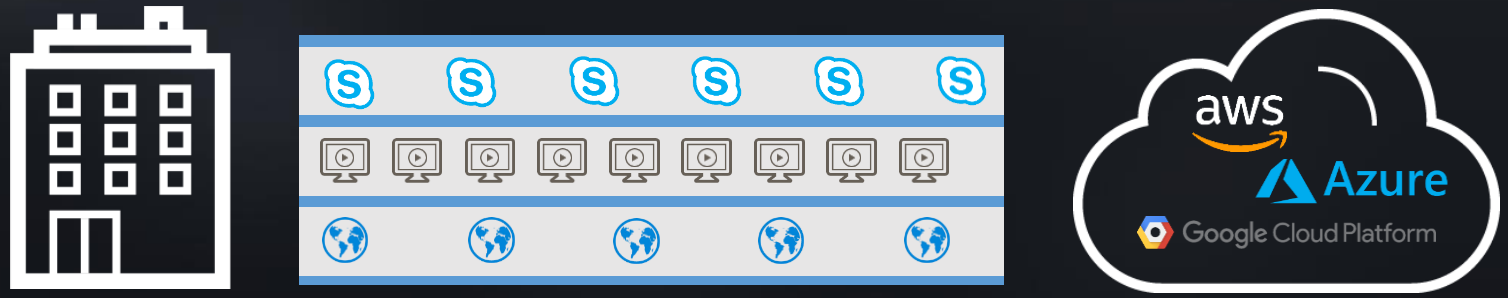
Optymalizacja wykorzystani pasma:

- Dynamic Bandwidth & Latency Detection
- Performance Based Transport Selection

Cloud Generation SD-WAN

Optymalizacja wykorzystani pasma:

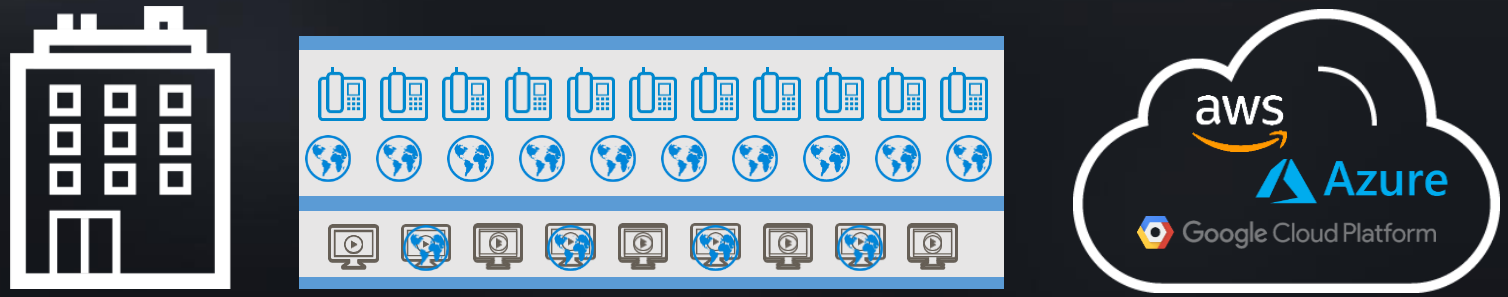
- Dynamic Bandwidth Detection
- Performance Based Transport Selection
- Adaptive (Re)Balancing



Cloud Generation SD-WAN

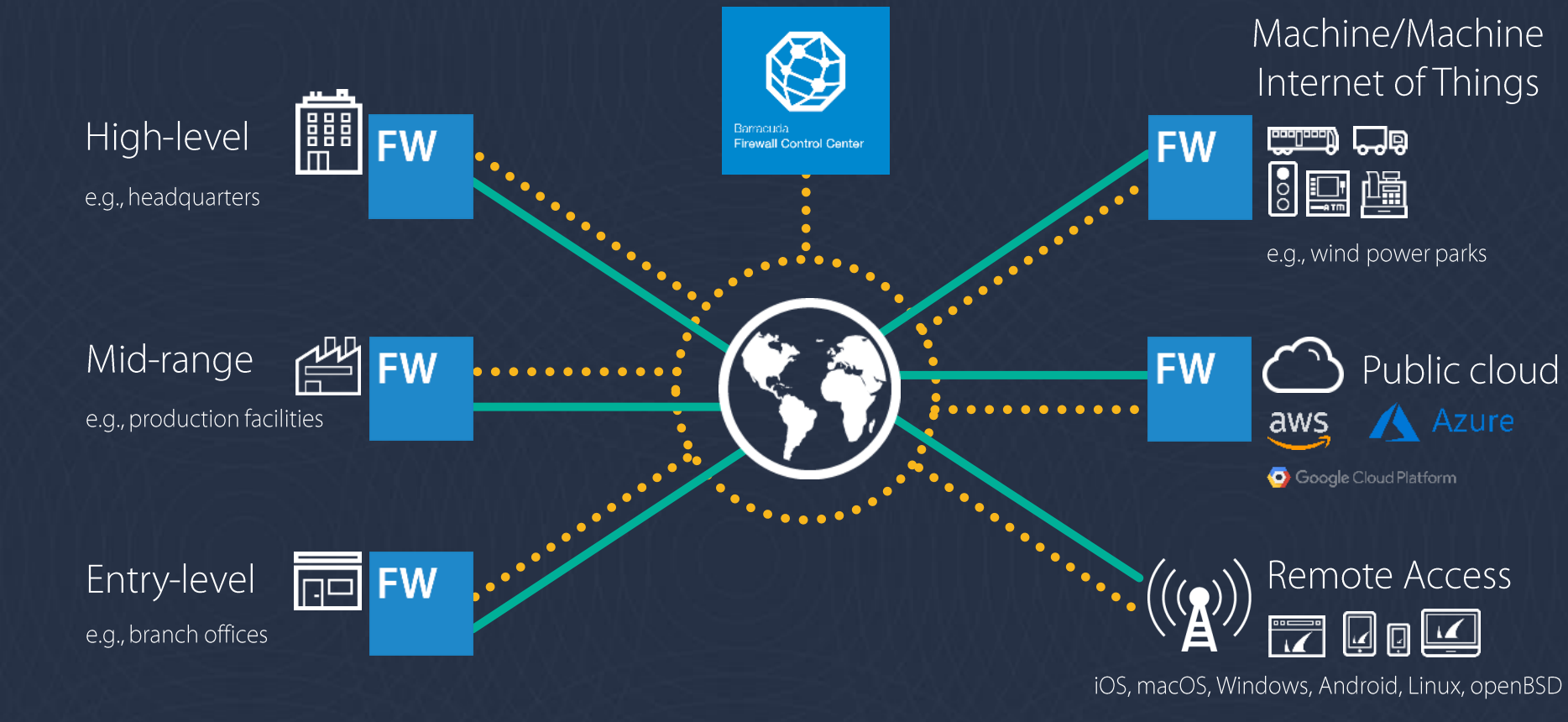
Ochrona ruchu krytycznego biznesowo

- Immunity to bandwidth fluctuations
- Voice/Video Packet Deduplication for Loss mitigation

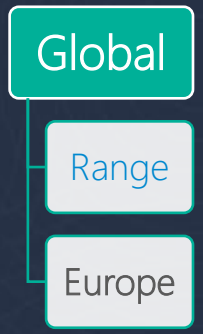


Barracuda CloudGen Firewall: Centralne Zarządzanie

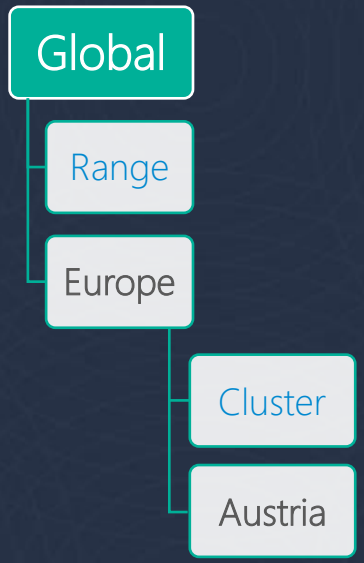
Barracuda CGF Control Center



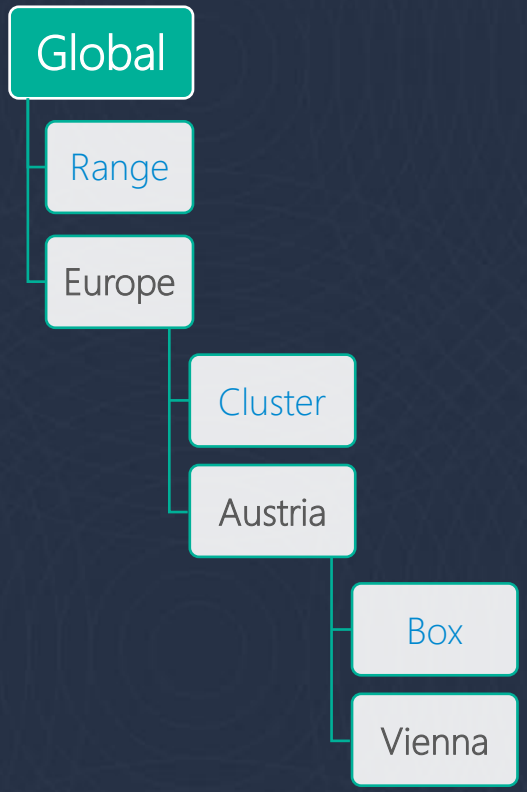
Koncepcja hierarchicznego „multi-tenancy”



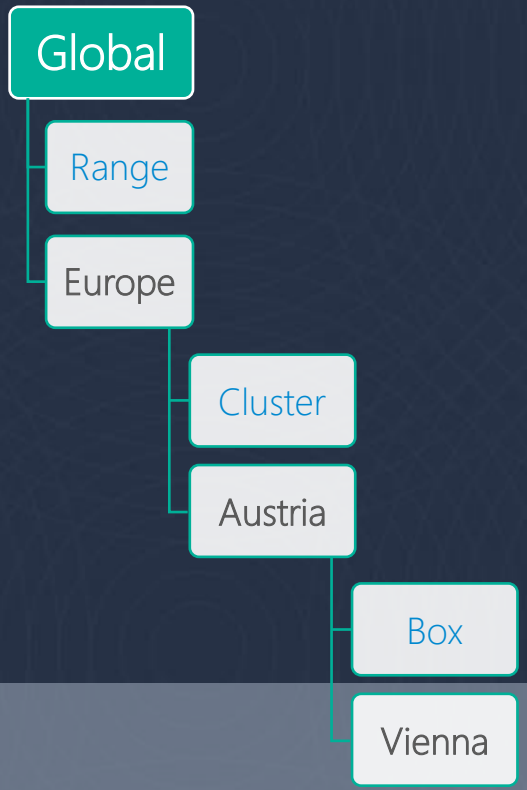
Koncepcja hierarchicznego „multi-tenancy”



Koncepcja hierarchicznego „multi-tenancy”

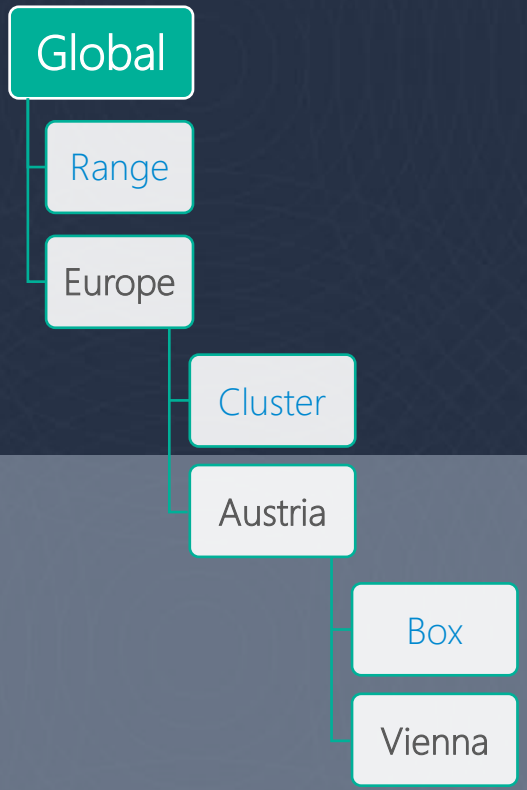


Koncepcja hierarchicznego „multi-tenancy”



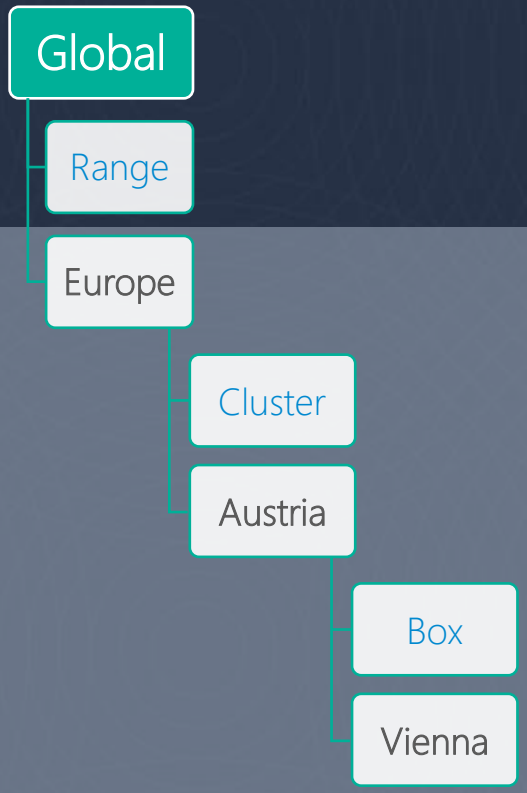
Dostęp admina do pojedynczego box’a

Koncepcja hierarchicznego „multi-tenancy”



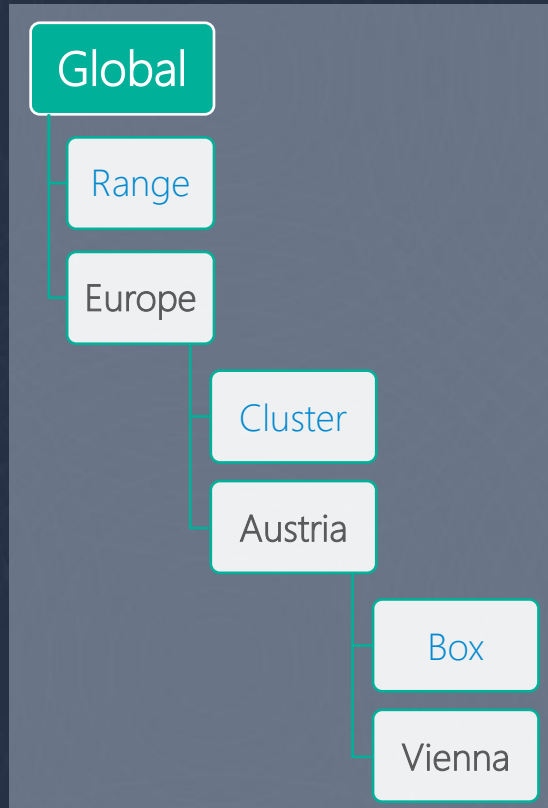
Dostęp admina na poziomie kraju

Koncepcja hierarchicznego „multi-tenancy”



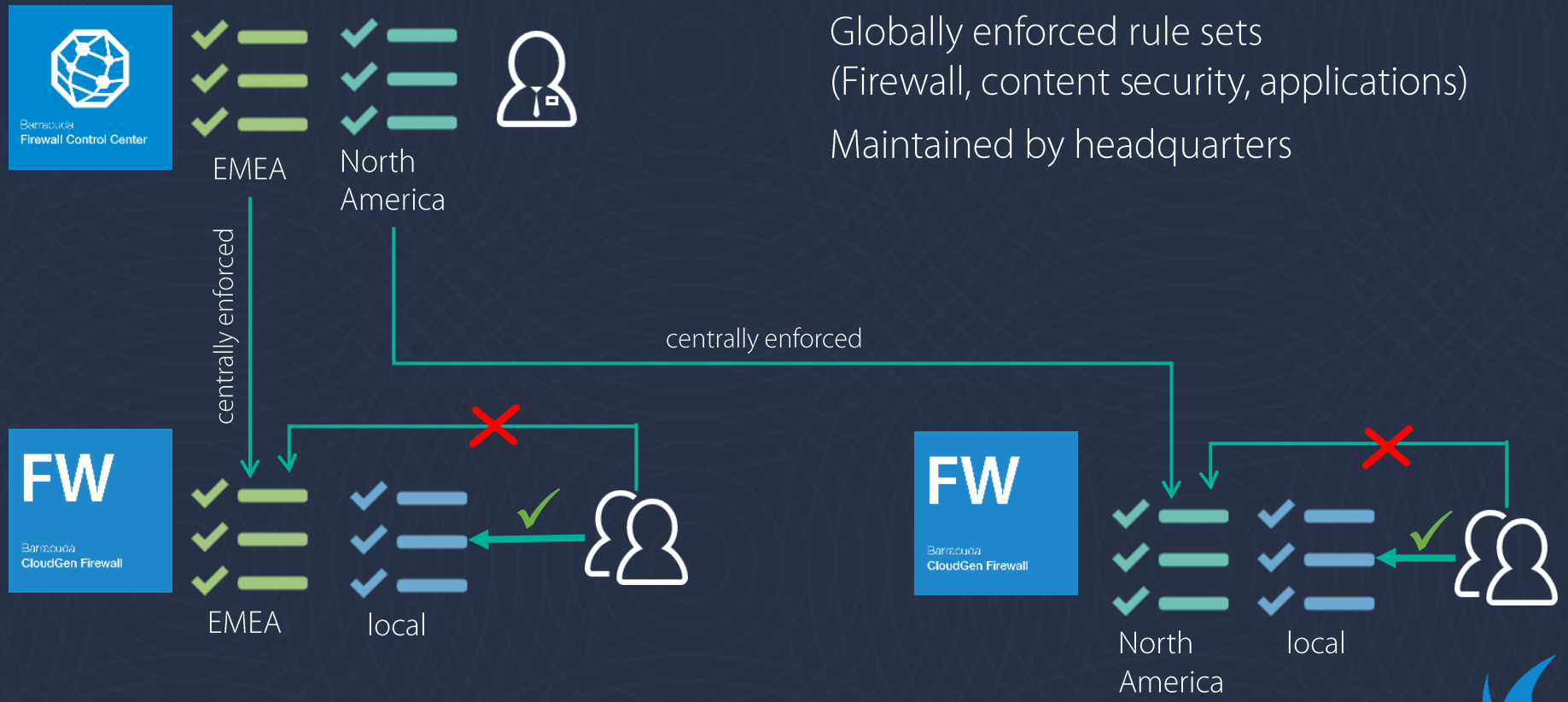
Dostęp admina na poziomie kontynentu

Koncepcja hierarchicznego „multi-tenancy”



Administrator globalny

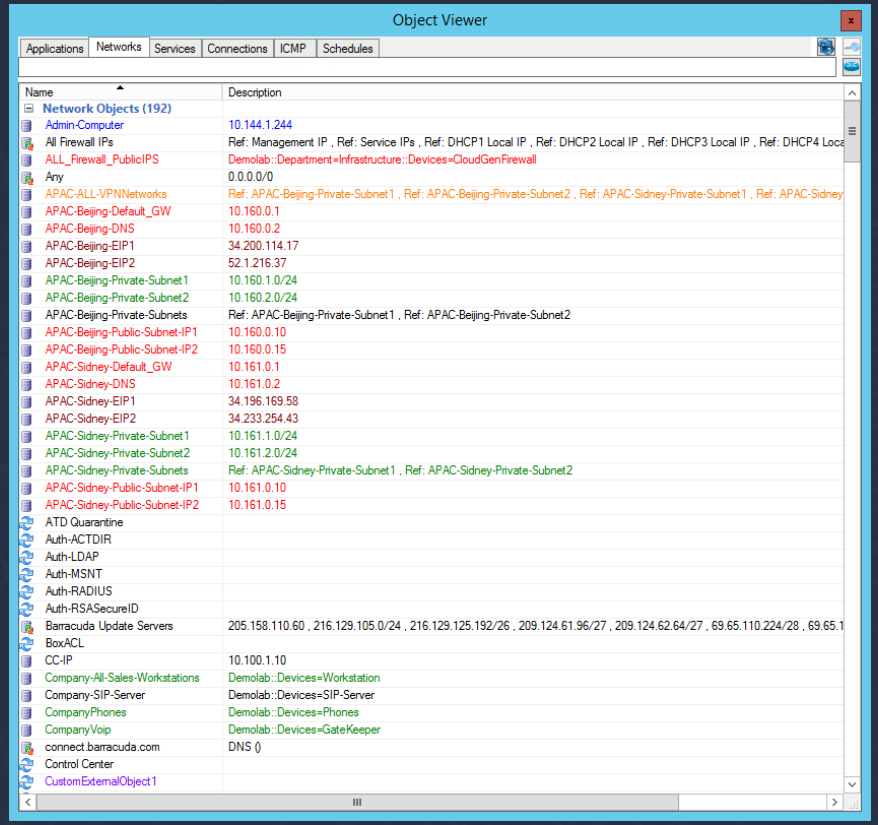
Distributed firewall



Globally enforced rule sets
(Firewall, content security, applications)

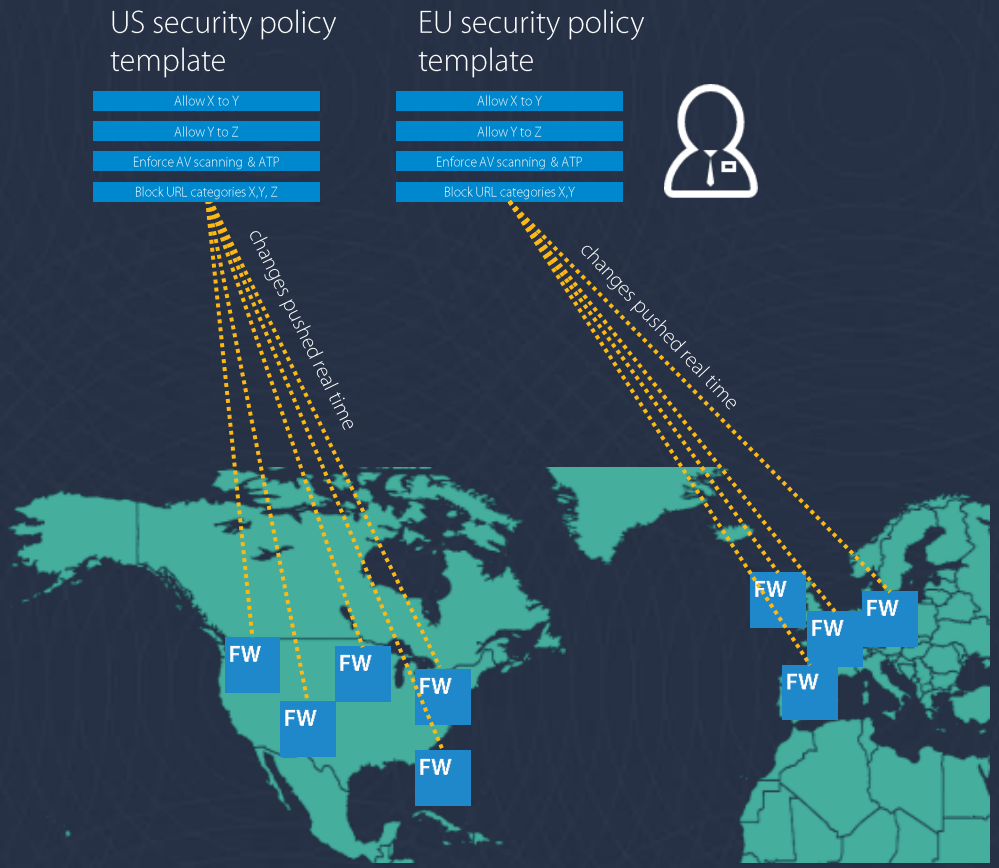
Maintained by headquarters

Globalne Repozytoria Obiektów



- Networks, application definitions, URL filter policies, file content policies, user definitions, schedules
- Distributed in real time
- Objects available to all managed firewalls
- Updates distributed in real-time on all managed firewalls
- Shared globally, per range, or per cluster
- Stackable (objects in objects)

Globalne Repozytoria Szablonów



- Permanently “linkable” configuration store
- ALL configuration items
- Available globally, per range, per cluster
- Exemptions/overrides available
- Quick deployment of “similar” deployments

Live Status Polling

5	Demo Environment Distributed Network					
AZURE001	AZURE Rio primary	172.31.6.101	6.0.1-033	Brazil	VF1000	AZ01VS
AZURE002	AZURE Rio secondary	172.31.6.102	6.0.1-033	Brazil	VF1000	Sec: AZ01VS
BOSRV001	DFFW Paris	172.31.6.103	6.0.1-033	France	VF100	BO1VS
BOSRV002	DFFW Madrid	172.31.6.104	6.0.1-033	Spain	VF100	BO2VS
BOSRV003	DFFW Rome	172.31.6.105	6.0.1-033	Italy	VF100	BO3VS
BOSRV004	DFFW Athens	172.31.6.106	6.0.1-033	Greece	VF100	BO4VS
BOSRV005	DFFW Tokyo	172.31.6.107	6.0.1-033	Japan	VF100	BO5VS
BOSRV006	DFFW Cairo	172.31.6.108	6.0.1-033	Egypt	VF100	BO6VS
HQSRV050	HQ primary	172.31.1.101	6.0.1-033	Austria	VF100	HQ050VS
HQSRV052	HQ secondary	172.31.1.102	6.0.1-033	Austria	VF100	Sec: HQ050VS
HQSRV053	Fake Internet and MPLS	172.31.1.100	6.0.1-033	Bahamas	VF100	HQ53VS

- REST API for status query available

ZTD Zero-Touch-Deployment

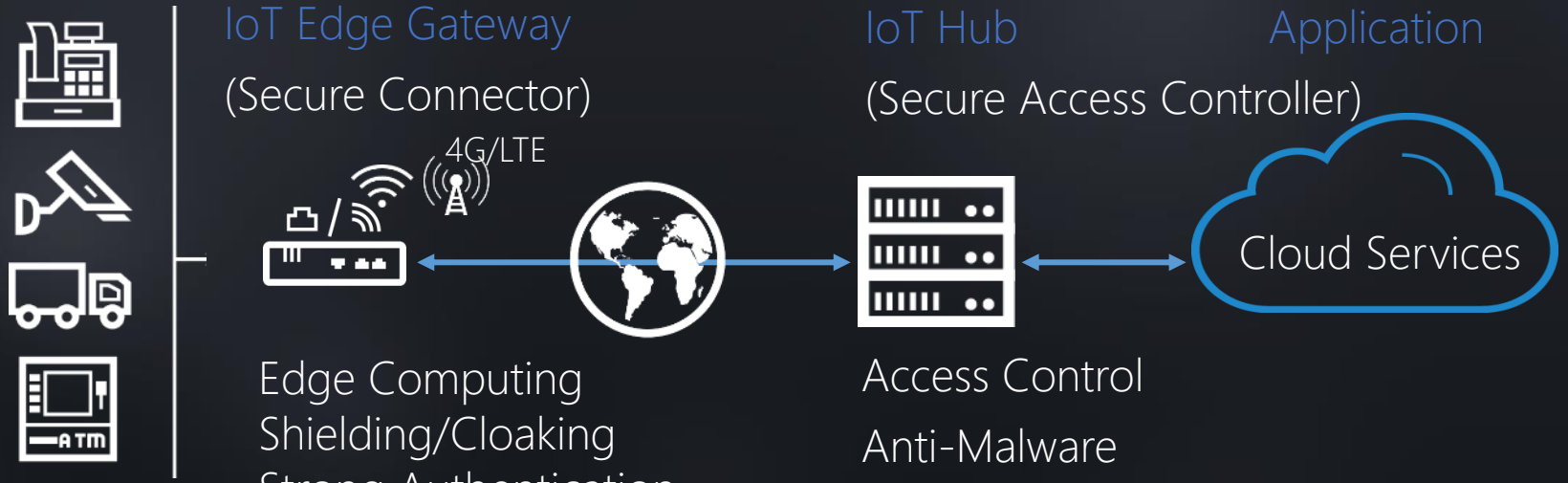
Przydatne w rozwiązaniach SD-WAN i IoT

Barracuda Firewall
Control Center

Barracuda Cloud Control

Barracuda CloudGen Firewall: IoT

Security architecture of an IoT deployment

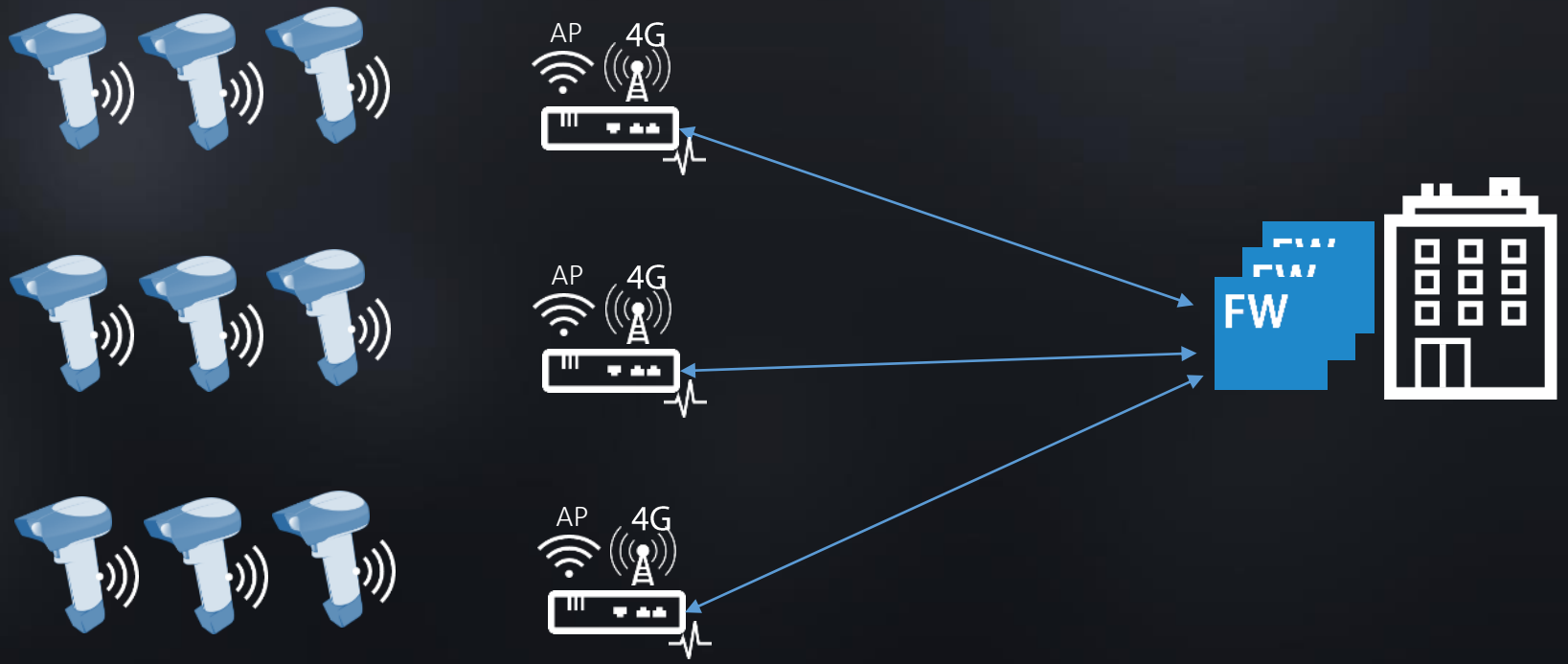


IIoT: Edge computing support

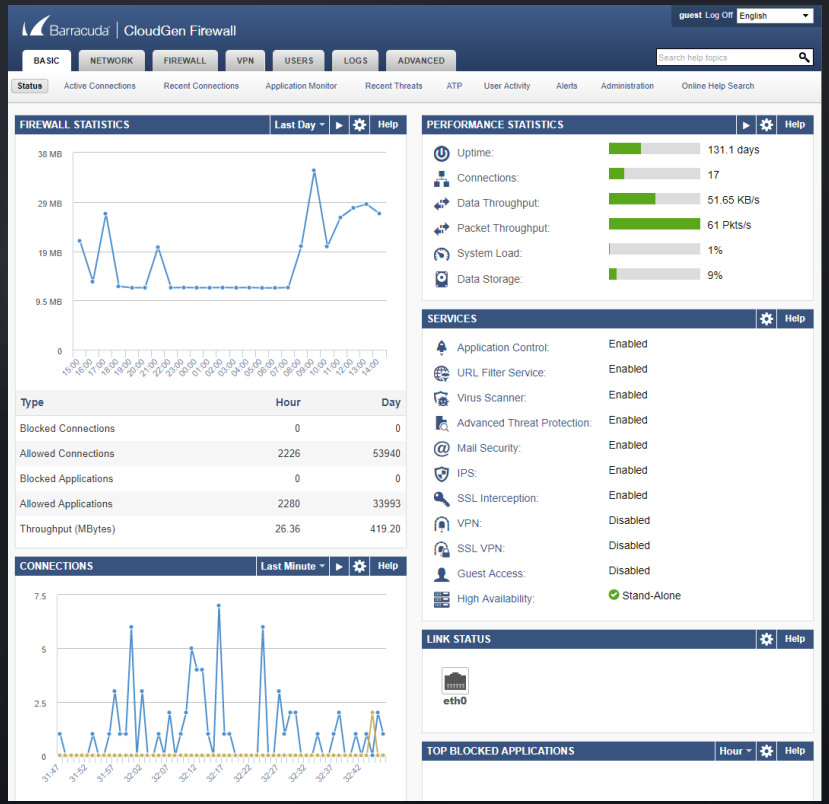
E.g. ticket validation via Wi-Fi barcode scanner

Secure Connector + Custom App installed

Secure Access Controller(s)



Ostatnia rzecz… interfejs web



OS-independent administration tool

Available for:

- Hardware appliances (F18 to F400)
- All virtual editions (VF10 to VF8000)
- All Cloud editions

Dziękuję za uwagę!

Michal Zalewski
Sales Engineer, CEE
mzalewski@barracuda.com

Barracuda
Your journey, secured.