iNNOVO
CLOUD

Die Cloud beim Kunden

Palo Alto Networks in the Cloud

Palo Alto Networks User Group
Frankfurt, 21.02.2013

Pablo Endres <pablo.endres@innovo.cloud.de>

Agenda

- About me
- What is iNNOVO CLOUD?
- Cloud Computing 101
- Multi-tenancy in the Cloud
- How we use are Palos
  - VSYS: Multi-tenancy support: Pros and Cons
  - Advance use-case of APP-ID: blocking SSH tunneling
  - Automation: scripts and intro to iNNOVO network control project
- Missing features
- Questions

About me

Pablo Endres

Security and Infrastructure consultant
Head of ITSEC @ iNNOVO Cloud GmbH

Email: pablo.endres@innovo-cloud.de
Twitter: @epablosensei
Blog: http://pabloendres.com

- Design and implementation of secure cloud based environments
- Penetration and security testing (design, planning and execution)
- Development of security programs and concepts
- Experienced project manager
- Holder of multiple certifications: CISSP, OPSA, OPST
- Active researcher @ ISECOM and contributor to Hacker High school
- Hands on experience in the telecommunications industry: wireless carriers, ITSPs, ISP and hosting providers

WHAT IS INNOVO CLOUD?

Provide Cloud-based solutions with the best possible security

- iNNOVO Cloud is a young company
  - Founded in October 2012 in Frankfurt
  - Provide Cloud-Solutions focused on SMB

- Provide SMB customers all the benefits of Cloud-based solutions and services
  - with the best possible security
  - without the “Cons” of going into an external data center

The Frankfurt Cloud becomes... ...the „iNNOVO Cloud“

iNNOVO CLOUD

Die Cloud beim Kunden

- iNNOVO Cloud surfaced from the Frankfurt Cloud Project
  - Goethe Universität Frankfurt
  - and a big german Bank
- We benefit from the experience gathered in the first two generations of the Frankfurt Cloud Project
  - Security relevant results
  - Customer experiences

One standard cloud solution for all sizes

iNNOVO CLOUD
Die Cloud beim Kunden

- Close work with Rittal since mid 2012
  - Standard and integrated Cloud-solution for SMB customers

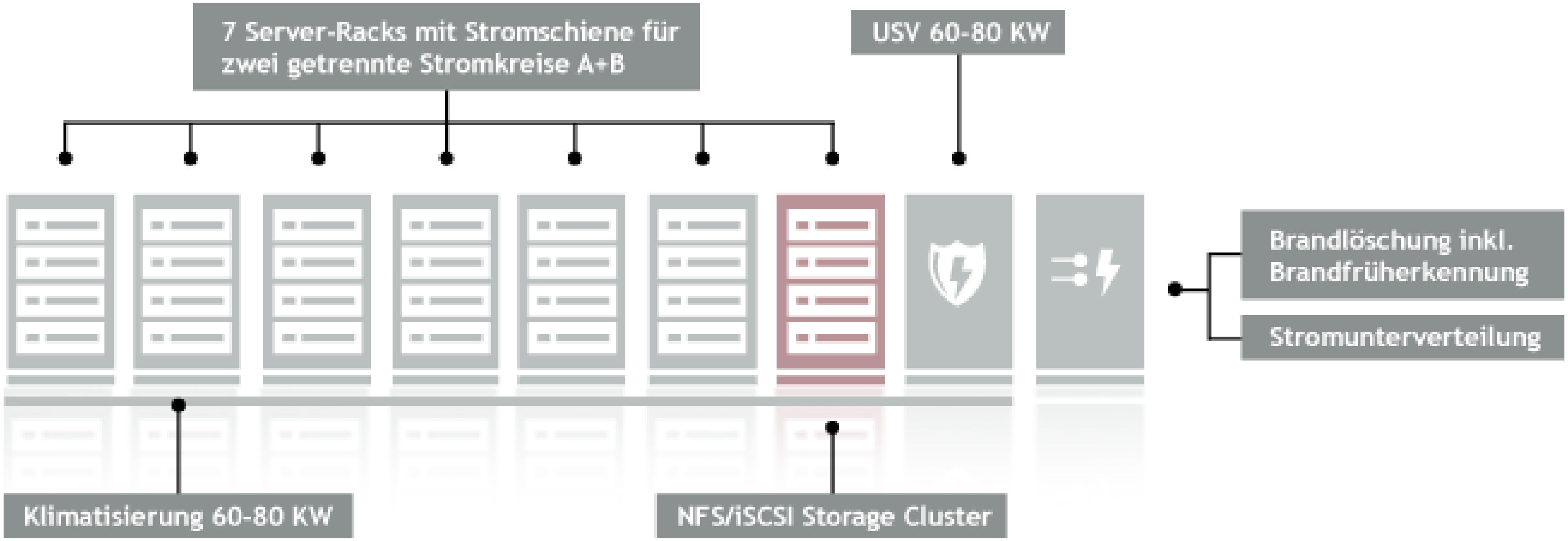
- One **standard** cloud data center turnkey solution in different forms and sizes
  - iNNOVO MCC
  - iNNOVO ICC
  - iNNOVO VPDC

- The iNNOVO MCC and iNNOVO ICC will be presented for the first time on CeBIT 2013
  - Halle 11 Stand F12

Die Cloud beim Kunden

Based on Rittal‘s RiMatrix-S Container

- 7 (cloud Hw) + 2 (UPS + Power) Racks
- Enriched with the iNNOVO Cloud-services
- Customized for your needs


7 Server-Racks mit Stromschiene für zwei getrennte Stromkreise A+B
USV 60-80 KW
Brandlöschung inkl. Brandfrüherkennung
Stromunterverteilung
Klimatisierung 60-80 KW
NFS/iSCSI Storage Cluster

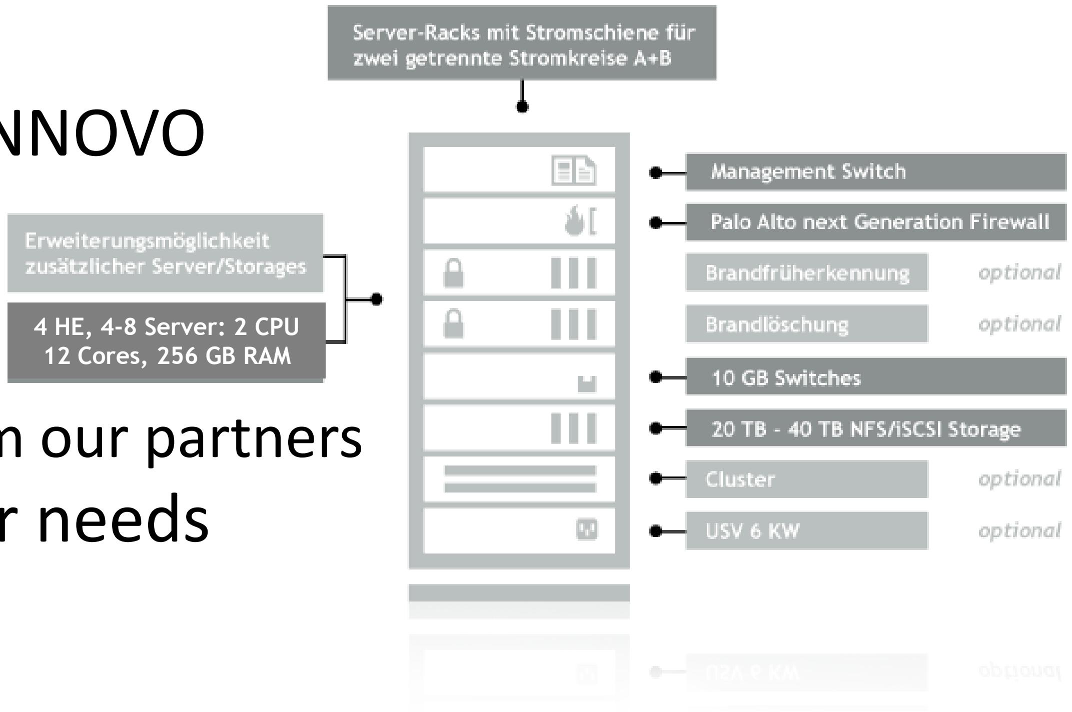
iNNOVO MCC

iNNOVO CLOUD

Die Cloud beim Kunden

Based on the RiMatrix X5 Series from Rittal

- 1-Rack Cloud data center
  - Can be placed in the office
- Enriched with the iNNOVO Cloud-services
  - IaaS
  - Virtual Desktops
  - SaaS solutions from our partners
- Customized for your needs



Server-Racks mit Stromschiene für zwei getrennte Stromkreise A+B

Erweiterungsmöglichkeit zusätzlicher Server/Storages

4 HE, 4-8 Server: 2 CPU 12 Cores, 256 GB RAM

Management Switch

Palo Alto next Generation Firewall

Brandfrüherkennung optional

Brandlöschung optional

10 GB Switches

20 TB - 40 TB NFS/iSCSI Storage

Cluster optional

USV 6 KW optional

iNNOVO
VPDC

iNNOVO
CLOUD
Die Cloud beim Kunden

Virtual Private Data Center

- For customers that don‘t really require their data on site
- Cloud services from our regional Frankfurt Data Center
- Privacy and security have the highest priority
  - Only you have access to your VMs and data
  - Based on the same “private cloud” concept used in all our products
    - isolation between tenants

A crash course in cloud computing

CLOUD COMPUTING 101

Evolution of virtualization tech + hosting model → Cloud computing

Cloud Computing

- Cloud Computing is an evolving model, which means that many definitions of the term exist.

Smartphone
Documents
Laptop
Chat
E-mail
GAL
Presentations
Blogs
Video
Calendar
Tablet
Pictures
Training
Address Book
Spreadsheets
Desktop

- Started as a marketing buzzword
- Born from:
  - *Cloud*, referring to networks, in particular the Internet;
  - and *Computing* that refers to the processing, storage, applications, services and hardware information infrastructure.

- Result of the evolution of a series of technologies
  - virtualization,
  - and the hosting model

Cloud-washing consists in:
s/managed service/cloud/g
s/managed server/cloud server/g

Are all Cloud Computing offerings for real?

- Too many marketing departments have abused the term *cloud*

- "We let our data processing be dealt with by a service provider in their data center. We are then already using *the cloud*, right?"

➡ **Wrong!**

- What once was a "managed server" or a service accessed via the Internet or VPN
  - Now labeled as Cloud Server

- This "Principle" is call **Cloud-washing**

Security is not one of the explicit trades of Cloud Computing

Characteristics or Features of Cloud Computing (according to NIST)

1. **On-demand self-service**
2. **Broad network access:**
   - different networks, (the Internet, cell services)
   - different devices (PC, smart phone, table)
   - applications (Web based, PC application, App)
3. **Resource pooling or sharing**
4. **Rapid elasticity or scalability**
5. **Monitoring and metering**
   - transparent and accurate

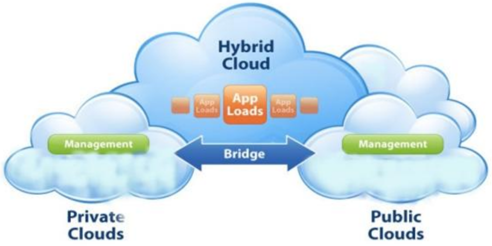
Traffic separation and real multi-tenancy… … that’s what it’s all about ….

Characteristics of a secure Cloud Computing environment

- Strict and transparent security policies
  - Ensure the availability and confidentiality of data
  - For example, the Ubuntu One
- Transparency in the controls
  - Logs
  - Alerts
- Real multi-tenancy in each module
- Effective traffic separation
  - Between different tenants
    - Can you see / access services of other tenants?
  - Between the provider and the tenants
    - Can the provider access your services?

Deployment Models

- **Public:** Anyone can consume resources i.e. Amazon EC2
- **Private:** Available only to the owner i.e. local Cloudstack instance
- **Community:** shared resources between multiple organizations with similar concerns or requirements: security, compliance i.e. cloud for banks
- **Hybrid:** Infrastructure build with 2 o more models. Normally private + public for burst or HA



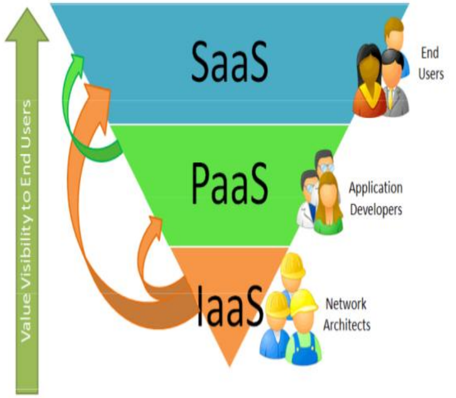
SaaS -> end users - PaaS -> Develpers IaaS -> SysAdmins

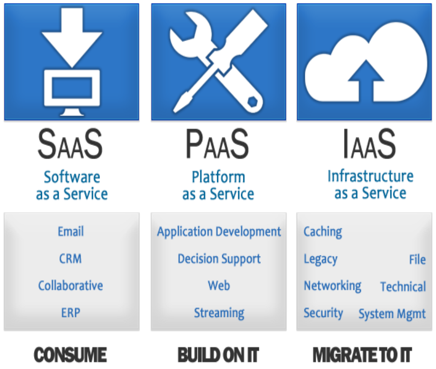
iNNOVO CLOUD

Die Cloud beim Kunden

Types of service

- **Software as a Service (SaaS)**
  - Consume – End users
  - Gmail, Sales force, Office 365
- **Platform as a Service (PaaS)**
  - Build on it - Developers
  - Azure, Google Apps
- **Infrastructure as a Service (SaaS)**
  - Migrate to it - SysAdmins
  - Amazon EC2, Rackspace, iNNOVO CLOUD





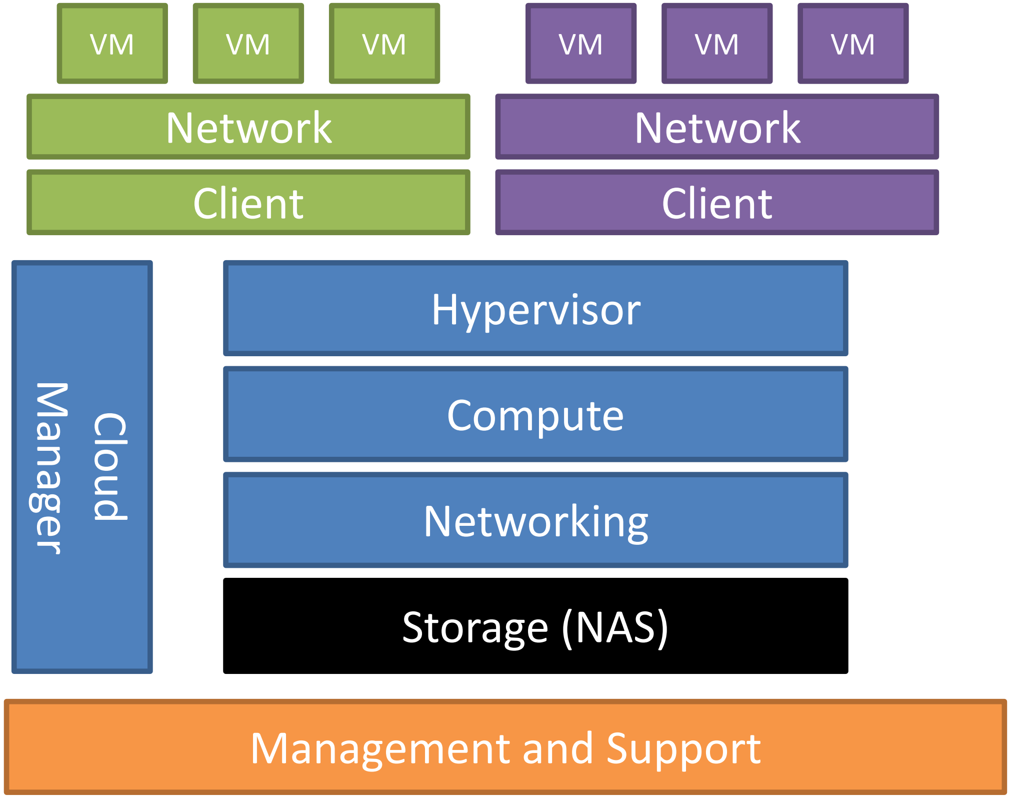
Security issues in cloud environment

MULTI-TENANCY AND THE CLOUD

Standard Cloud Architecture

iNNOVO CLOUD

Die Cloud beim Kunden

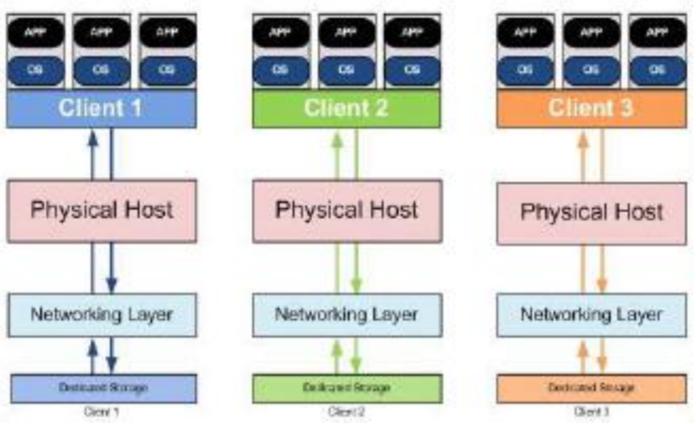


The Cloud Architecture implies sharing resources with other tenants

iNNOVO CLOUD
Die Cloud beim Kunden

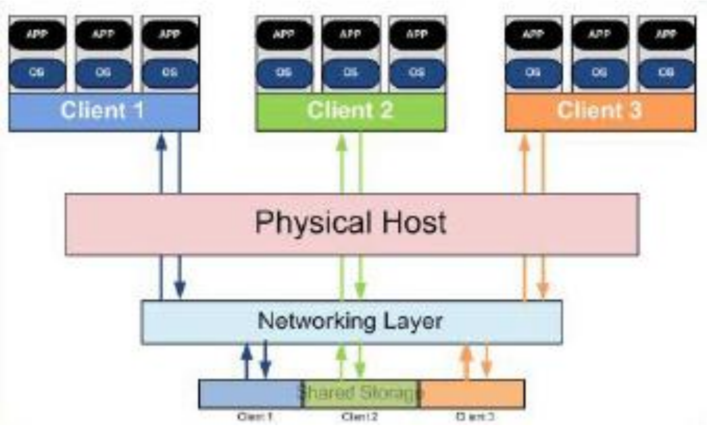
Traditional Datacenter Architecture

- Shared management?
- Traffic separation
  - Dedicated switches
  - vlans



Cloud Multi-tenancy Architecture

- Shared physical host?
- Shared storage
  - Different shares?
- Traffic separation
  - vlans, routers, firewalls?

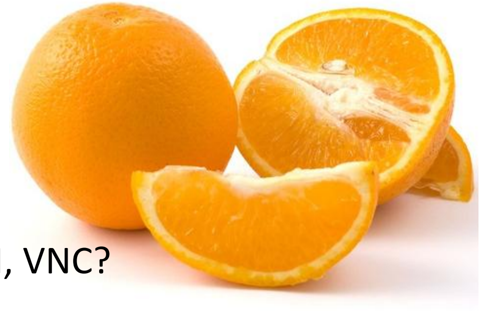


Isolation enables real multi-tenancy

Cloud ready products and infrastructures should support **real multi-tenancy**, providing:

- Isolated contexts for each tenant and the provider
- Isolated management interfaces
  - Not only for traffic, but also services: auth, logging, monitoring
- Separate administration for each virtual container
- Heavy use of roles to permit delegation and separation of duties

Both the provider and the tenant prove to be juicy targets



Juicy targets in a cloud environment

- Tenant machines
  - To access their resources
  - To access the cloud management interfaces
  - Normally reachable using remote management protocols RDP, SSH, VNC?
- The Cloud manager
  - To gain control of the cloud: free resources, access to tenant machines / data
  - Normally reachable via a Web site or API

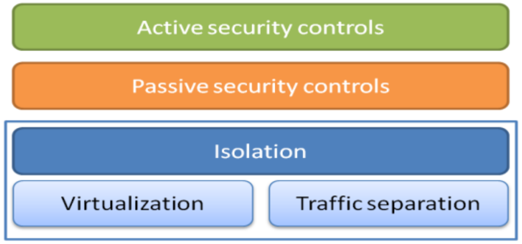
Countermeasures

- Isolation must be implemented in all components of the Cloud
- All normal security and hardening measures and processes should be in place on:
  - Cloud Manager
  - Firewalls
  - Hypervisors
  - OSS
  - BSS

A combination of isolation, active and passive security controls are important

iNNOVO CLOUD
Die Cloud beim Kunden

Security measures



- Active security controls
  - Operations monitoring
  - Compliance scans (state monitoring)
  - Vulnerability scans and penetration testing in regular intervals.

- Passive security controls
  - Hardening of all components in the architecture (network, hypervisor, operating system, storage…)
  - Log correlation and behaviour analysis
  - Combination of both: IDS / IPS

- Isolation must be implemented in all components of the Cloud

Our Palo Alto devices provide most of the isolation required on the network layer

	PANOS feature
Isolation	
Context for provider	Virtual System
Context for each tenant	Virtual System
Isolated mgmt. interfaces	
Traffic	Virtual Router
Additional mgmt interface for tenant services	Not possible, everything via mgmt port
Auth services	Multiple services configurable (traffic via mgmt port)
Roles and auth	
Administrator for each container	Vsys admin
Different roles	Present
Logs and Auth	
Central logging	Panorama, syslog
Alerting and monitoring	syslog, snmp, Splunk App
Central auth	LDAP, Radius, Local

Benefits of the Palo Alto Networks Next Generation Firewalls

HOW WE USE ARE PALOS

Palo Alto products play a central role in the iNNOVO CLOUD products

iNNOVO CLOUD
Die Cloud beim Kunden

- Palo Alto firewalls are part of our products
  - 5000 Series for the data centers and iNNOVO ICC
  - 3000 Series for the iNNOVO MCC
  - 200 series as emergency access device

- Subscriptions:
  - Are available and used in the VPDC
  - Are optional of ICC and MCC

- Benefit of the GlobalProtect-Satellite
  - for VPN deployment
  - interconnection with remote sites and customers

Vsys enable multi-tenancy, but could use some pimping

	Pros	Cons
vsys	Provides isolation (provider + tenant)	
	Enables multi-tenancy	
	Enables self-service (tenant vsysadmin)	
	Multiple auth services	All traffic via mgmt port
		SNMP context is not restricted to each vsys
		Can’t use the same IP on multiple interfaces (different vr and vsys)
		Vsys admin can’t see the interfaces

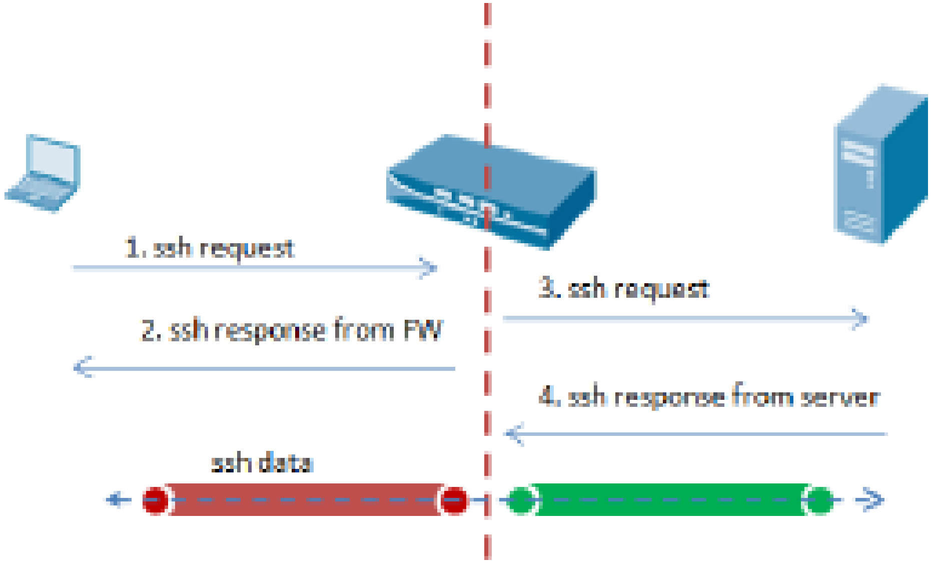
APP-ID provides advance protection to tenants

iNNOVO CLOUD

Die Cloud beim Kunden

Use case: Block SSH tunnels

- Customer in the finance sector
- Test and QA VMs
- Uses APP-ID to allow SSH but block the use of SSH tunnels
  - Allow SSH
  - Deny ssh-tunnel



We use the API and scripting capabilities to enable automation

Automation via scripts and API

- Automatically export config backups
- Initialize a device out of the box
- Part of our automation and management portal (in development)

Automation portal

Creates new tenants in the firewall :

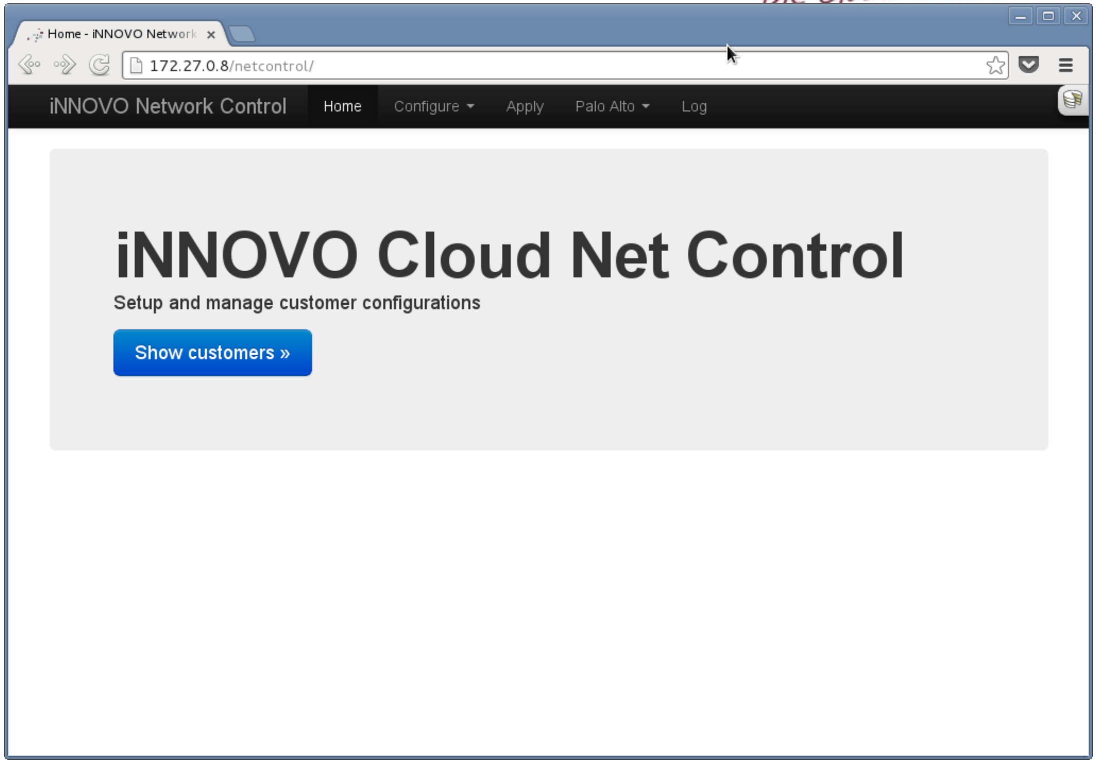
- New vsys
- New vr
- Creates the zones
- Configures the sub-interfaces
- Enables NAT
- Allows outgoing traffic

Manual configuration (GUI): 20 min

Configuration via portal: 1-2 min

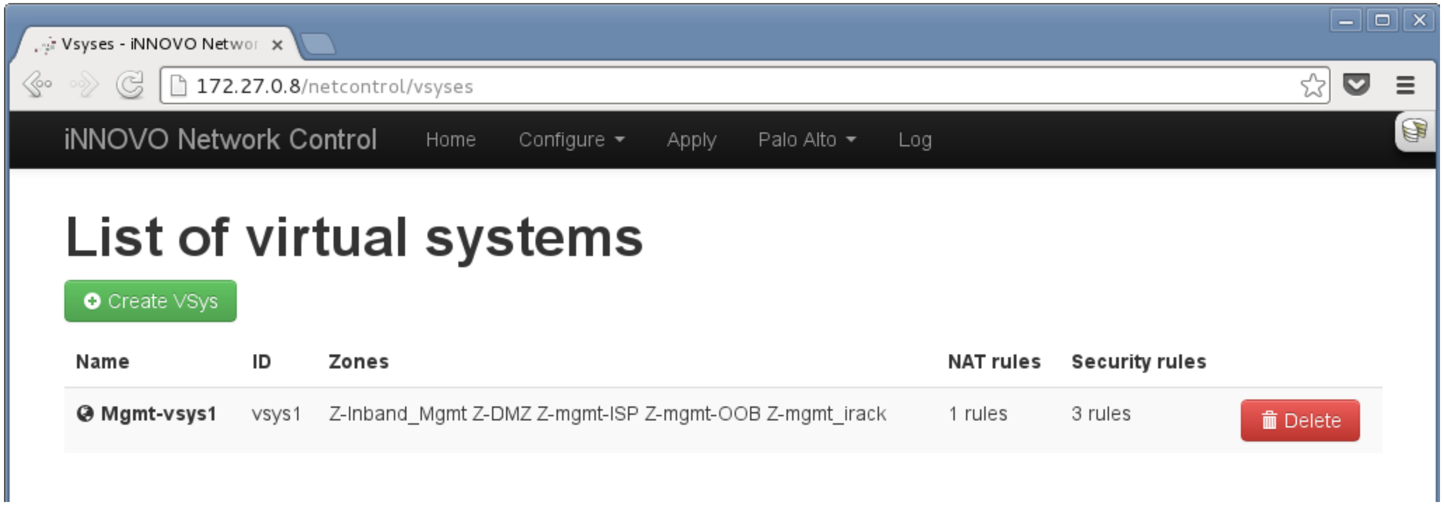
Next steps:

- Switches
- Fully integrate in the OSS and BSS



iNNOVO Cloud Net Control

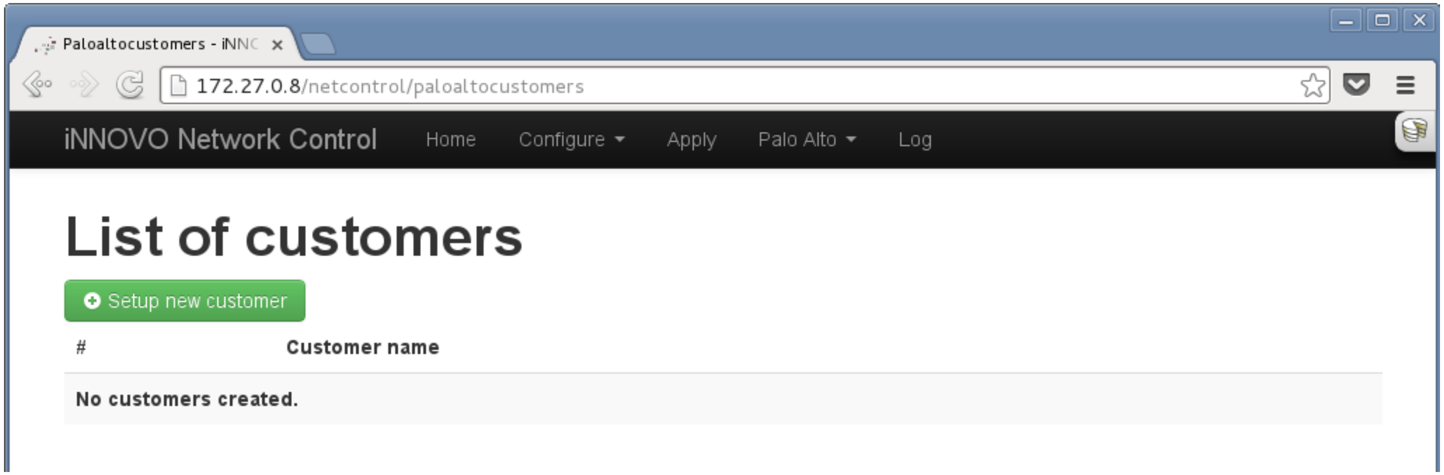
Setup and manage customer configurations



List of virtual systems

Create VSys

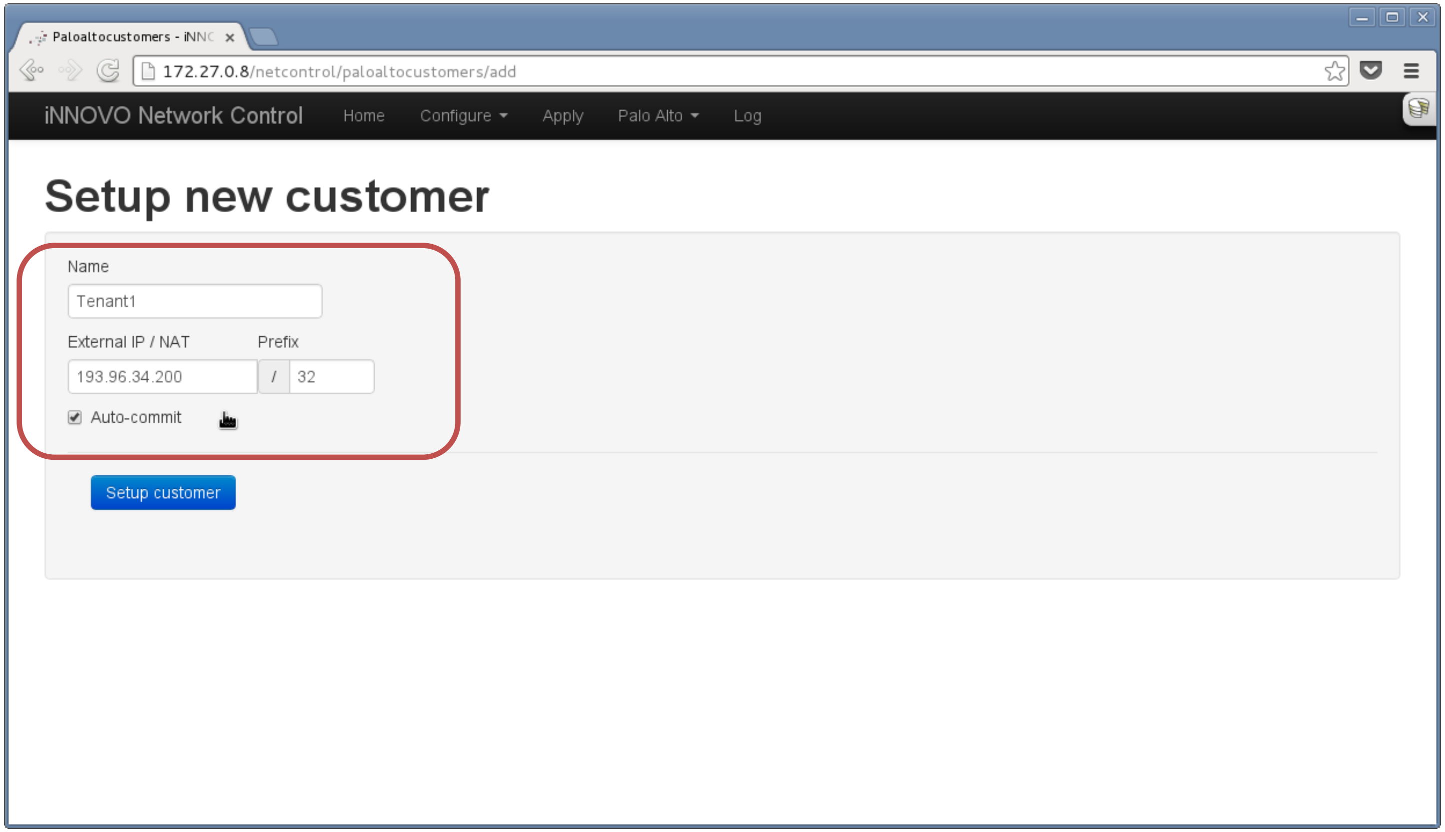
Name	ID	Zones	NAT rules	Security rules	
Mgmt-vsys1	vsys1	Z-Inband_Mgmt Z-DMZ Z-mgmt-ISP Z-mgmt-OOB Z-mgmt_irack	1 rules	3 rules	Delete



List of customers

Setup new customer

#	Customer name
No customers created.	



Setup new customer

Name

Tenant1

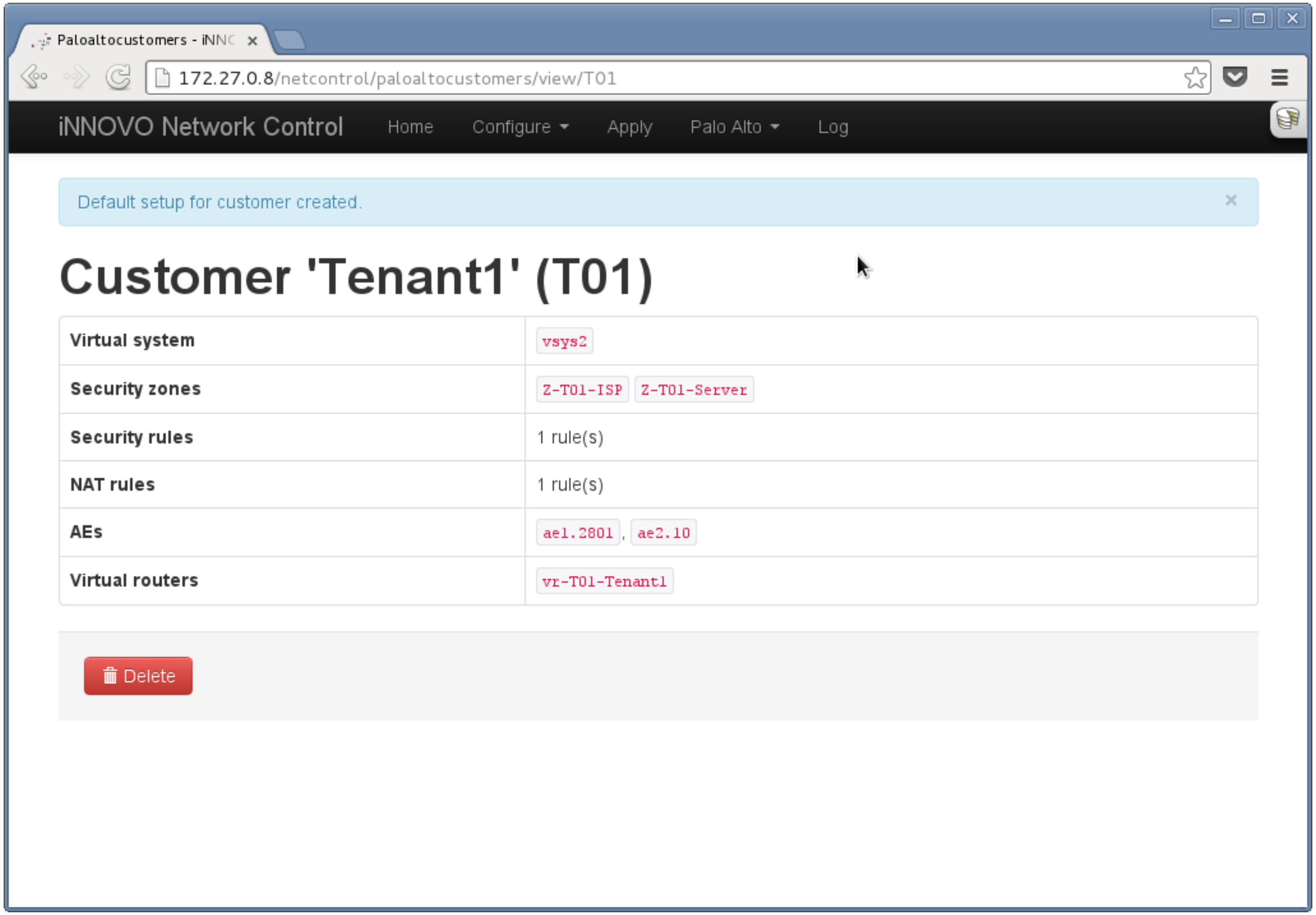
External IP / NAT

193.96.34.200

Prefix

/ 32

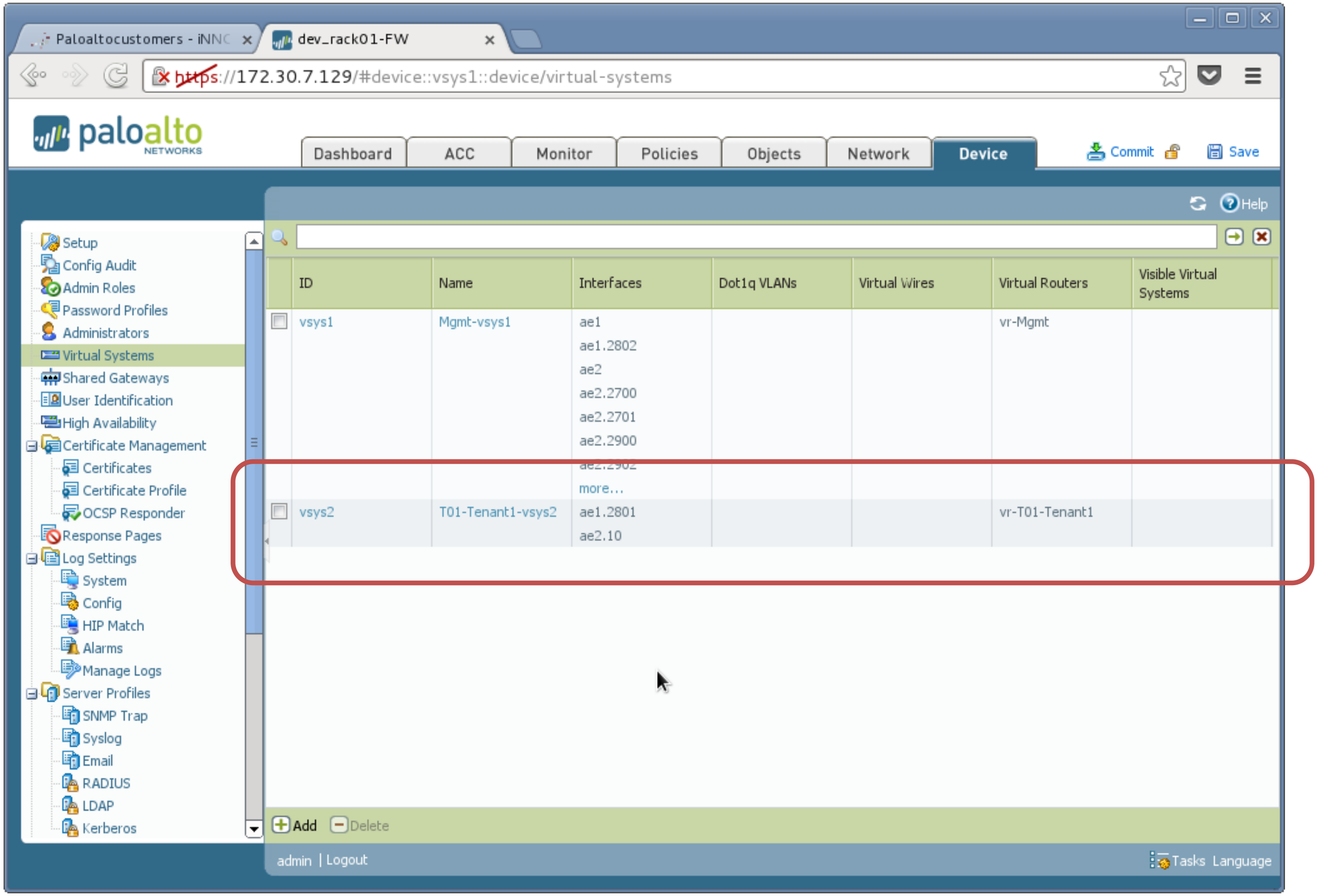
☑ Auto-commit



Default setup for customer created.

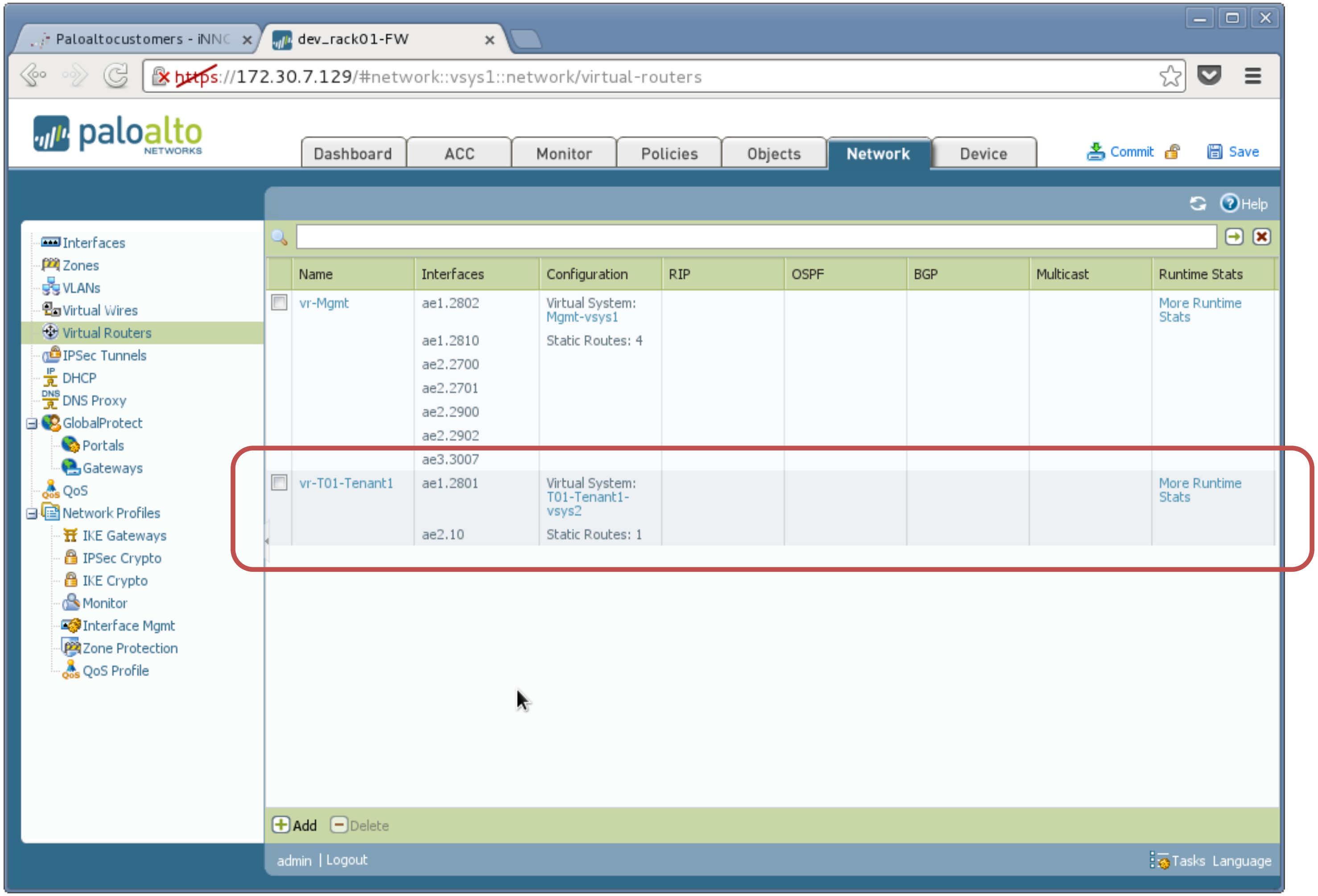
Customer 'Tenant1' (T01)

Virtual system	`vsys2`
Security zones	`Z-T01-ISP` `Z-T01-Server`
Security rules	1 rule(s)
NAT rules	1 rule(s)
AEs	`ae1.2801`, `ae2.10`
Virtual routers	`vr-T01-Tenant1`



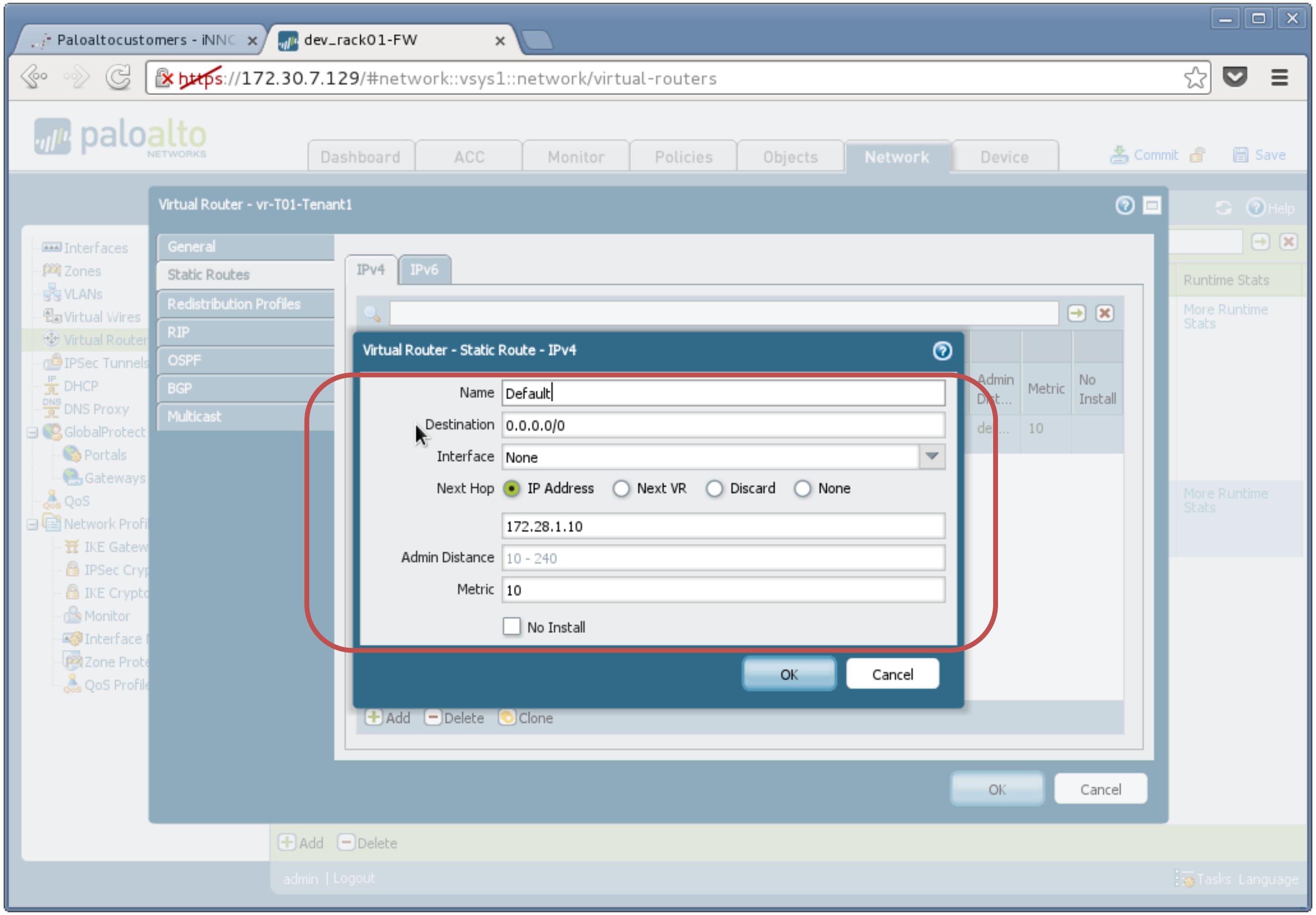
~~https~~://172.30.7.129/#device::vsys1::device/virtual-systems

	ID	Name	Interfaces	Dot1q VLANs	Virtual Wires	Virtual Routers	Visible Virtual Systems
□	vsys1	Mgmt-vsys1	ae1 ae1.2802 ae2 ae2.2700 ae2.2701 ae2.2900 ae2.2902 more...			vr-Mgmt	
□	vsys2	T01-Tenant1-vsys2	ae1.2801 ae2.10			vr-T01-Tenant1	



~~https~~://172.30.7.129/#network::vsys1::network/virtual-routers

	Name	Interfaces	Configuration	RIP	OSPF	BGP	Multicast	Runtime Stats
☐	vr-Mgmt	ae1.2802 ae1.2810 ae2.2700 ae2.2701 ae2.2900 ae2.2902 ae3.3007	Virtual System: Mgmt-vsys1 Static Routes: 4					More Runtime Stats
☐	vr-T01-Tenant1	ae1.2801 ae2.10	Virtual System: T01-Tenant1-vsys2 Static Routes: 1					More Runtime Stats



https://172.30.7.129/#network::vsys1::network/virtual-routers

Virtual Router - vr-T01-Tenant1

Virtual Router - Static Route - IPv4

Name: Default

Destination: 0.0.0.0/0

Interface: None

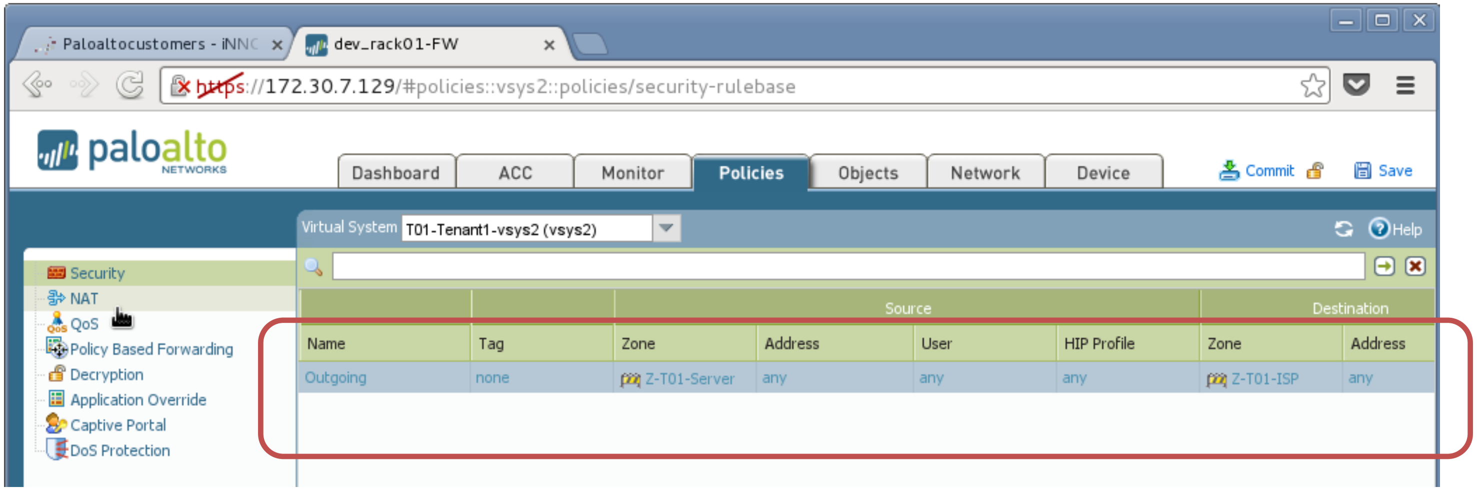
Next Hop: ● IP Address ○ Next VR ○ Discard ○ None

172.28.1.10

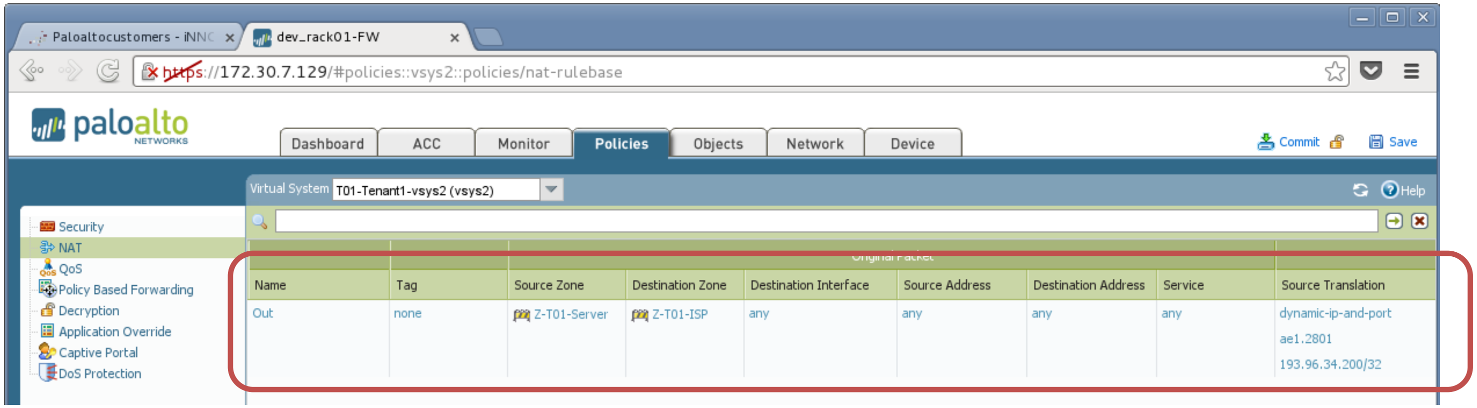
Admin Distance: 10 - 240

Metric: 10

□ No Install



		Source				Destination	
Name	Tag	Zone	Address	User	HIP Profile	Zone	Address
Outgoing	none	Z-T01-Server	any	any	any	Z-T01-ISP	any



		Original Packet						
Name	Tag	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation
Out	none	Z-T01-Server	Z-T01-ISP	any	any	any	any	dynamic-ip-and-port ae1.2801 193.96.34.200/32

iNNOVO CLOUD

Die Cloud beim Kunden

Additional features and short comings

WHISH LIST

Vsys

- vsysadmin can’t see the interfaces
- No individual SNMP context per vsys
  - No individual auth (SNMPv3)
- Can’t use the same IP on different interfaces when in different vr and vsys
- Should be able to configure mgmt interface for different tenants i.e. for LDAP auth and logging

Short comings

- Can’t run SSL and IPsec VPNs on the same external IPs
- No support for openVPN
- When IP is changed on an interface, reference is not cleanly changed on all dependencies
  - Global Protect portal
  - Global protect gateway
  - NAT rules

QUESTIONS

Pablo Endres	<pablo.endres@innovo.cloud.de>
Twitter:	@epablosensei
Blog:	http://www.PabloEndres.com

THANK YOU FOR YOUR TIME