

Best Practice Large Scale Firewall Management

Alexander Holzer
Barracuda Networks

SINOG 24.5.2017



Zero Touch Deployment





Why Zero Touch Deployment?

Large scale rollout

- USB keys require logistics to ensure they arrive in the correct location
- Transport of USB drive is insecure
- Alternatively appliances need to be centrally configured before shipping

Remote locations don't always have onsite technical resources

- Each „store“ doesn't have it's own IT technician or admin

Onsite technical resources cost \$\$\$\$

- This only increases with scale (headcount, accomentation)

Convenience



Zero Touch Deployment

Lean IT

- Zero-touch self-provisioning hardware for rapid deployment
- No on-site IT needed - Ideal for retail
 - Order Box
 - Configure Box Remotely
 - Box Arrives Directly at Location
 - Plug in Box
 - Box Self-Provisioning



Security, Connectivity & Deployment

Simple to deploy and manage

- ZTD builds on Barracuda's industry leading Central Management for Firewalls
- Deploy and manage your entire network from one NextGen Control Centre

Secure

- “Minimal” configuration is send from ZTD to appliance
- Security sensitive full configuration only sent between the CC and Box directly

Variety of Appliances

- ZTD will work for F-Series (Phase 1) and FSC Appliances (Phase 2)

What is needed?

ZTD comes with F-series 7.1 (7.0.2 manufactured) release

- Place an order specified as ZTD or claim on demand
- Works with newly ordered desktop appliances (F18, F80, F82, F180, F280 Rev. B, F380, F400 Rev. B)

Control Center with firmware version 7.1

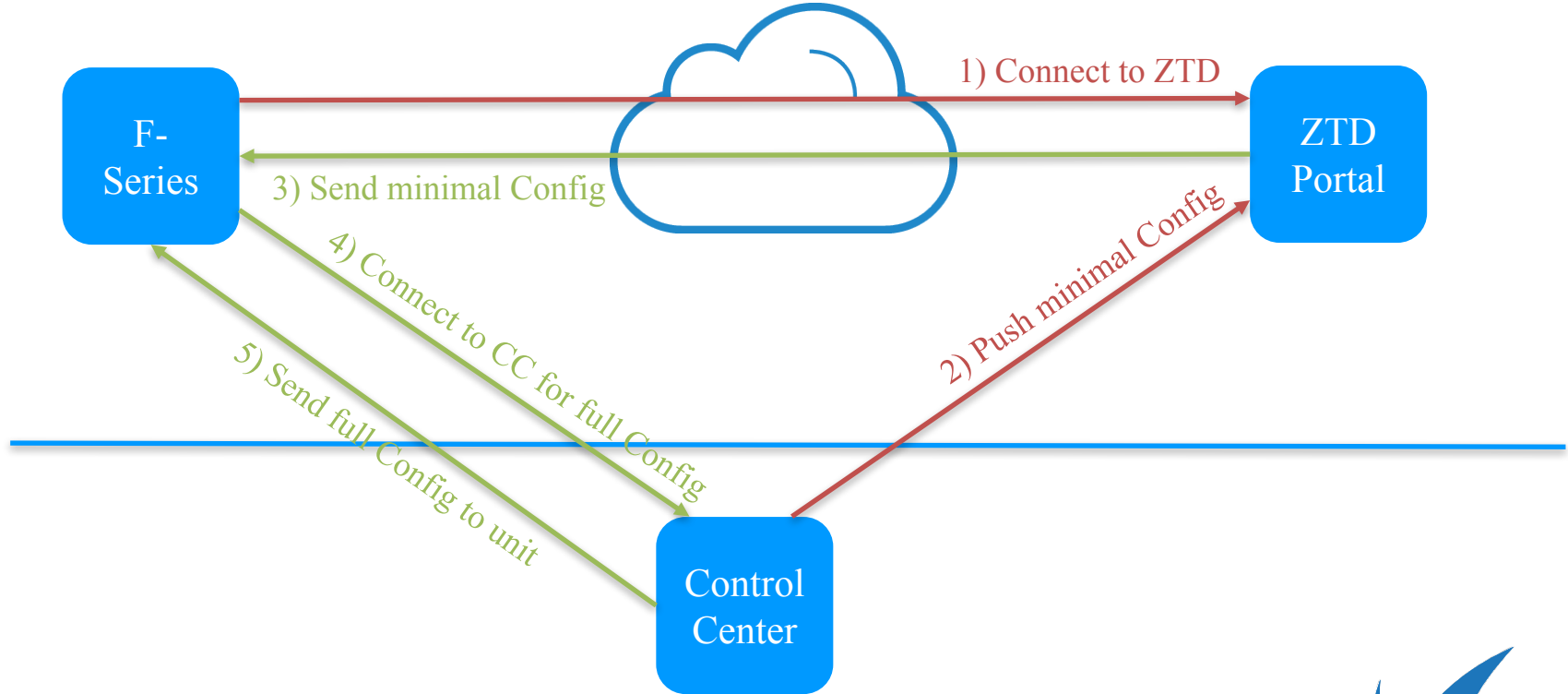
- Using BCC account to link CC to the Zero Touch Deployment Portal

Barracuda Cloud Control Account

- Ordered appliances are linked to customer BCC account



How does it work?

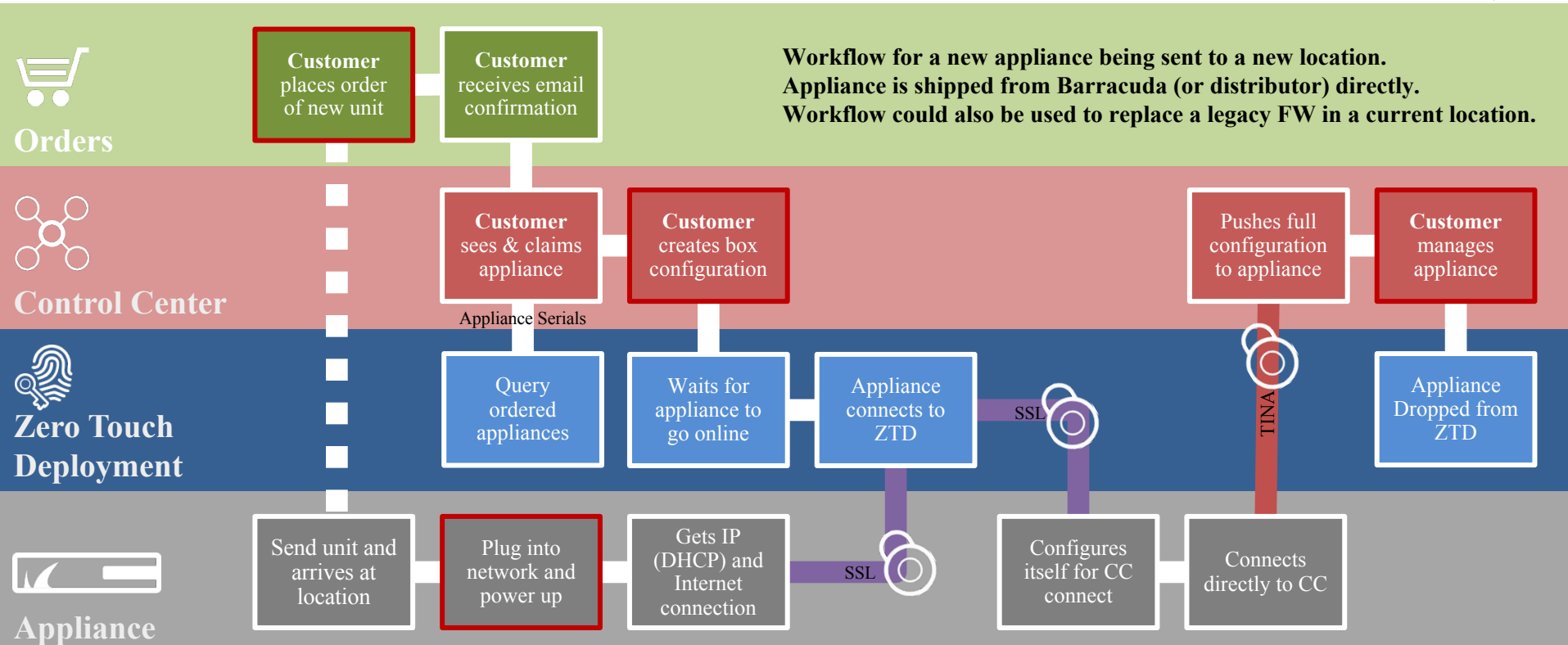


New Box Rollout Workflow

Manual
Action

Automated
Action

Time



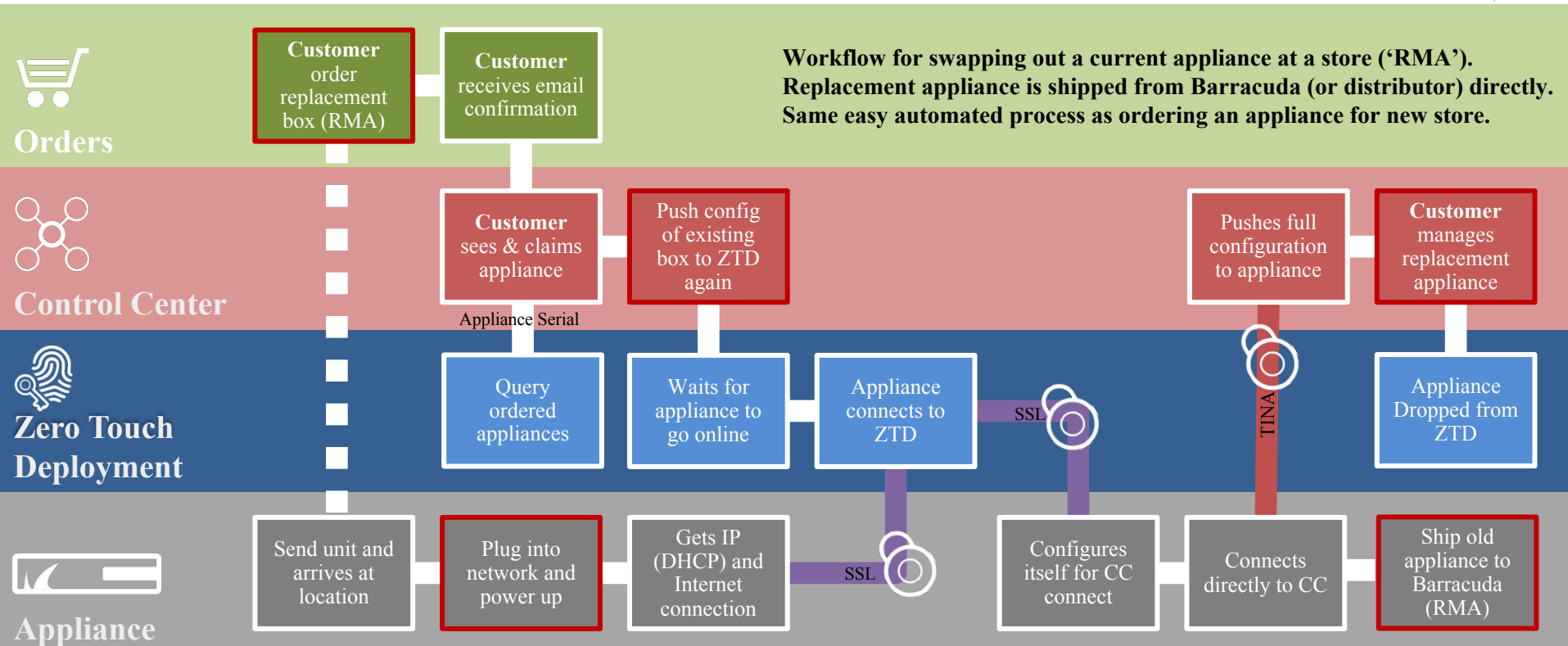
Replacement Box Workflow *

* Coming post 7.1

Manual
Action

Automated
Action

Time



Re-Deployment Box Workflow *

* Original Box must have been ordered post ZTD

GA

Time

Manual
Action

Automated
Action

**Workflow for a re-deployment of an existing appliance (factory defaults).
Same easy automated process as ordering an appliance for new store.**



Orders



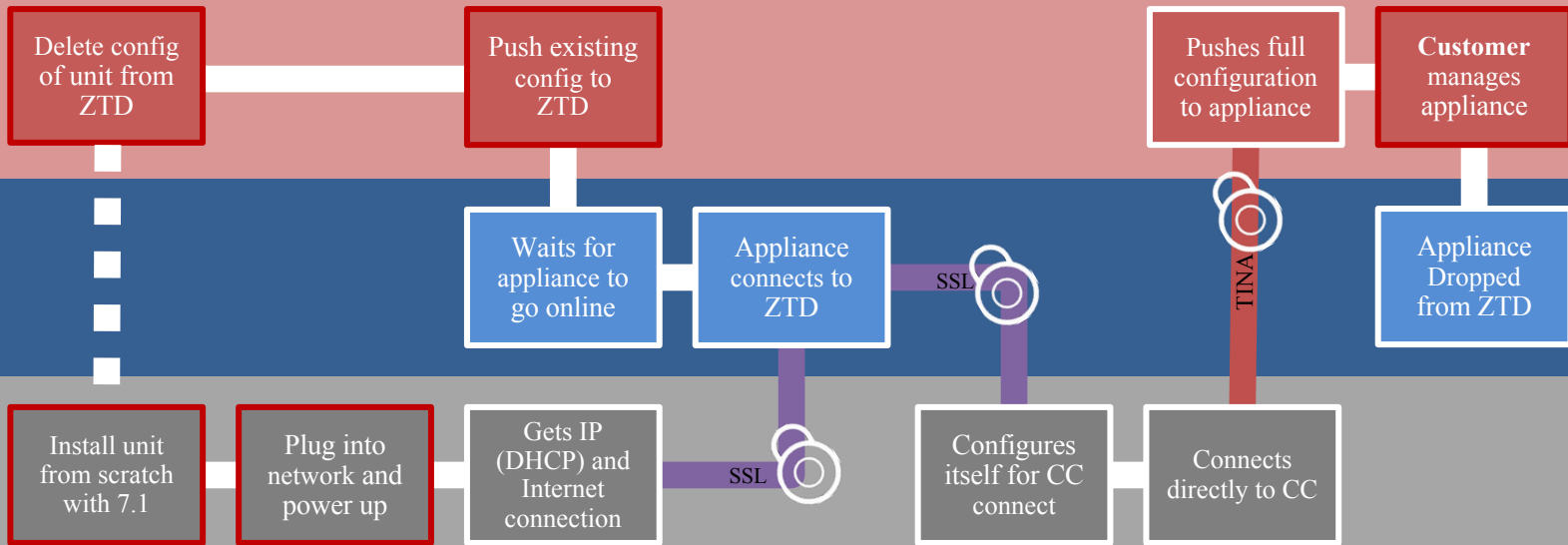
Control Center



Zero Touch
Deployment



Appliance



Manage via the Control Center

OPTIONS 10.17.78.131 QA-EU 10.17.78.131 cc710-zt-131

CONTROL CONFIGURATION DATABASE ADMINS STATISTICS EVENTS NETWORK ACCESS CLIENT

Status Map ZTD Map Geo Maps Configuration Updates File Updates Sessions Barracuda Activation

Appliances and Configurations

Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
Type	Range	Cluster	Box	Serial	Status	Product	Model	Remote IP	
Appliance					In Progress	BNG	F280B		
Appliance					Pending	BNG	F280B		
Configured Appliance	1	1	test1		Completed	BNG	F280B		
Configured Appliance	1	1	test2		Completed	BNG	F280B		

Floating licenses Statistics Collection Remote Execution Scanner Versions Firmware Update Update Tasks

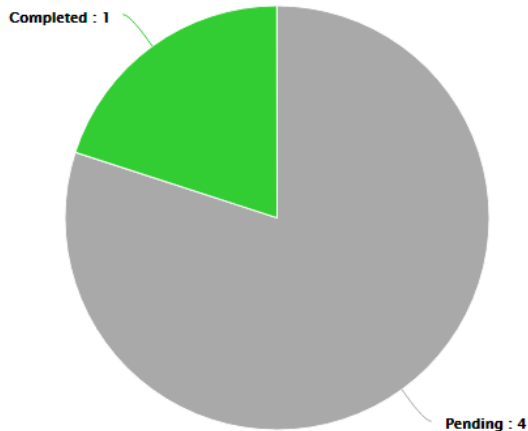
Filter	Filter	Filter	Filter	Filter	Filter	Filter
Local IP	Matching Type	Matching Value	Action applied	Last Seen 03-02-2017 14:56:28	Registered 03-02-2017 14:56:28	Completed 03-02-2017 11:51:00
	Local IP/Subnet		applied	24-01-2017 15:19:10	24-01-2017 15:19:05	24-01-2017 15:25:11
	Serial Number	-----	applied	24-01-2017 16:39:46	24-01-2017 16:39:41	24-01-2017 16:49:40



Monitor via the ZTD Web UI

[Zero Touch Deployment](#)[Dashboard](#)[Appliances](#)[Configurations](#)[Audit Log](#)[Notifications](#)

Appliance Status



Configuration Status

Appliances awaiting Registration and Configuration	4
Appliances awaiting Registration and Configured	0
Appliances Registered and awaiting Configuration	0
Appliances Registered and Configured	0
Appliances completed Configuration	1
Available Configurations	0
Assigned Configurations	0

Recent Activity

Appliance Events

Activity	Product	Serial	Time
Last Claimed	BNG F280B		Mar. 31, 16:44
Last Ignored	-		-
Last Registered	BNG F280B		Mar. 31, 16:55
Last Registered with no Configuration	BNG F280B		Mar. 31, 16:55
Last Assigned Configuration	BNG F280B		Mar. 31, 17:30
Last Unassigned Configuration	BNG F280B		Apr. 04, 11:55
Last Updated	BNG F280B		Mar. 31, 17:36
Last Completed	BNG F280B		Mar. 31, 17:40
Last Failure	-		-
Last Reverted	BNG F280B		Mar. 31, 17:28

Administrative Events

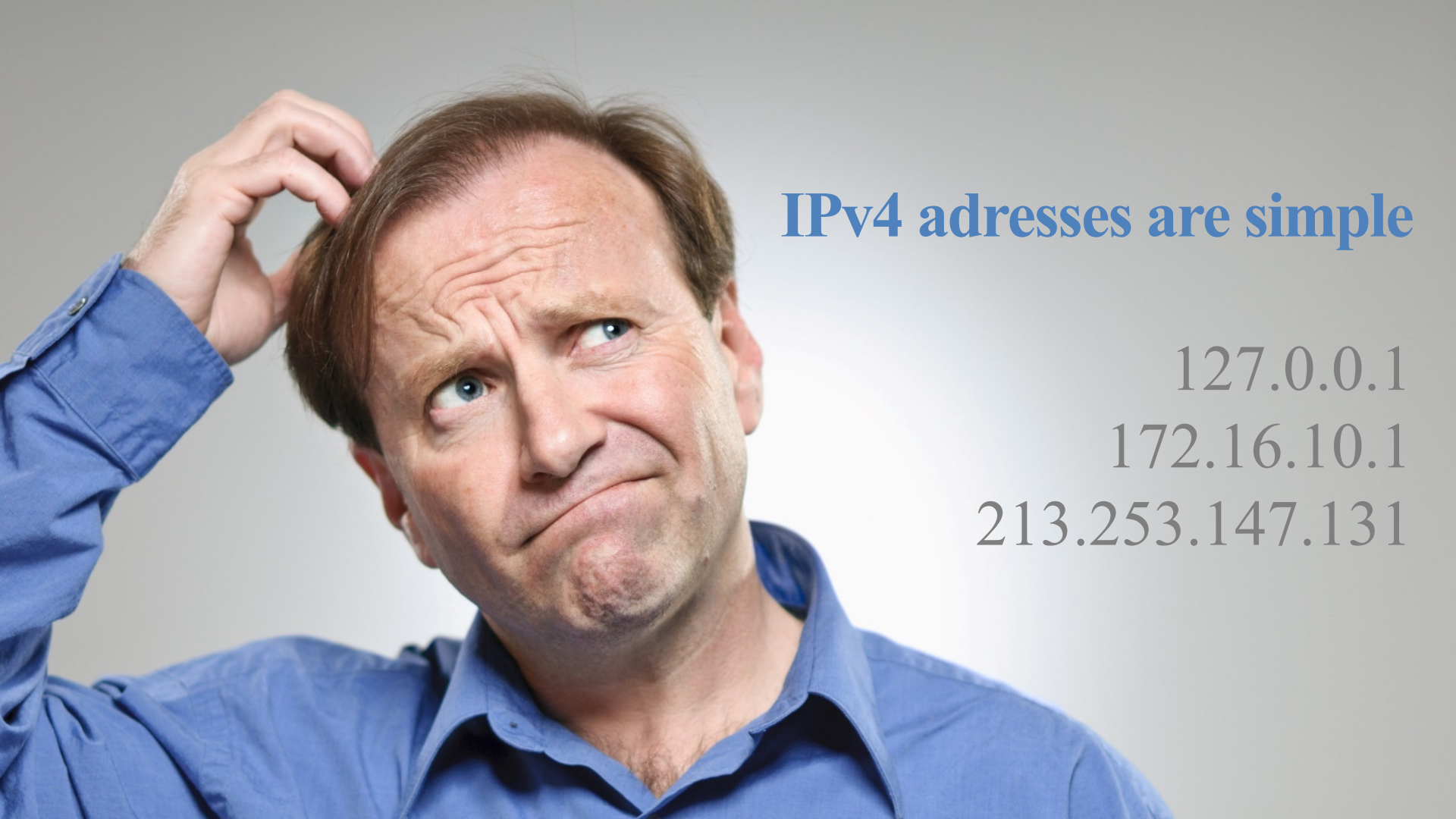
Activity	Name	Time
Last Created Configuration	OQXGXU:1_1_1	Apr. 04, 12:31
Last Deleted Configuration	OQXGXU:1_1_1	Apr. 04, 14:03
Last Created Notification	Completed	Mar. 31, 16:40
Last Deleted Notification	-	-

LIVE DEMO



Named Networks





IPv4 addresses are simple

127.0.0.1

172.16.10.1

213.253.147.131



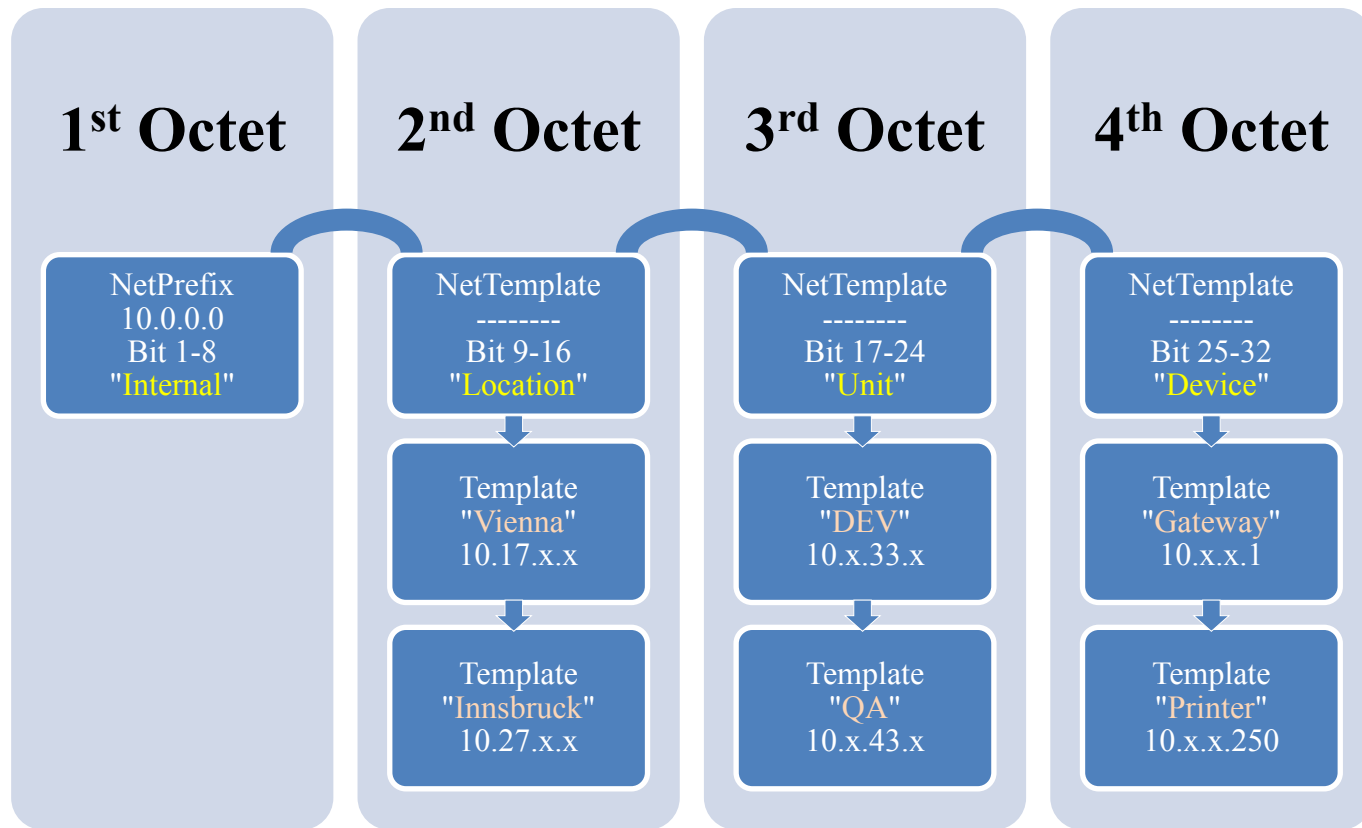
IPv6 addresses are not

2001:0db8:85a3:0000:0000:8a2e:0370:7334

2001:db8:85a3:0:0:8a2e:370:7334

2001:db8:85a3::8a2e:370:7334

IP-less configuration (Named Networks) concept



Named Networks Editor (NextGen-Admin)

Edit Network Prefix Object

Internal
10.*.* StaticBits=1-8

Location
DynBits=9-16

Values

Vienna

10.17.*.*.*.*.*.*.*.*

Innsbr...

10.27.*.*

Unit
DynBits=17-24

Values

DEV

10.*.33.*.*.*.*.*.*

QA

10.*.43.*

Device
DynBits=25-32

Values

Gateway

10.*.*.1.*.*.*.*.*.*

Printer

10.*.*.250

Named Networks Editor (NextGen-Admin)

Edit/Create Network Object

General

Type: Generic IPv4 Network Object (IP, Network, Ranges) ▼

Name: Resolve

Description:

Network Color:

Include Entries

IP / Ref / Geo

Internal/Innsbruck/<ANY>Unit/Gateway 10.27.0.1/255.255.0.255

Exclude Entries

IP / Ref / Geo

Comment

☐ Enable L3 Pseudo Bridging

OK Cancel

Add Prefix

10.27.0.1/255.255.0.255

Prefix: Internal ▼

Location: Innsbruck ▼

Unit: <ANY> ▼

Device: Gateway ▼

OK Cancel



Named Networks Visibility

A..	Org	IP Pr...	Last	Rule	Source	Src. Prefix	Interface	Destination	Output-IF	Application	URL Category
	FWD	TCP	22h 01m 11s	<App>:Advertisement-BLOCK	172.16.20.221	corp/EU/Innsbruck/Finance/PC	eth1	216.58.214.206		Google Analytics	Computing/Technology
	FWD	TCP	22h 30m 50s	drop	172.16.20.221	corp/EU/Innsbruck/Finance/PC	eth1	216.58.214.206			
	FWD	TCP	4d 05h 57m 55s	<App>:Advertisement-BLOCK	172.16.20.221	corp/EU/Innsbruck/Finance/PC	eth1	216.58.214.232		Google Analytics	Computing/Technology
	FWD	TCP	6d 02h 18m 49s	drop	172.16.20.221	corp/EU/Innsbruck/Finance/PC	eth1	93.184.220.70			
	FWD	TCP	6d 02h 26m 45s	<App>:Advertisement-BLOCK	172.16.20.221	corp/EU/Innsbruck/Finance/PC	eth1	216.58.214.200		Google Analytics	Computing/Technology
	FWD	TCP	6d 03h 21m 16s	<App>:Advertisement-BLOCK	172.16.20.221	corp/EU/Innsbruck/Finance/PC	eth1	216.58.209.200		Google Analytics	Computing/Technology
	FWD	TCP	6d 05h 11m 10s	drop	172.16.20.221	corp/EU/Innsbruck/Finance/PC	eth1	40.127.129.109			
	FWD	TCP	6d 05h 11m 10s	<App>:Skype-BLOCK	172.16.20.221	corp/EU/Innsbruck/Finance/PC	eth1	40.127.129.109		Skype General	Computing/Technology
	FWD	TCP	7d 01h 16m 51s	F301	172.16.20.221	corp/EU/Innsbruck/Finance/PC	eth1	64.235.144.94	eth0		
	FWD	TCP	7d 05h 13m 00s	drop	172.16.20.221	corp/EU/Innsbruck/Finance/PC	eth1	216.58.214.232			
	FWD	TCP	13d 00h 38m 55s	F301	172.16.20.221	corp/EU/Innsbruck/Finance/PC	eth1	199.16.156.52	eth0		
	IPRX	TCP	13d 00h 38m 55s	<App>:Web-Surfing	172.16.20.221	corp/EU/Innsbruck/Finance/PC	eth1	199.16.156.52		Twitter Base	Social Networking
	FWD	TCP	13d 00h 38m 56s	F301	172.16.20.221	corp/EU/Innsbruck/Finance/PC	eth1	31.13.64.35	eth0		
	IPRX	TCP	13d 00h 38m 56s	<App>:Facebook	172.16.20.221	corp/EU/Innsbruck/Finance/PC	eth1	31.13.64.35		Facebook SocialPlugins	Social Networking
	IPRX	TCP	13d 00h 38m 56s	<App>:Google	172.16.20.221	corp/EU/Innsbruck/Finance/PC	eth1	216.58.214.238		Google API	Search Engines/Portals
	IPRX	TCP	13d 00h 38m 56s	<App>:Advertisement-BLOCK	172.16.20.221	corp/EU/Innsbruck/Finance/PC	eth1	216.58.214.238		Google Analytics	Computing/Technology
	FWD	TCP	13d 00h 38m 56s	F301	172.16.20.221	corp/EU/Innsbruck/Finance/PC	eth1	216.58.214.238	eth0		
	IPRX	TCP	13d 00h 39m 30s	<App>:Web-Surfing	172.16.20.221	corp/EU/Innsbruck/Finance/PC	eth1	52.43.9.103		Web browsing	Software/Hardware
	FWD	TCP	13d 00h 39m 33s	F301	172.16.20.221	corp/EU/Innsbruck/Finance/PC	eth1	52.43.9.103	eth0		
	IPRX	TCP	13d 00h 39m 57s	<App>:Google	172.16.20.221	corp/EU/Innsbruck/Finance/PC	eth1	216.58.209.174		Google Safe Browsing	Search Engines/Portals
	FWD	TCP	13d 00h 39m 58s	F301	172.16.20.221	corp/EU/Innsbruck/Finance/PC	eth1	216.58.209.174	eth0		
	FWD	TCP	13d 00h 39m 58s	F301	172.16.20.221	corp/EU/Innsbruck/Finance/PC	eth1	172.217.22.238	eth0		
	IPRX	TCP	13d 00h 39m 58s	<App>:Google	172.16.20.221	corp/EU/Innsbruck/Finance/PC	eth1	172.217.22.238		Google Safe Browsing	Search Engines/Portals
	IPRX	TCP	13d 01h 06m 53s	<App>:Web-Surfing	172.16.20.221	corp/EU/Innsbruck/Finance/PC	eth1	52.218.144.74		Amazon Webservices	Content Server
	IPRX	TCP	13d 01h 06m 53s	<App>:Web-Surfing	172.16.20.221	corp/EU/Innsbruck/Finance/PC	eth1	192.0.73.2		Web browsing	Computing/Technology
	IPRX	TCP	13d 01h 06m 55s	<App>:Google	172.16.20.221	corp/EU/Innsbruck/Finance/PC	eth1	216.58.214.227		Google Services Base	Content Server

Named Networks advantages

- Structure and flexible masks for IPv4 (v7.1) & IPv6 (v7.2)
- Support for Host and Networks
- Binary presentation and integrated conversion (hex/dec)
- Built-in “Subnet Calculator” in NG Admin
- Visualization with names instead numbers (Troubleshooting)
- Set on single Bits (not fixed to octets xxxx.yyyy.xxxx.yyyy)
- Fit into existing and growing network topologies



Thank You



Screen Shots



Managed via the Control Center

OPTIONS + 10.17.78.131 QA-EU 10.17.78.131 cc710-zt-131

CONTROL CONFIGURATION DATABASE ADMINS STATISTICS EVENTS NETWORK ACCESS CLIENT

Status Map ZTD Map Geo Maps Configuration Updates File Updates Sessions Barracuda Activation

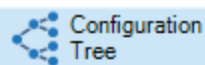
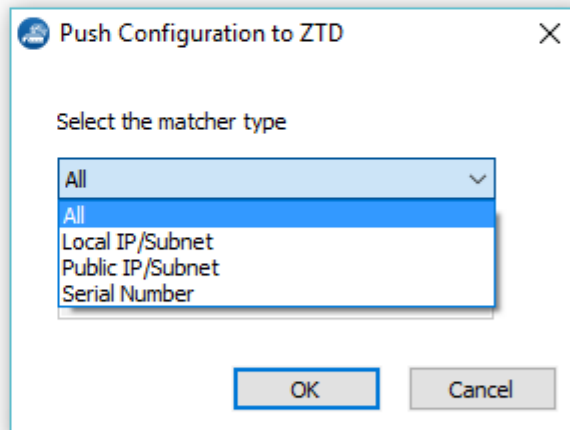
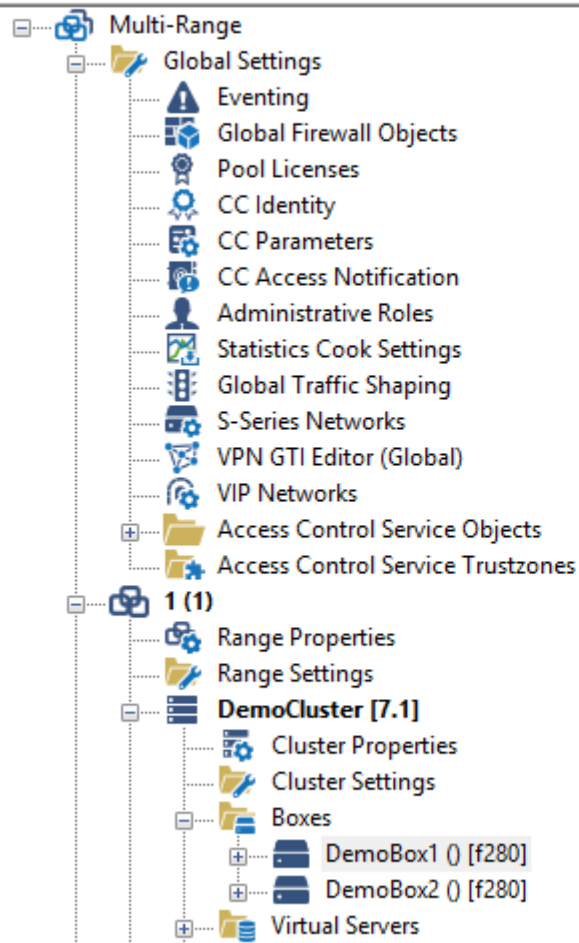
Appliances and Configurations

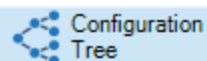
▼ Filter	Filter	Filter	Filter	Filter	▼ Filter	Filter	Filter	Filter
Type	Range	Cluster	Box	Serial	Status	Product	Model	Remote IP
Appliance					In Progress	BNG	F280B	
Appliance					Pending	BNG	F280B	
Configured Appliance	1	1	test1		Completed	BNG	F280B	
Configured Appliance	1	1	test2		Completed	BNG	F280B	

Floating licenses Statistics Collection Remote Execution Scanner Versions Firmware Update Update Tasks

Filter	Filter	Filter	Filter	Filter	Filter	Filter
Local IP	Matching Type	Matching Value	Action applied	Last Seen 03-02-2017 14:56:28	Registered 03-02-2017 14:56:28	Completed 03-02-2017 11:51:00
	Local IP/Subnet		applied	24-01-2017 15:19:10	24-01-2017 15:19:05	24-01-2017 15:25:11
	Serial Number	-----	applied	24-01-2017 16:39:46	24-01-2017 16:39:41	24-01-2017 16:49:40



Configuration
TreeCC
IdentityCC
Parameters



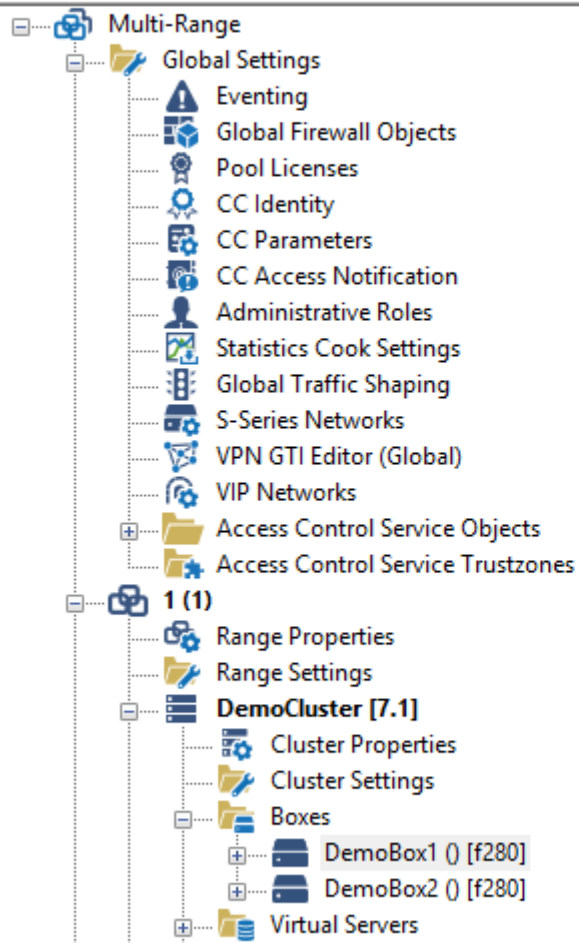
Configuration Tree



CC Identity



CC Parameters



Push Configuration to ZTD

Select the matcher type

Serial Number

Enter the matching value

831955

831955

832793

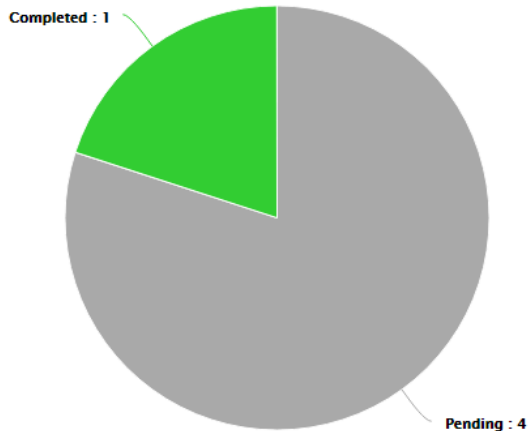
OK Cancel



Viewed via the ZTD Web UI

[Zero Touch Deployment](#)[Dashboard](#)[Appliances](#)[Configurations](#)[Audit Log](#)[Notifications](#)

Appliance Status



Configuration Status

Appliances awaiting Registration and Configuration	4
Appliances awaiting Registration and Configured	0
Appliances Registered and awaiting Configuration	0
Appliances Registered and Configured	0
Appliances completed Configuration	1
Available Configurations	0
Assigned Configurations	0

Recent Activity

Appliance Events

Activity	Product	Serial	Time
Last Claimed	BNG F280B		Mar. 31, 16:44
Last Ignored	-		-
Last Registered	BNG F280B		Mar. 31, 16:55
Last Registered with no Configuration	BNG F280B		Mar. 31, 16:55
Last Assigned Configuration	BNG F280B		Mar. 31, 17:30
Last Unassigned Configuration	BNG F280B		Apr. 04, 11:55
Last Updated	BNG F280B		Mar. 31, 17:36
Last Completed	BNG F280B		Mar. 31, 17:40
Last Failure	-		-
Last Reverted	BNG F280B		Mar. 31, 17:28

Administrative Events

Activity	Name	Time
Last Created Configuration	OQXGXU:1_1_1	Apr. 04, 12:31
Last Deleted Configuration	OQXGXU:1_1_1	Apr. 04, 14:03
Last Created Notification	Completed	Mar. 31, 16:40
Last Deleted Notification	-	-

Serial ▼

+

-

Apply

Copy

CSV

PDF

Claim Appliance

Serial ^	Product	Model	Version	Status	Action	Configuration	Public IP	Registered	Last Seen	Actions
	BNG	F280B	7.0.2	Pending						Ignore
	BNG	F280B	7.0.2-094	Completed				2017-03-31 16:55	2017-03-31 17:36	Ignore
	BNG	F280	7.1.0	Pending						Ignore
	BNG	VF500	7.1.0	Pending						Ignore
	BNG	VF500B	7.1.0	Pending						Ignore

Showing 1 to 5 of 5 entries

Previous

1

Next



Created ▾

All Time ▾

+

-

Apply

Copy

CSV

PDF

Created ▾	Type	Name	Serial	Description	Status	Public IP	Administrator
2017-04-04 14:03	Administrator Action	Delete Configuration		Deleted Configuration for 'BNG', model 'F10', supported on version '7.0' and above. Checksum was '+RMYPfXn+SR2nQs5unwXADymR+m1KbPZh9NqR9pRz8l='.	Successful		@hotmail.co.uk
2017-04-04 12:31	Administrator Action	Create Configuration		Created Configuration for 'BNG', model 'F10', supported on version '7.0' and above. Checksum was '+RMYPfXn+SR2nQs5unwXADymR+m1KbPZh9NqR9pRz8l='.	Successful		@hotmail.co.uk
2017-04-04 12:21	Administrator Action	Delete Configuration		Deleted Configuration for 'BNG', model 'F280B', supported on version '7.0' and above. Checksum was '7+OkS2+7n2bFvpe4qNVJIT6waJCEQX9DgJg3leZklKw='.	Successful		@hotmail.co.uk
2017-04-04 12:19	Administrator Action	Create Configuration		Created Configuration for 'BNG', model 'F280B', supported on version '7.0' and above. Checksum was '7+OkS2+7n2bFvpe4qNVJIT6waJCEQX9DgJg3leZklKw='.	Successful		@hotmail.co.uk

Name ▾

+

-

Apply

Copy

CSV

PDF

Add Notification

Name ^	Events	Status	Administrators	Actions
completed	Appliance Completed	All	@barracuda.com	Edit Delete

Showing 1 to 1 of 1 entries

Previous

1

Next

