
Barracuda
TECHSUMMIT19
BARRACUDA TECHNICAL SUMMIT
Barracuda Firewall Insights
CloudGen Firewall Firmware 7.2.4 > 8.0.1


I need a … Report !

Reporting Overview

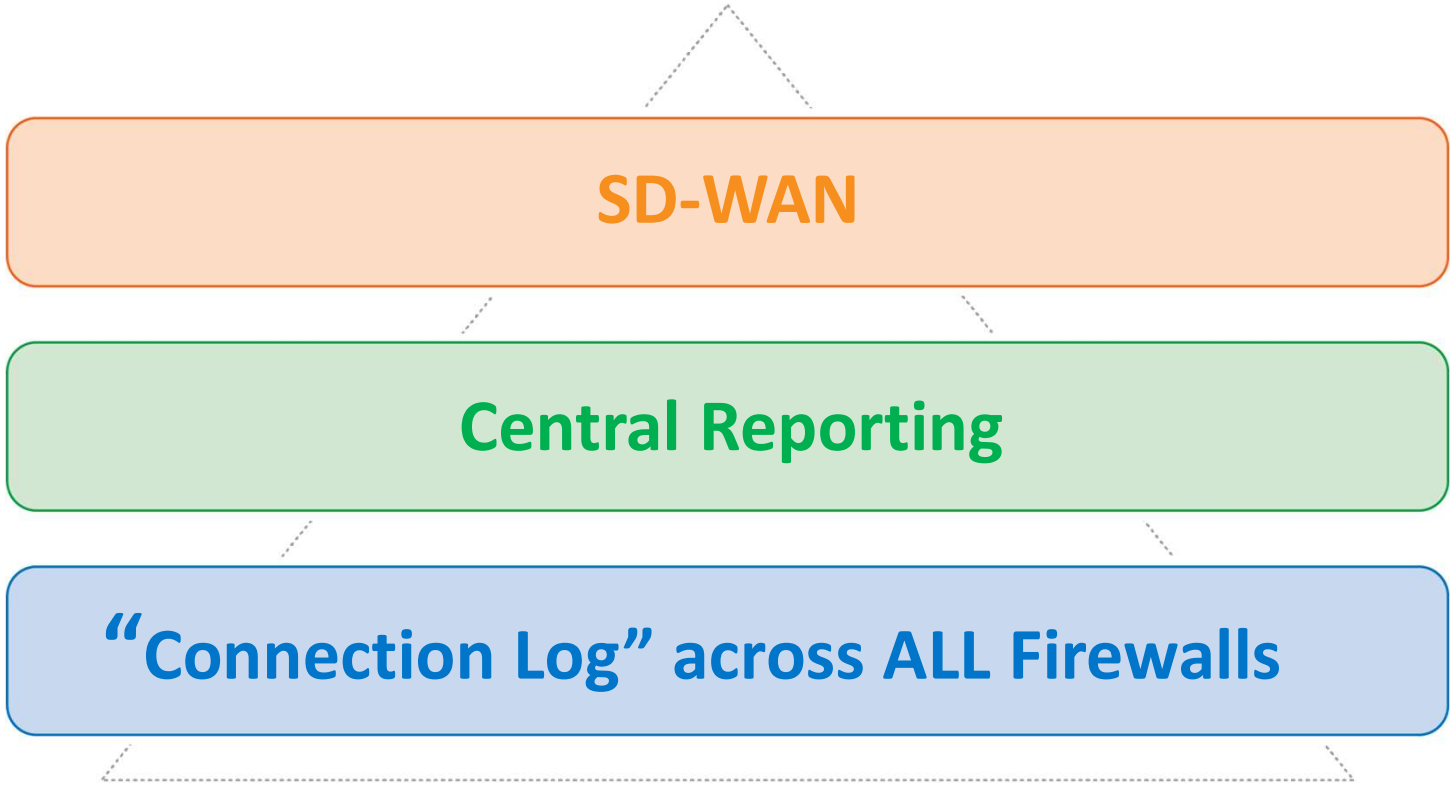
- Challenges
  - Limited retention on firewall
  - Real-time information
  - Easy data flow and analysis

Firewall Insights

Report Creator

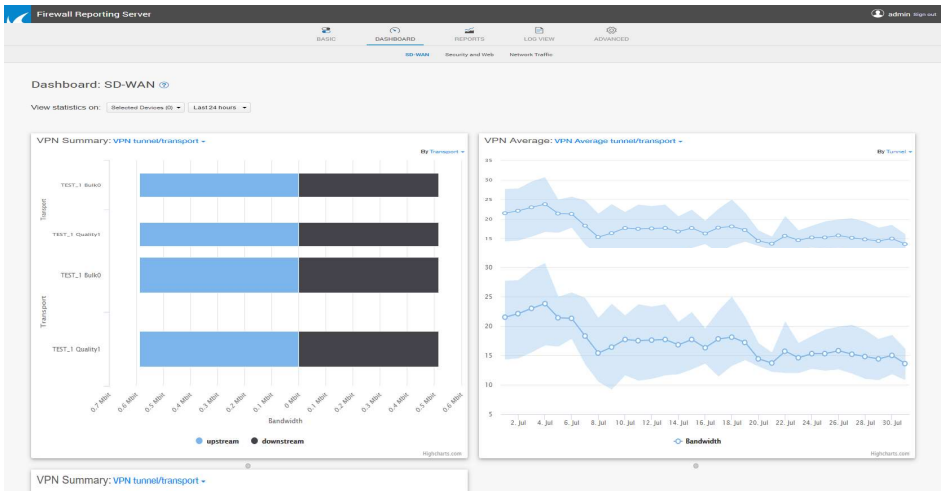
Firewall Admin Dashboards

Firewall Insights



Firewall Advanced Reporting

- Long-term reporting for hundreds of firewalls
- Tight integration with CloudGen Firewall family
- New SD-WAN and WAN reporting



Firewall Insights - Features

- Firewall dashboards
  - SD-WAN
  - Web and security
  - Firewall traffic
- Reports
  - Scheduled and on-demand
  - HTML, PDF, TXT, and CSV formats
- Log Viewer
  - Long-term Firewall History / Threat Monitor across all connected firewalls

Firewall Insights Sizing

- Supported virtualization: KVM, VMware, Hyper-V

	Virtualization			
Product Model	SMALL	MEDIUM	LARGE	X-LARGE
Virtual Cores	8	12	16	32
Min. RAM	32 GB	64 GB	128 GB	512 GB
Min. SSD	2 TB	6 TB	10 TB	20 TB

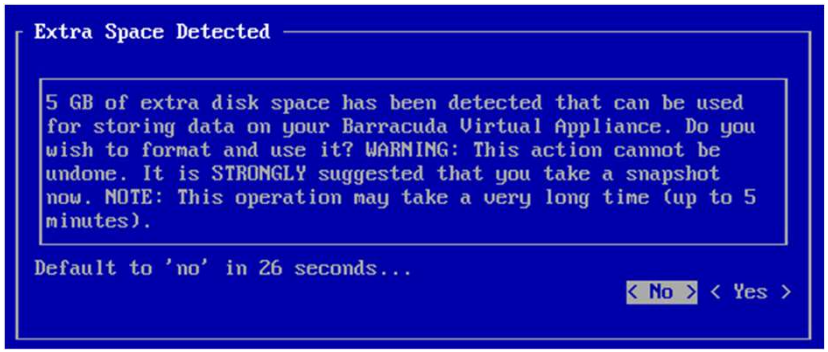
Deployment

1) Download the Insights image from the Download Portal
2) Deploy Firewall Insights on a supported hypervisor

	Virtualization			
	Vmware ESXi	Hyper-V	KVM	Proxmox
Image Format	*.ova	*.vhd	*.kvm.zip	*.tar.gz
Min.System Requirements	5.5.0 + ALL updates		5.4.2 or higher	
Recommendations	• Disk format: Thick provisioned format • More IOPS		Free IP address: 192.168.200.200	

Getting Started

- Log into your machine on console
  - All available data storage will be used automatically on boot



- Log into Firewall Insights
  - admin / admin
- Enter network settings
  - Automatically reboot
- Enter the license token for Barracuda Firewall Insights
  - Automatically reboot

Checklist

- Email notifications
- License
- Network
- How to stream data
  - Ports
  - Remote management tunnel

Licensing

- Barracuda Firewall Insights server

> The only restriction is the system performance

- A Barracuda Firewall Insights subscription on every CGF

box					
bdns	2	16	149456	Caching-DNS	
boxconfig	4	21	97120	Config	
boxfw	18	138	3004432	Host-Firewall	
brsd	1	7	13432	Firewall Insights	Firewall Insights is not licensed
bsms	1	4	5748	SMS-Control	
bsnmp	1	4	12208	SNMP-Service	

Supported CGFs

CGF “Firewall Insights“ subscription

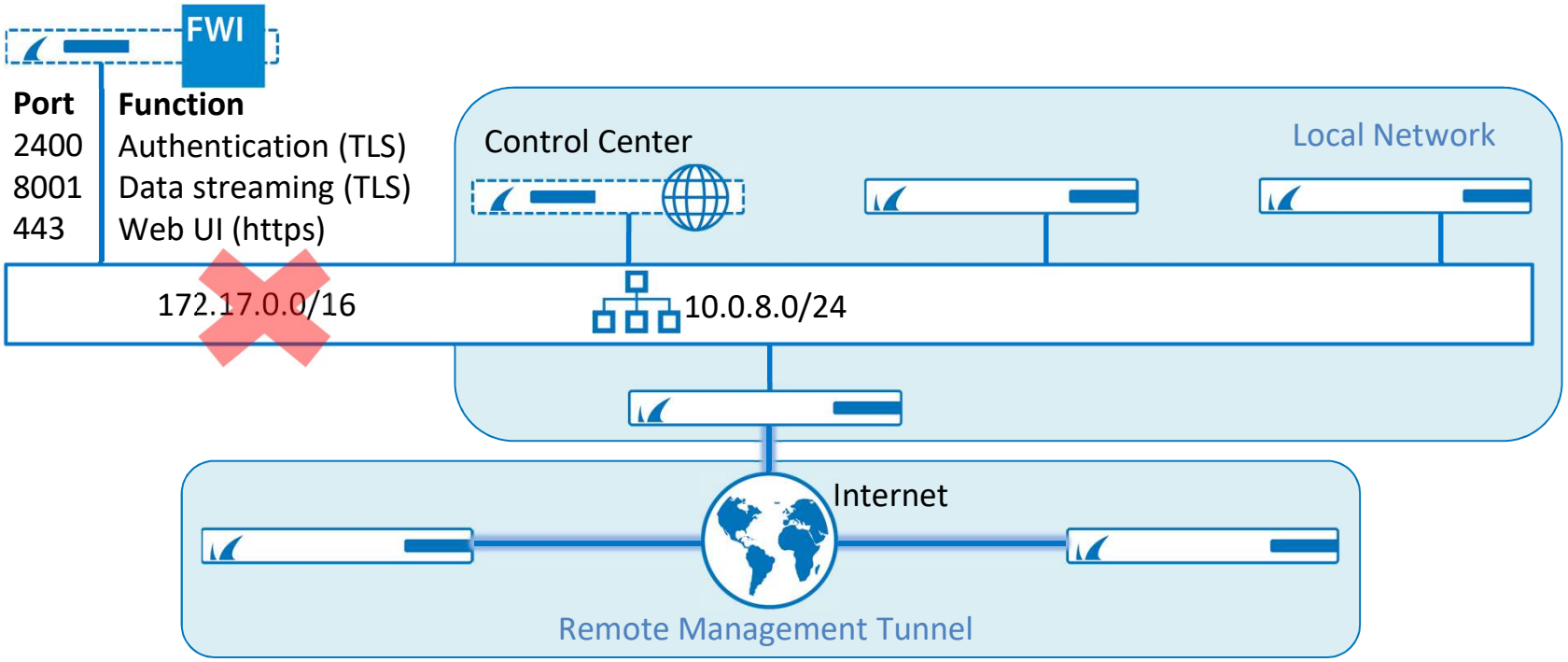
CGF firmware > 7.2.4, > 8.0.1

Hardware

Virtual Systems (Vx)

Public Cloud

Network


FWI
Port
Function
2400
Authentication (TLS)
8001
Data streaming (TLS)
443
Web UI (https)
Control Center
Local Network
172.17.0.0/16
10.0.8.0/24
Internet
Remote Management Tunnel

Network Restrictions

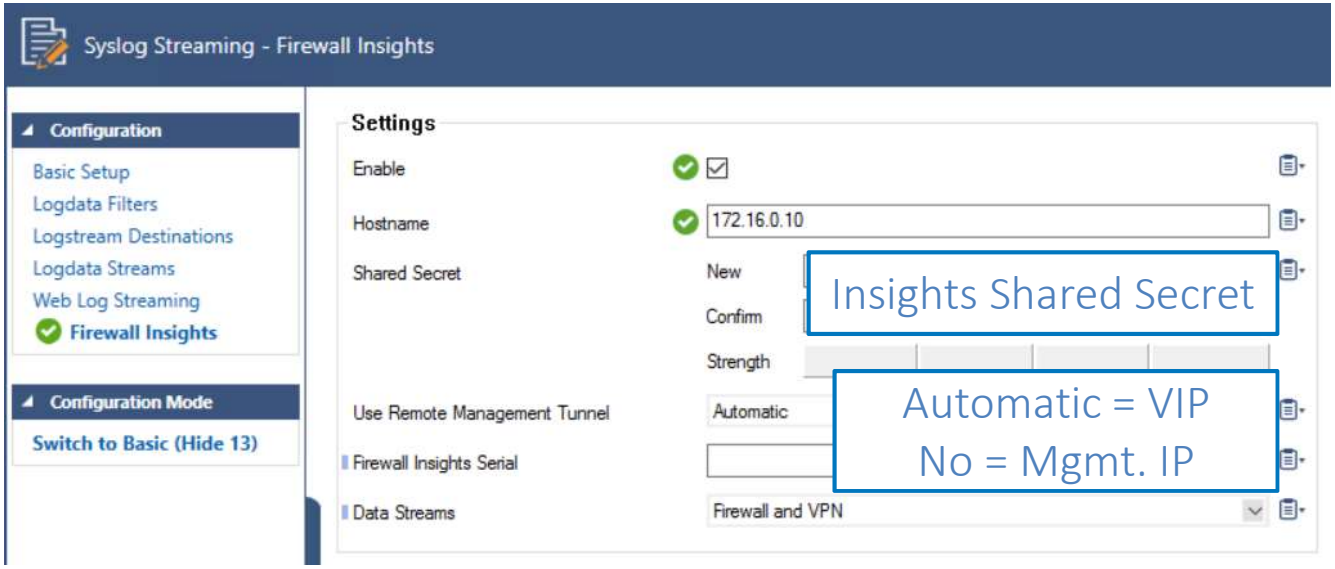
- Unique stand-alone firewall host names
  - Range / Cluster / Host Name
- Only one Control Center per Insights supported
- CGF HA clusters are displayed as a single unit
  - Primary firewall name

Which Data Are Forwarded to Insights?

- Firewall activity data
  - No Blocking Access Rules !
- SD-WAN data
- Threat log

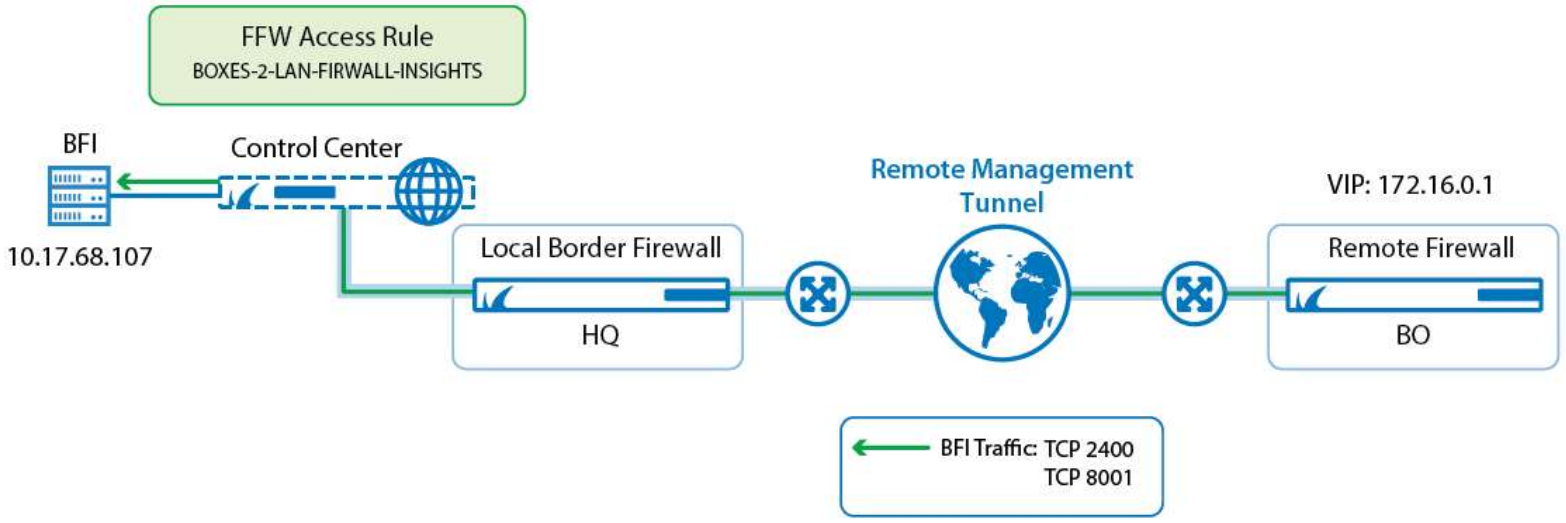
CGF Configuration

- Configure Firewall Insights in syslog streaming
- Control Center -> Use repository links



Remote Management Tunnel

- Newly deployed CC with firmware 7.2.4 or higher
- Migrate a CC to firmware 7.2.4 or higher

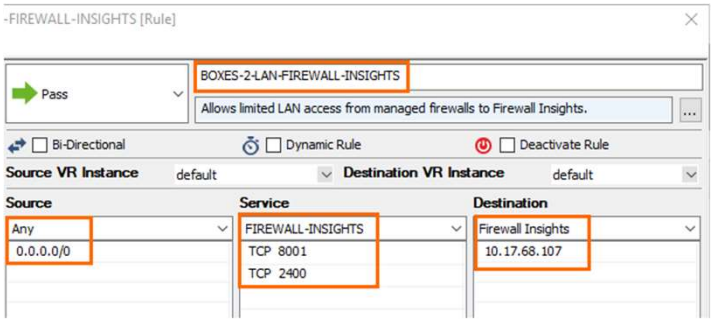


Remote Management Tunnel

- Newly deployed CC with firmware 7.2.4 or higher
- CC preconfigured configuration:
  - Service object 'FIREWALL-INSIGHTS‘
  - Network object 'FIREWALL-INSIGHTS‘
  - NOTE: You must fill in the “Insights Srv IP” manually
  - Forwarding access rule ‘BOXES-2-LAN-FIREWALL-INSIGHTS'
- Add Firewall Insights to the remote network addresses

Remote Management Tunnel

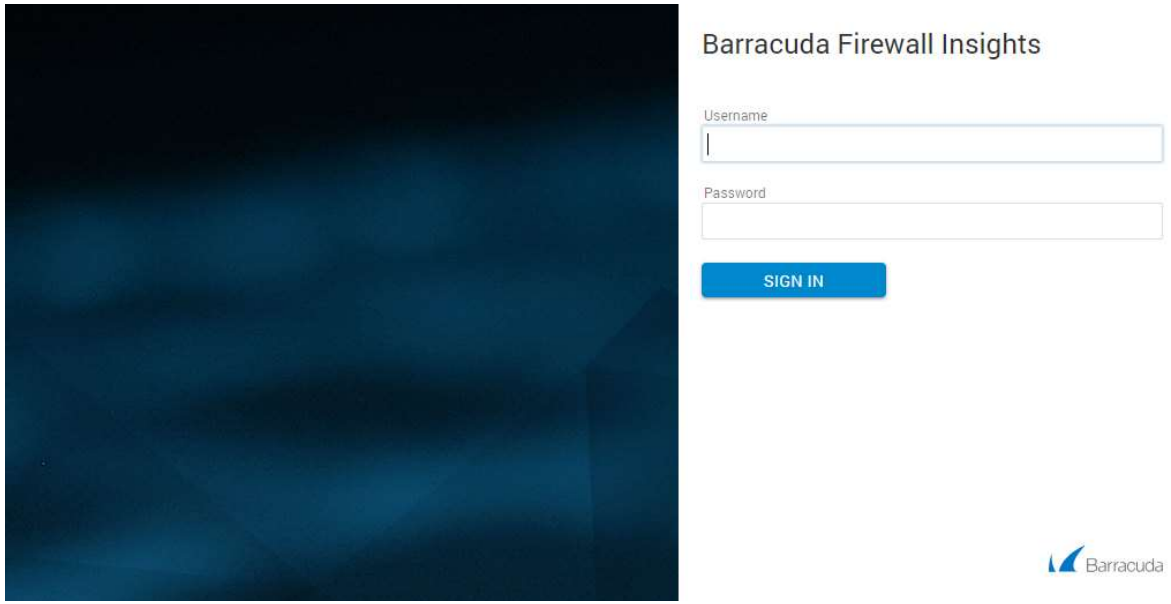
- Migrate a CC to firmware 7.2.4 or higher
- Add Firewall Insights to the remote network addresses
- Create on the CC:
  - NEW service object 'FIREWALL-INSIGHTS‘ [TCP-2400 and TCP-8001]
  - NEW network object 'FIREWALL-INSIGHTS‘
  - NEW forwarding access rule ‘BOXES-2-LAN-FIREWALL-INSIGHTS'



Checklist

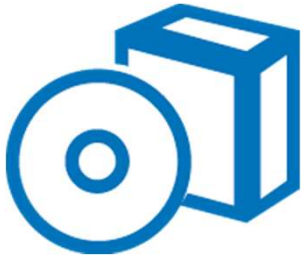
- Email notifications ✓
- License ✓
- Network ✓
- How to stream data ✓
  - Ports
  - Remote management tunnel

Firewalls Insights Login



Firewall Insights BASIC Configuration

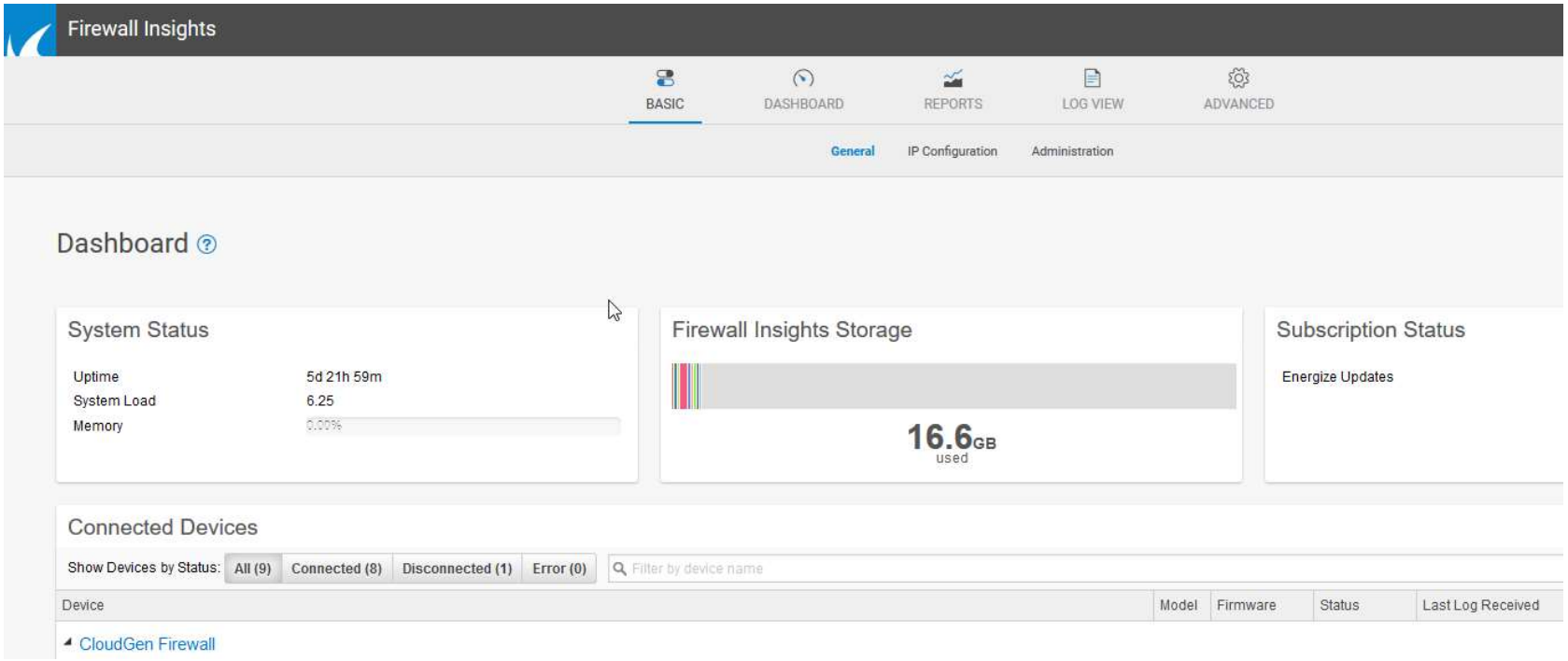
- Changing admin password
  - 5 to 20 characters and can include letters, numbers, and special characters
- Setting up email notification
- Connected devices / shared secret
  - Can include letters, numbers, and special characters, except the hash sign (#)



BASIC – Overview

- (General) System status
- (General) Firewall Insights storage
- (General) Subscription status
- (General) Connected devices

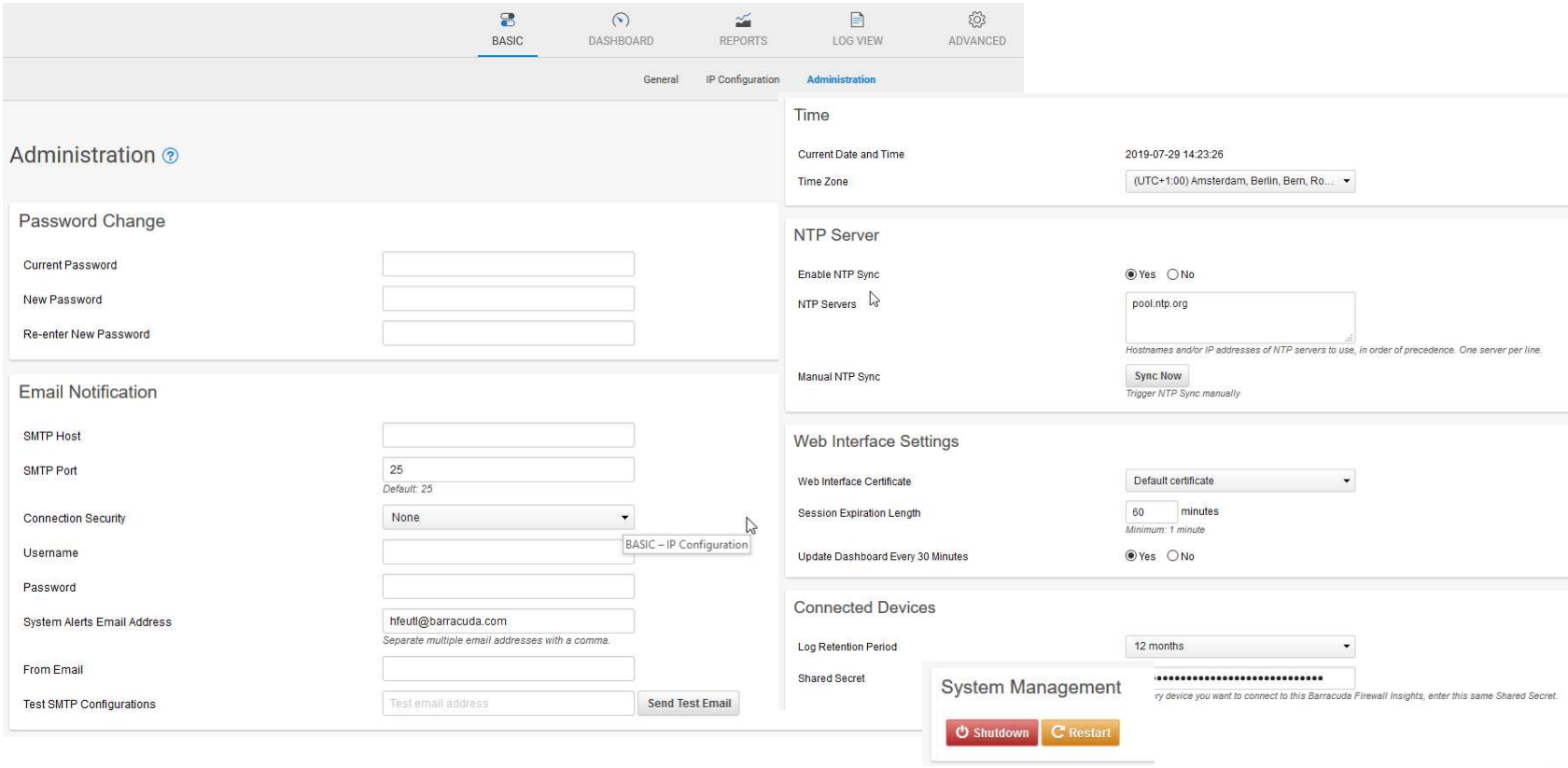
BASIC – Overview



BASIC – Administration

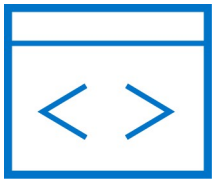
- Password change
- Email notification
- Time (Reboot!) / NTP
- Web interface settings
  - Web interface certificate
- Connected devices
  - Log retention period (1-12 months)
  - Shared secret (for all CGFs)

BASIC – Administration

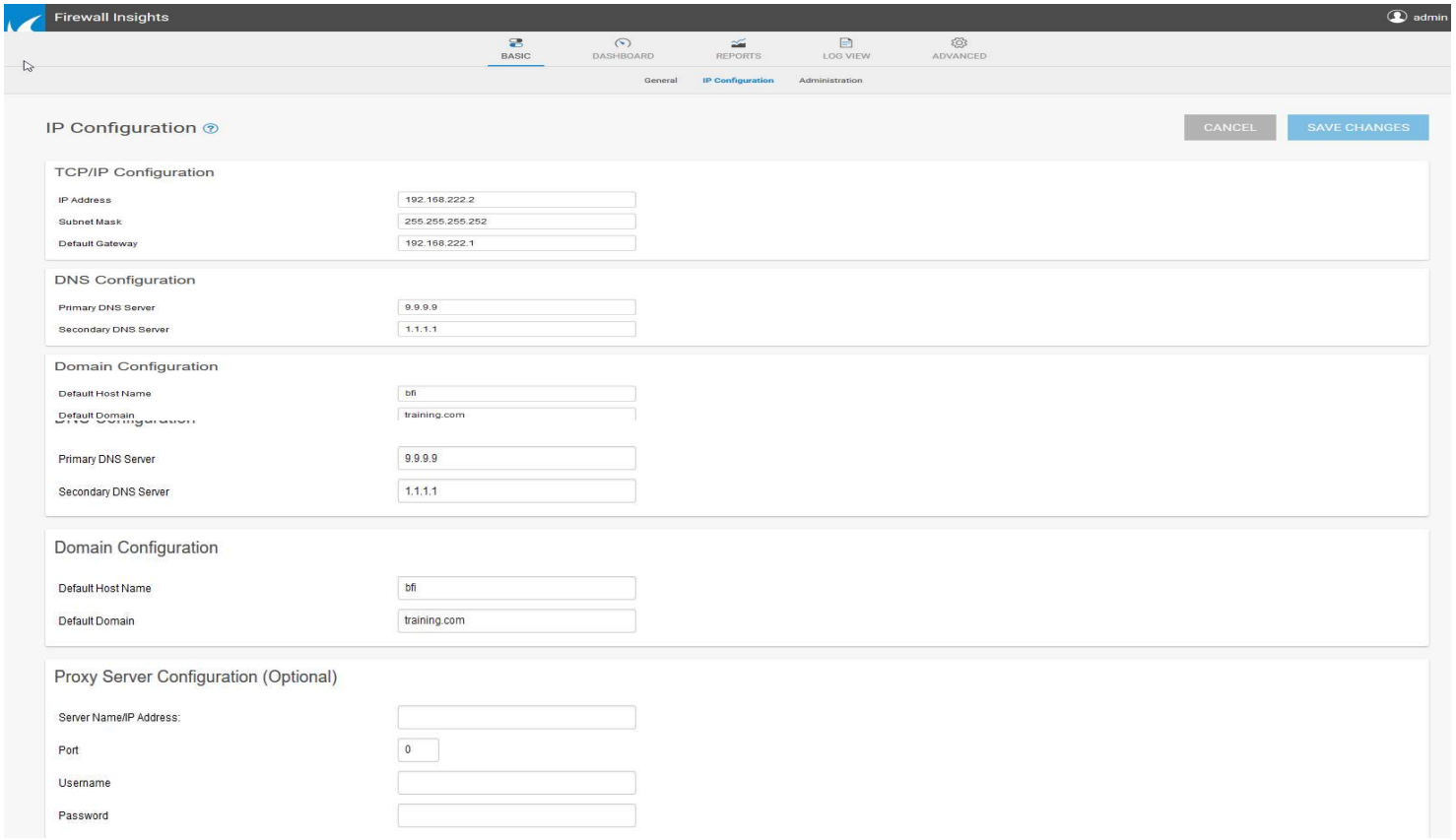


BASIC – IP Configuration

- TCP/IP configuration
- DNS configuration
- Domain configuration
- Proxy server configuration (optional)

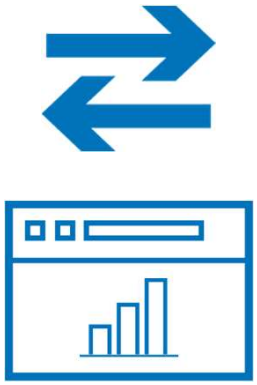


BASIC – IP Configuration

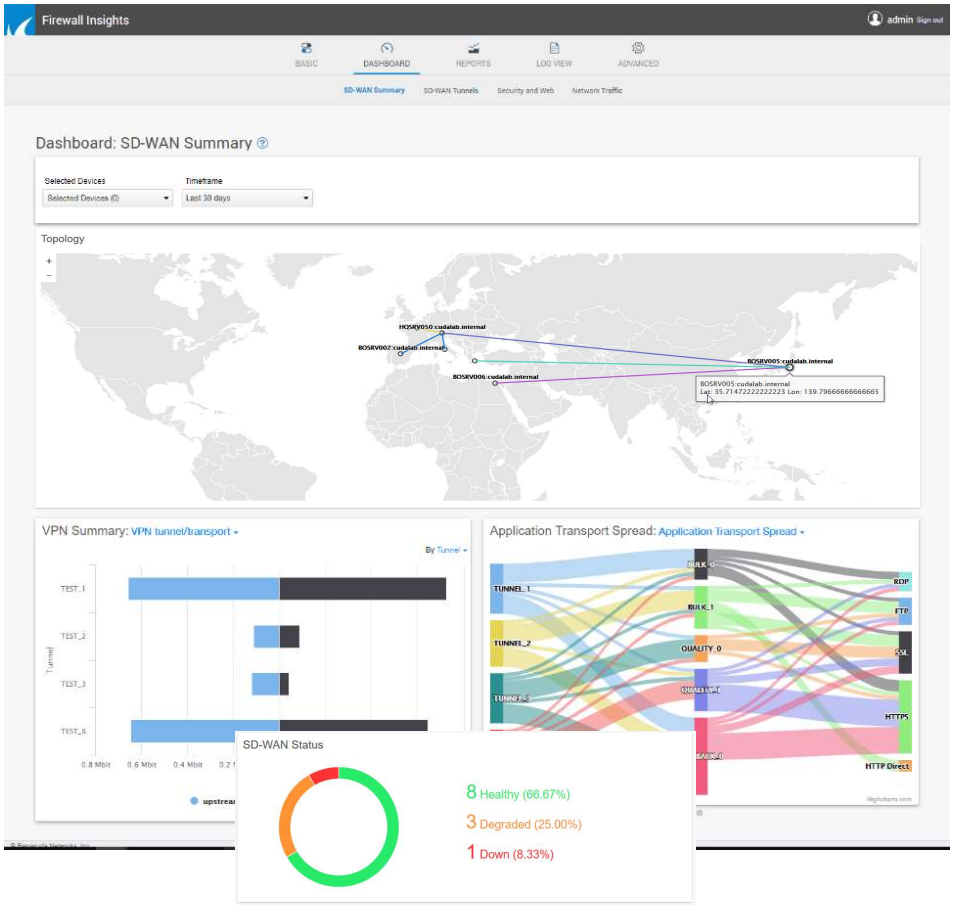


Insights - DASHBOARD Features

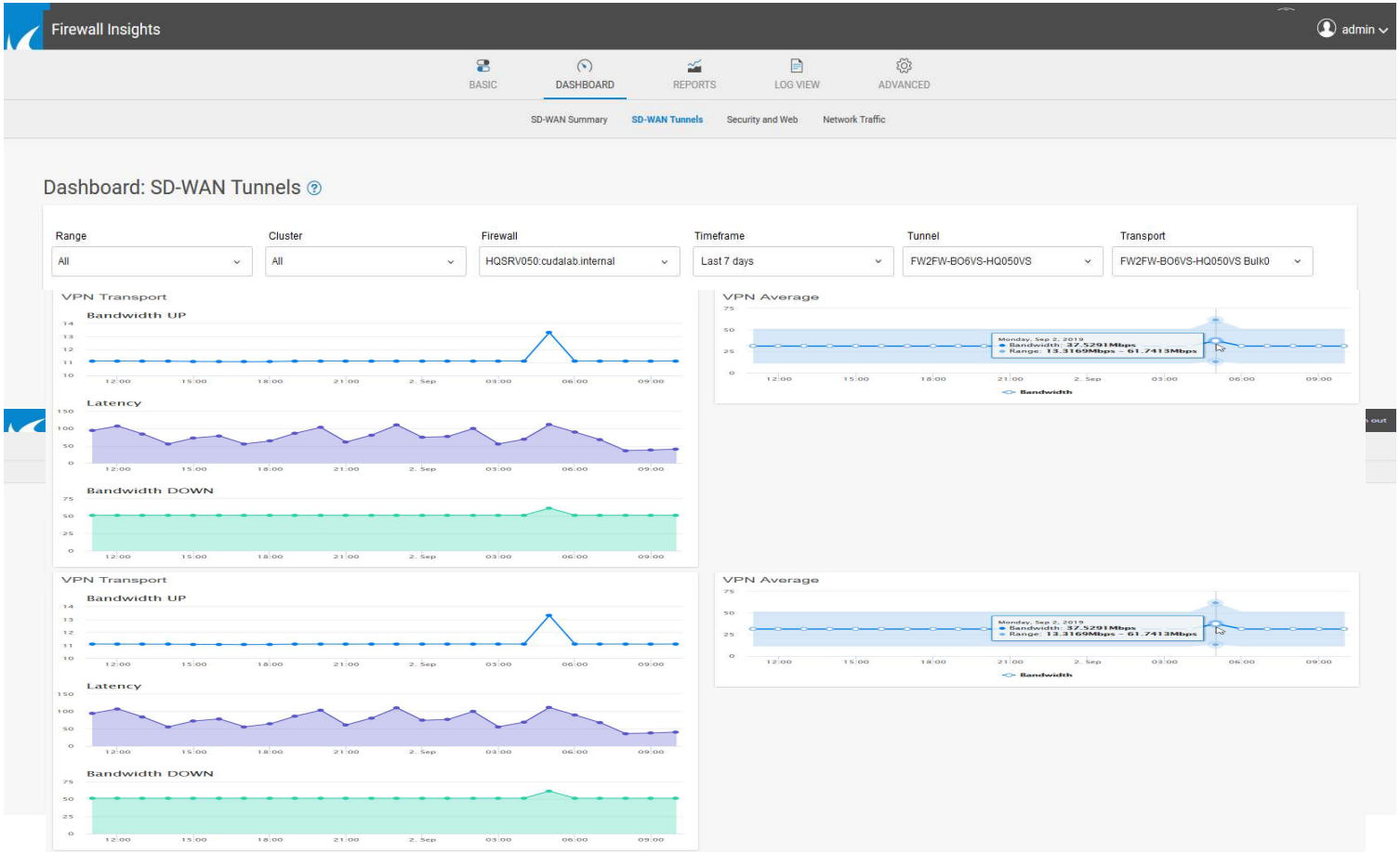
- SD-WAN / VPN
- Security & web
  - Top 10 applications
  - URL categories
  - Web requests, …
- Firewall traffic
  - Network Discovery graph
  - Bandwidth used by web traffic, …



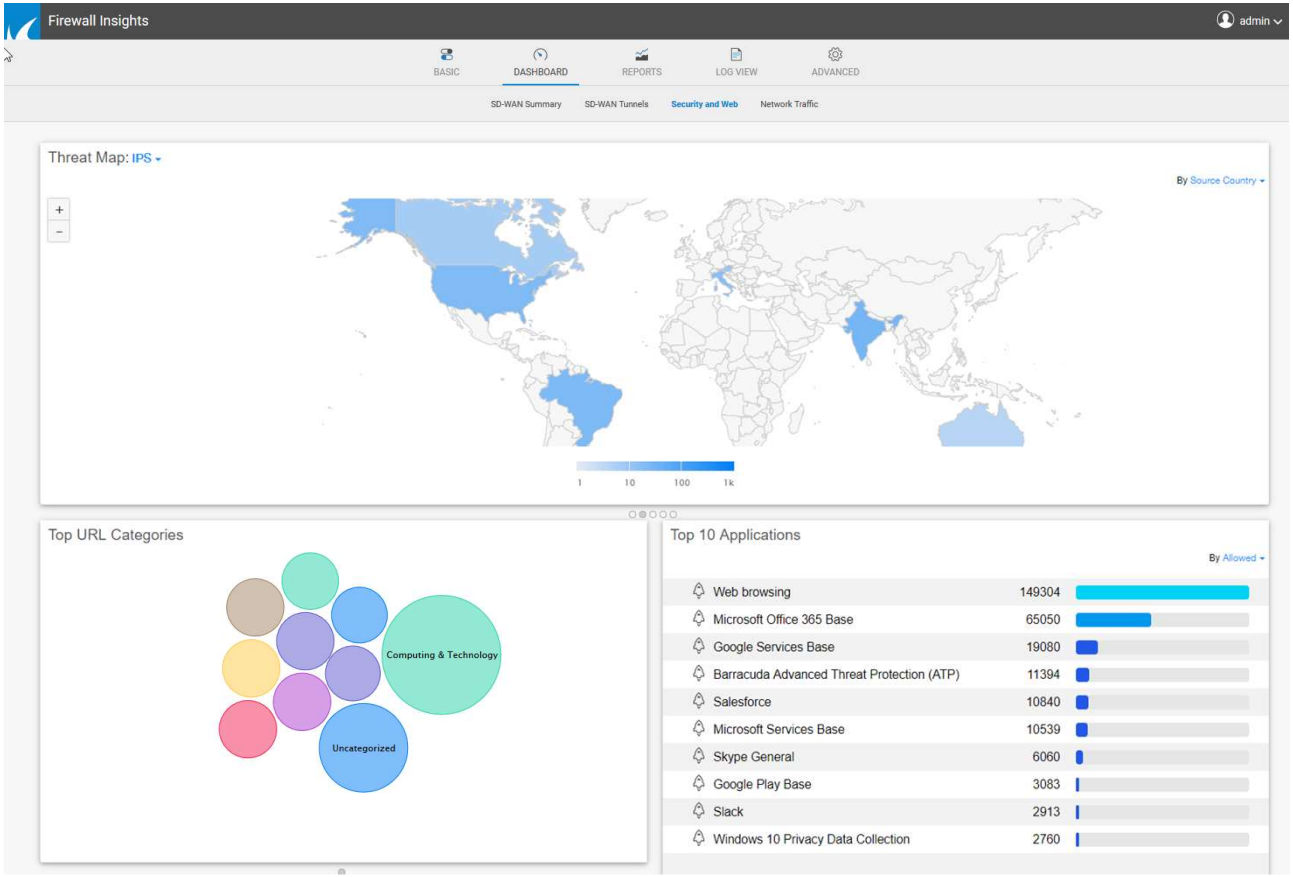
Insights – Dashboard – SD-WAN



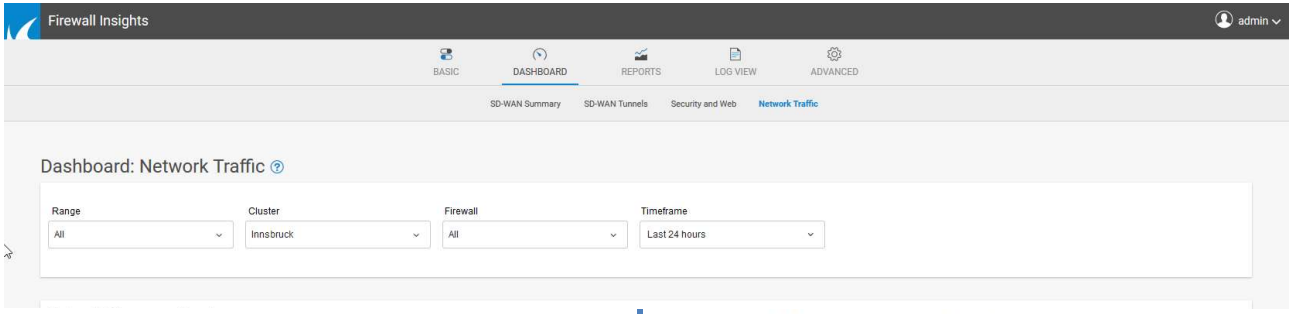
Insights – Dashboard – SD-WAN

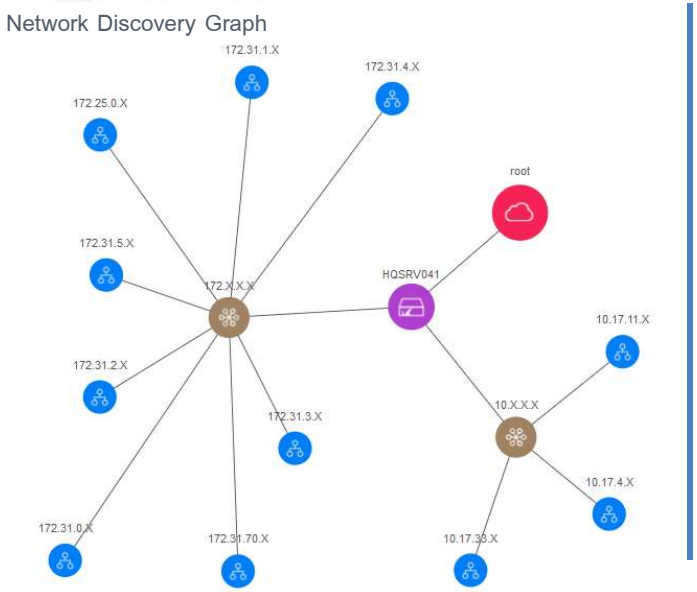


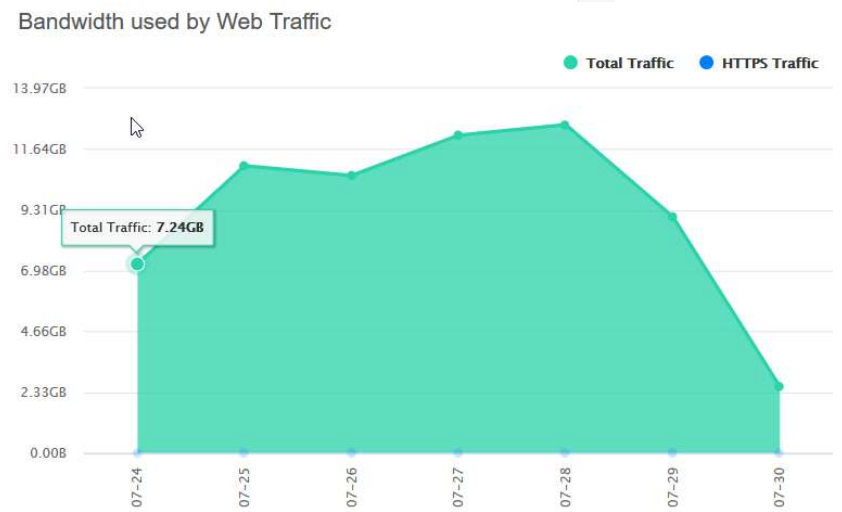
Insights – Dashboard – Security and Web



Insights – Dashboard – Network Traffic



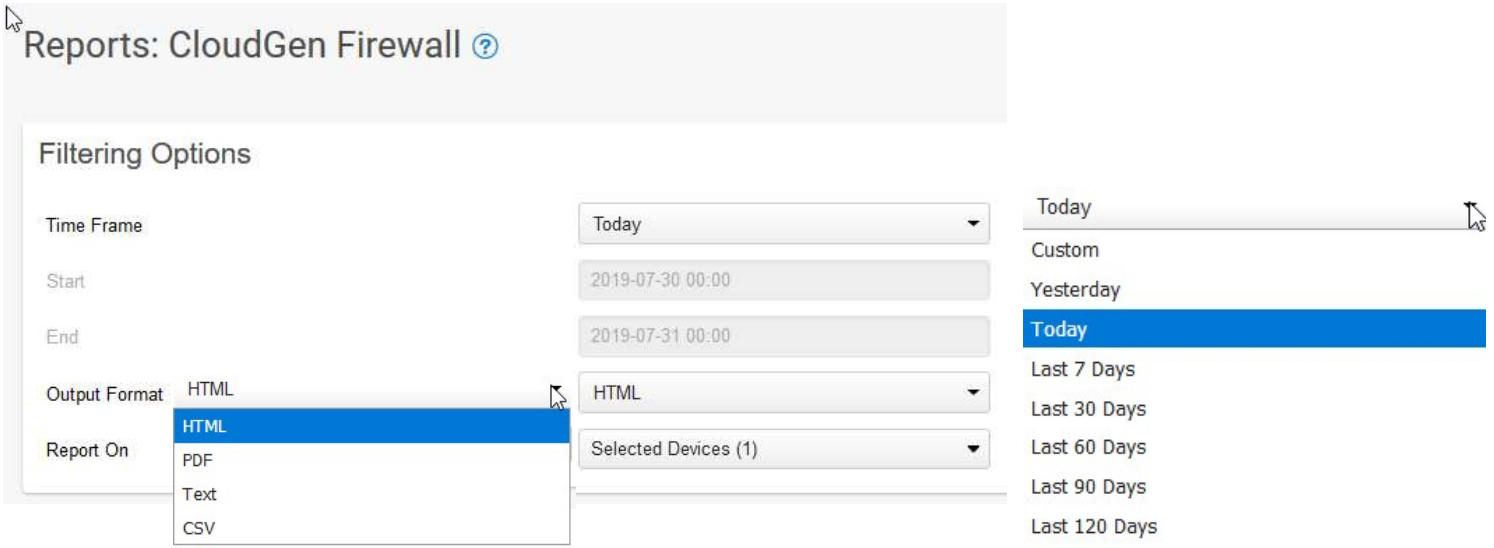




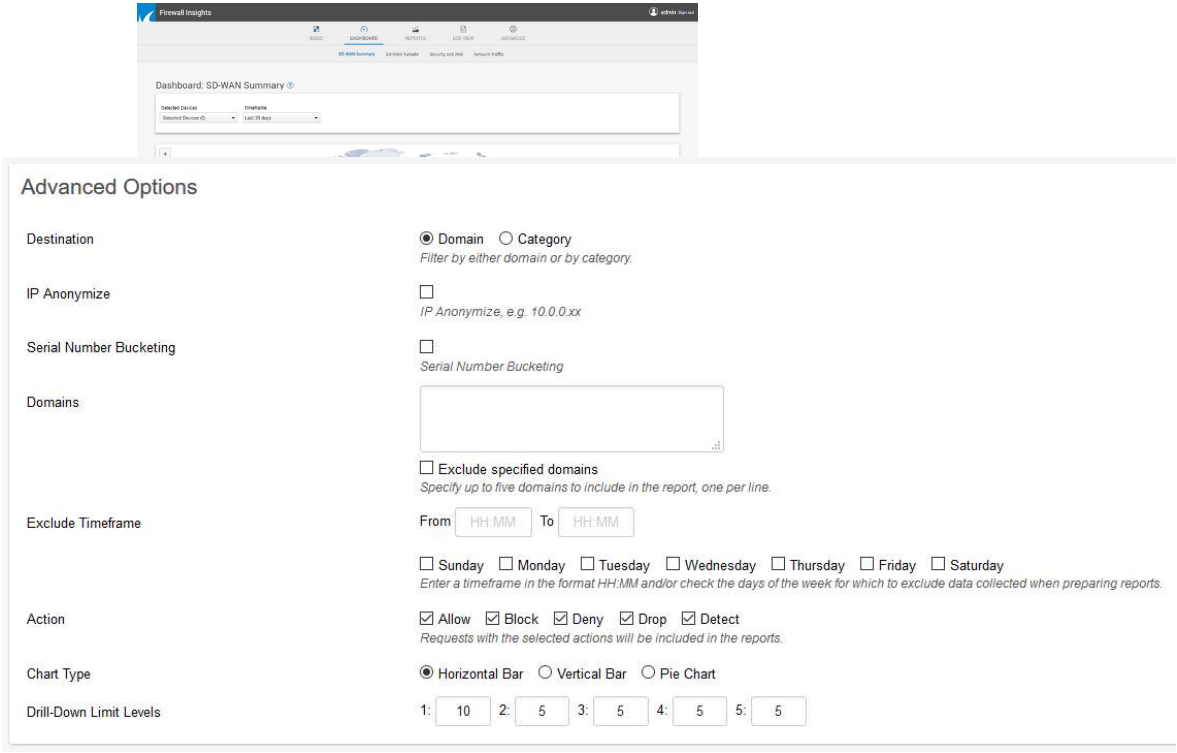
Insights – REPORTS Features

- Filtering options
  - Time frame (Today – Last 6 months)
  - Output format (HTML, PDF, TEXT, or CSV)
- Advanced options
- Schedule Report
  - Delivery options (email or external server)
  - Frequency (once – monthly)

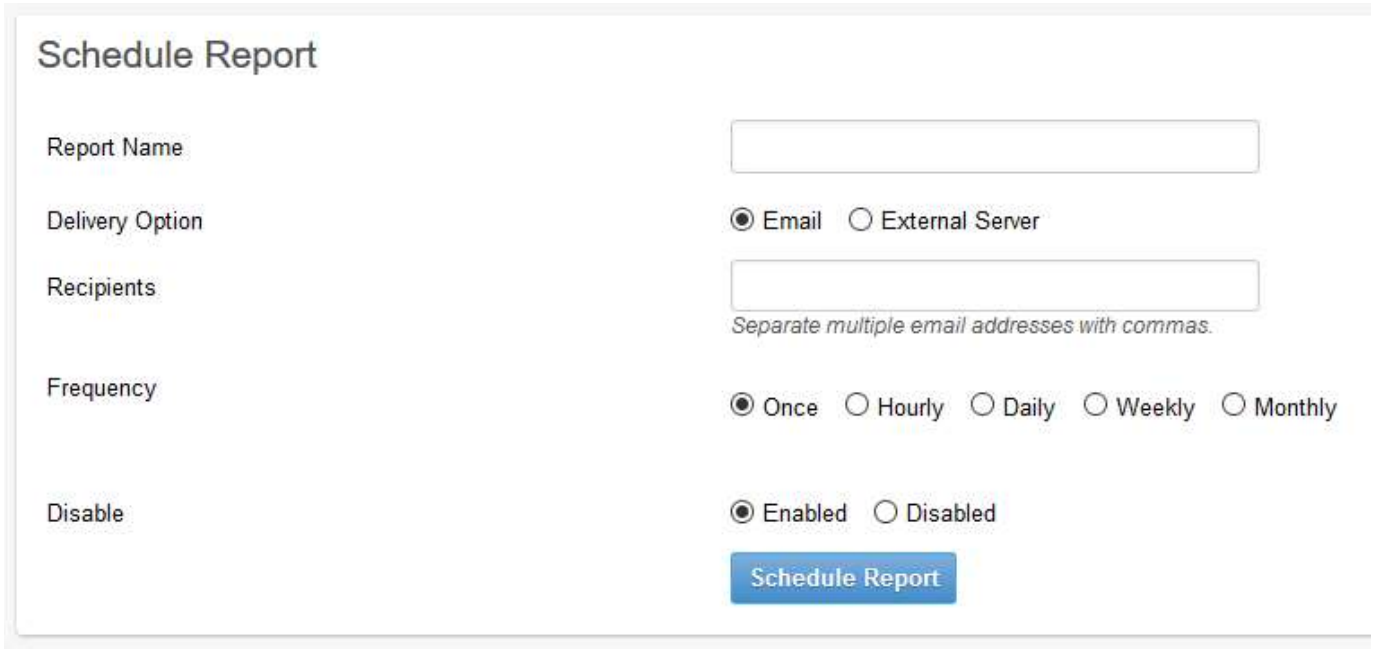
Insights – Reports – Filtering Options



Insights – Reports – Advanced Options

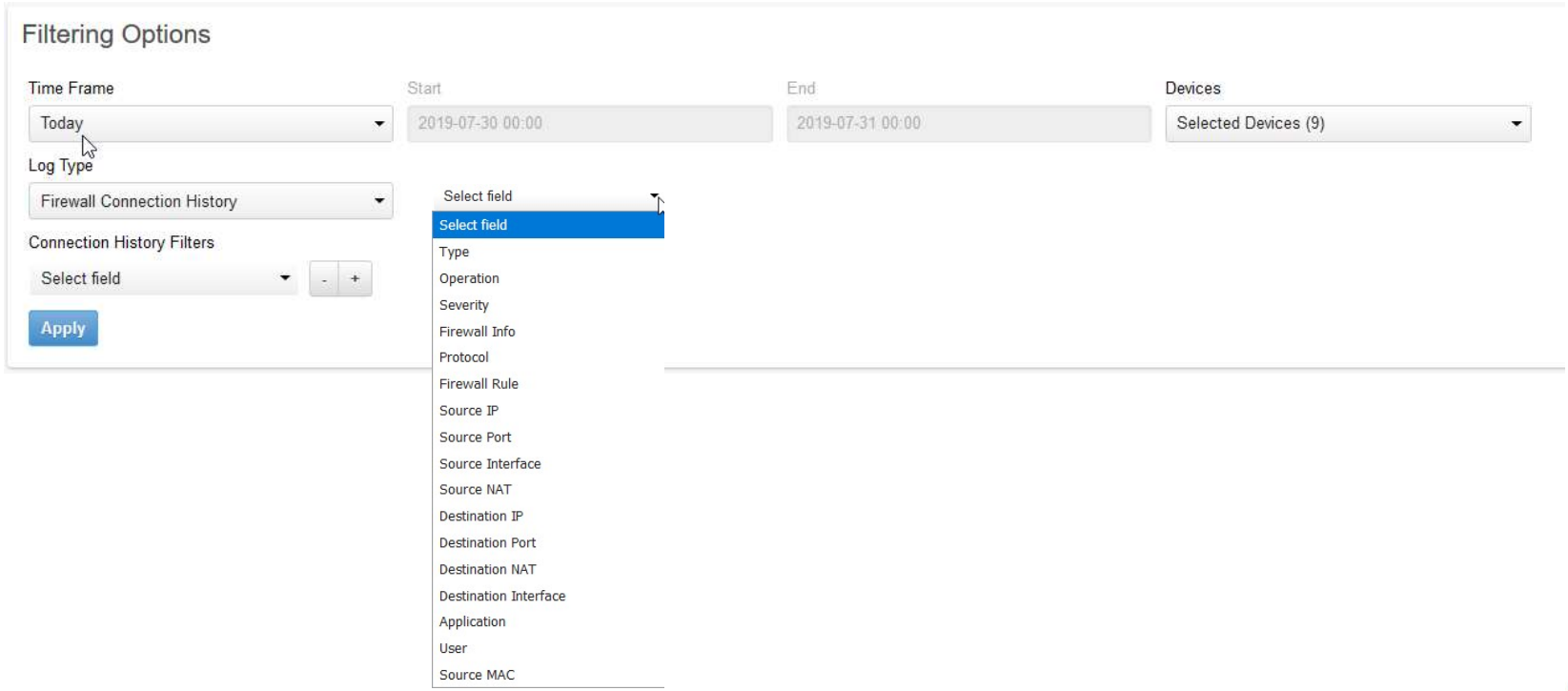


Insights – Reports – Schedule Report



Insights – LOG VIEW Features

- Filtering options

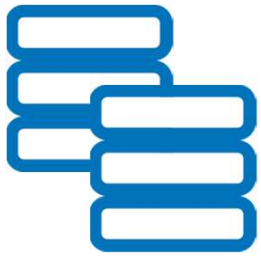


Insights – ADVANCED Features

- Backups
- Energize Updates
- Firmware updates
- External servers
- Troubleshooting
- Support
  - Help topics (online help)

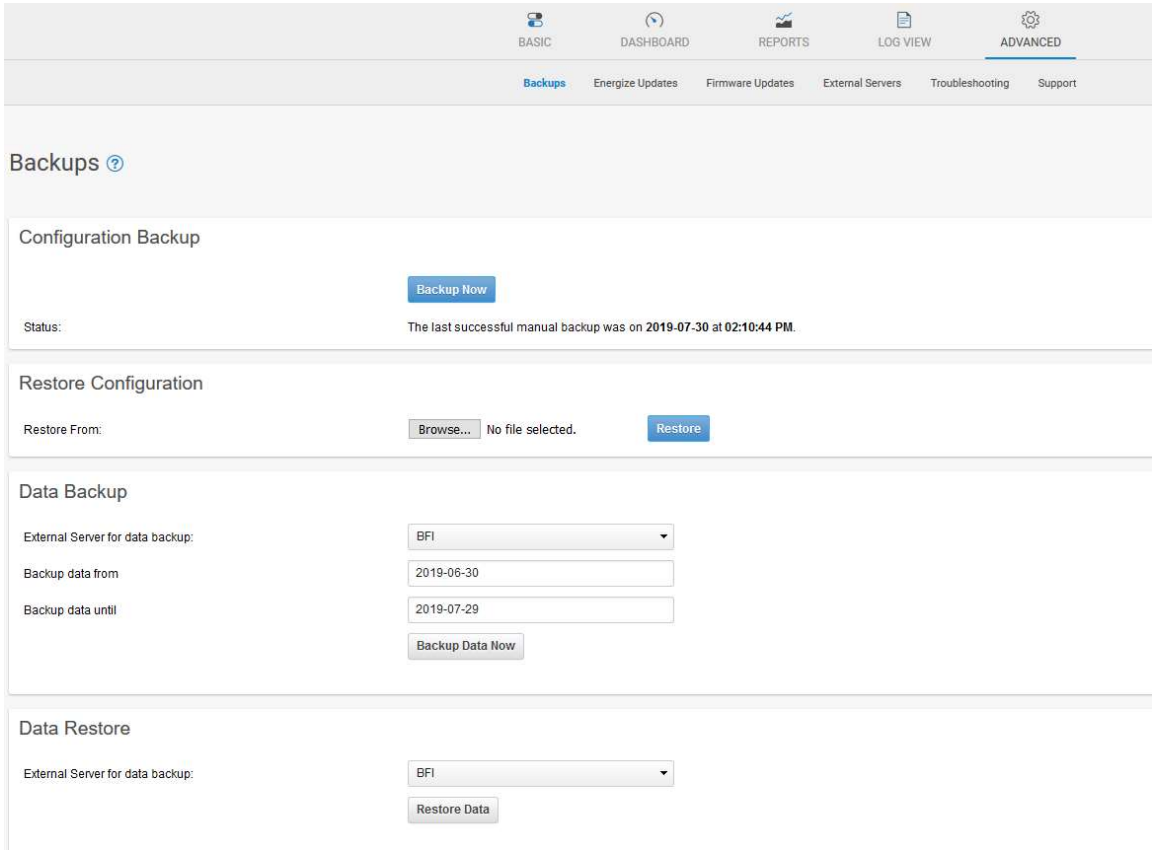
Insights – ADVANCED – Backups

- Configuration backup
- Restore configuration
- Data backup
  - You must use an external server
- Data restore
  - You must select an external server



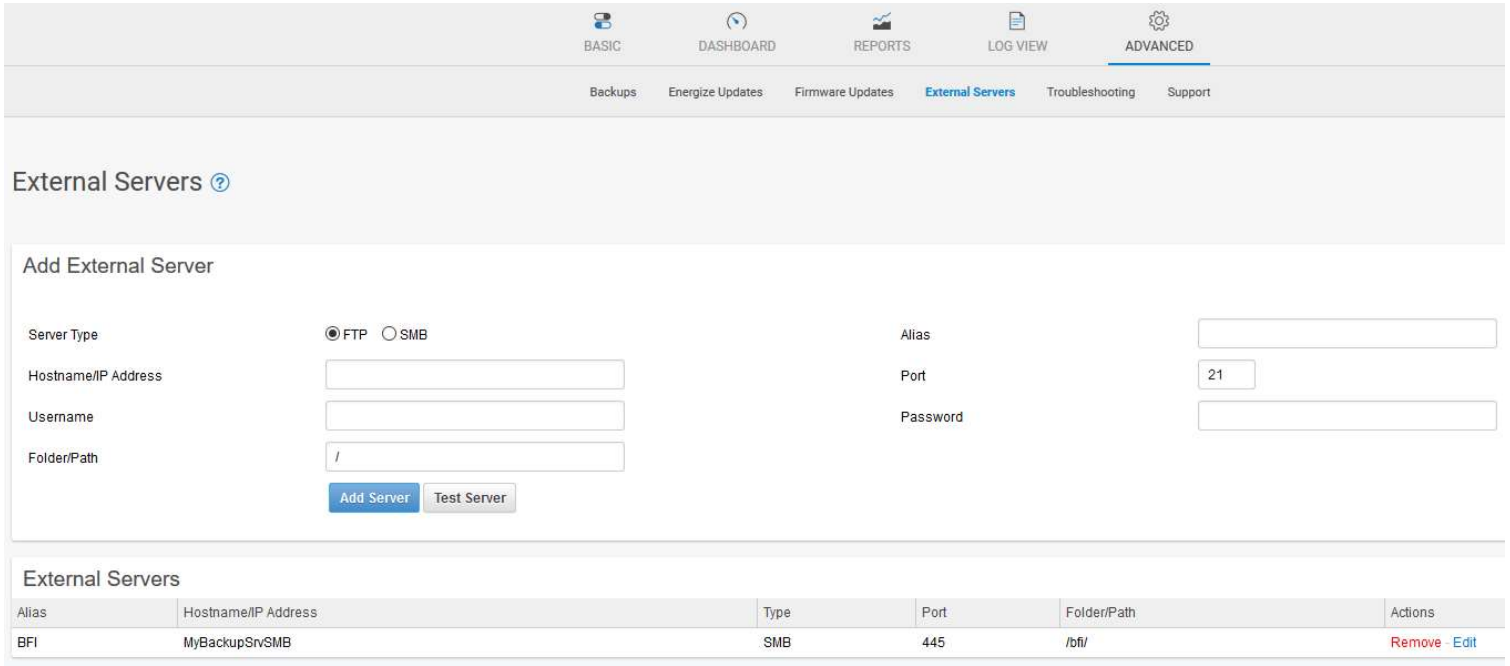
! Data and config. backup **must** always be done together !

Insights – ADVANCED – Backups



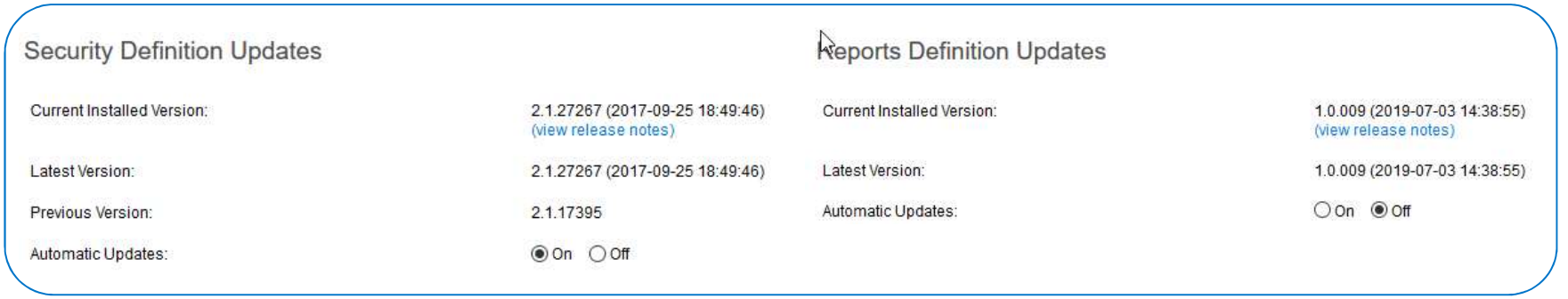
Insights – ADVANCED – External Servers

Add external server



Insights – ADVANCED – Updates

- Energize Updates

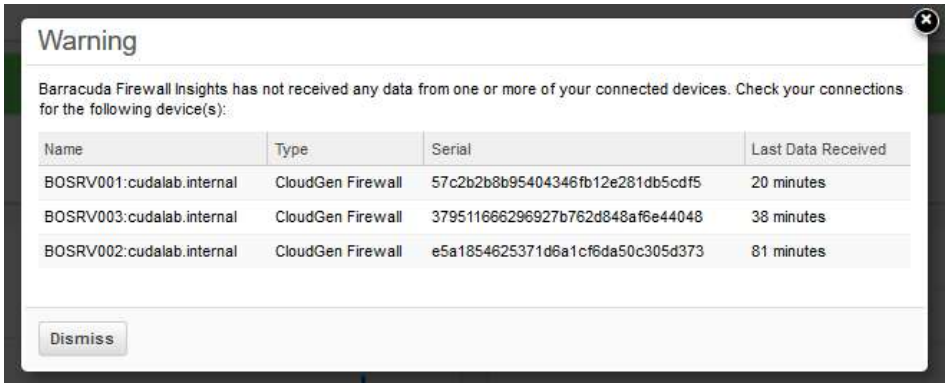


- Firmware updates

Nice to Know

- Troubleshooting
  - CHECK minimum requirements
  - Wait a couple of minutes at the first prompt for the containers to start up before logging in with admin/admin

- On the roadmap:
  - Custom reporting
  - Cloud images
  - Multi-user support



Questions

- Q: How many resources will I need for xx firewalls?
- *A: This depends on*
  - *model/*
  - *number of sessions/*
  - *enabled features / etc…*
- Q: Is this just for the enterprise?
- *A: No, for every customer managing*
  - *SD-WAN / Web Reporting / Firewalls*

Documentation Links

- Barracuda Firewall Insights
  - https://campus.barracuda.com/doc/84968178/
- CGF streaming config how-to
  - https://campus.barracuda.com/doc/73720518/
- Subscriptions
  - https://campus.barracuda.com/product/cloudgenfirewall/doc/78151827/


Thank you
Barracuda
TECHSUMMIT19
BARRACUDA TECHNICAL SUMMIT