



Barracuda.  
**TECHSUMMIT19**  
BARRACUDA TECHNICAL SUMMIT

# Barracuda Firewall Insights

CloudGen Firewall Firmware 7.2.4 > 8.0.1





- **Challenges**

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

**Firewall Insights**

**Report Creator**

**Firewall Admin Dashboards**





**SD-WAN**

**Central Reporting**

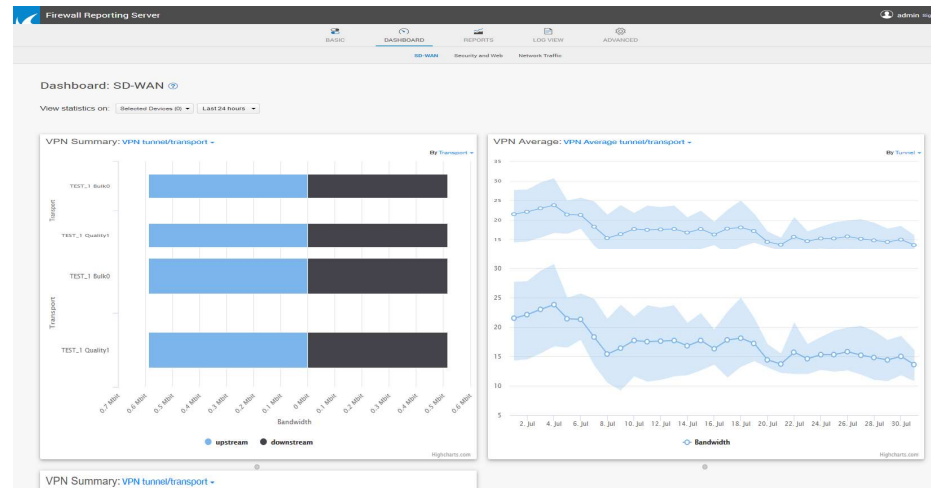
**“Connection Log” across ALL Firewalls**



# 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





- 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





- 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	<ul style="list-style-type: none"><li>• Disk format: Thick provisioned format</li><li>• More IOPS</li></ul>		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





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


















- Barracuda Firewall Insights server

 The only restriction is the system performance 

- A Barracuda Firewall Insights subscription on every CGF

 <b>box</b>						
	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

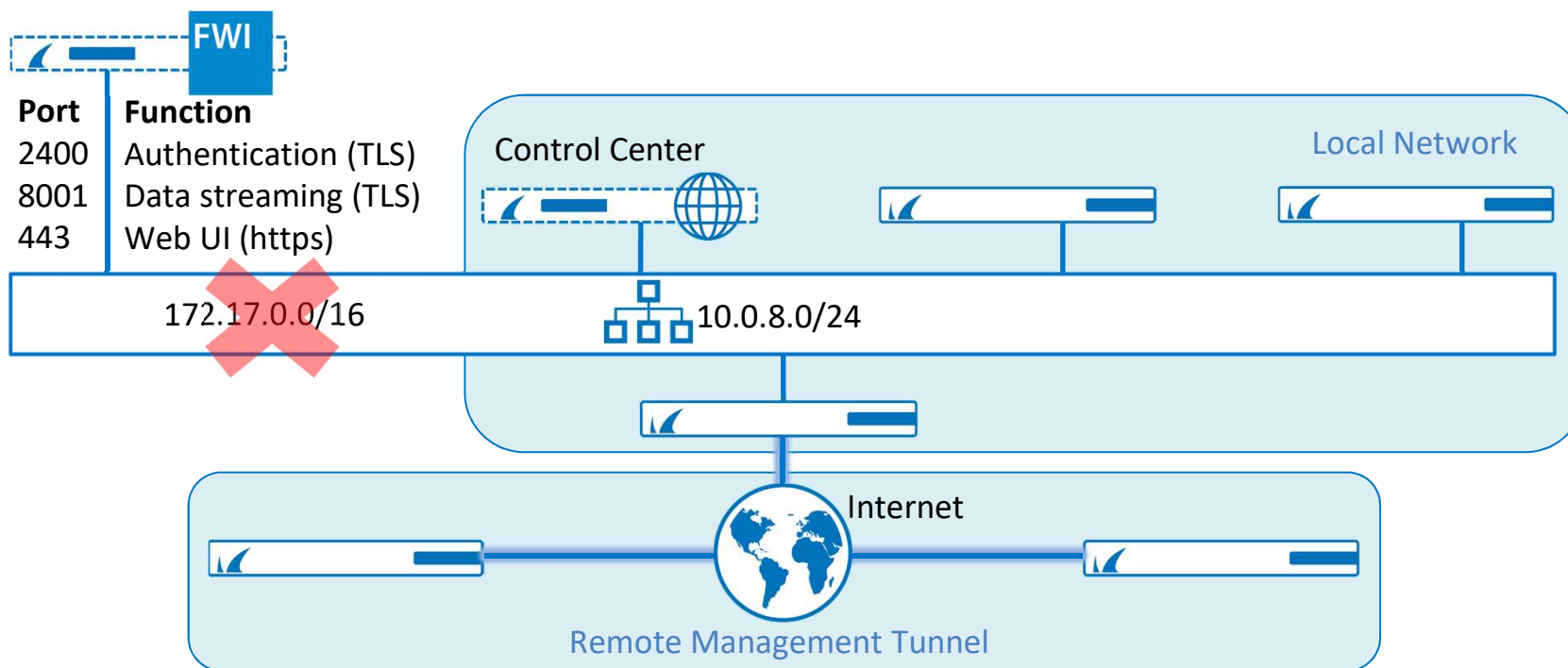


Virtual Systems  
(Vx)



Public Cloud







# Network 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





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

Syslog Streaming - Firewall Insights

**Configuration**

- Basic Setup
- Logdata Filters
- Logstream Destinations
- Logdata Streams
- Web Log Streaming
- Firewall Insights**

**Configuration Mode**

Switch to Basic (Hide 13)

**Settings**

Enable	<input checked="" type="checkbox"/>	
Hostname	<input checked="" type="checkbox"/>	172.16.0.10
Shared Secret	New	Insights Shared Secret
	Confirm	
	Strength	
Use Remote Management Tunnel	Automatic	Automatic = VIP No = Mgmt. IP
Firewall Insights Serial		
Data Streams	Firewall and VPN	

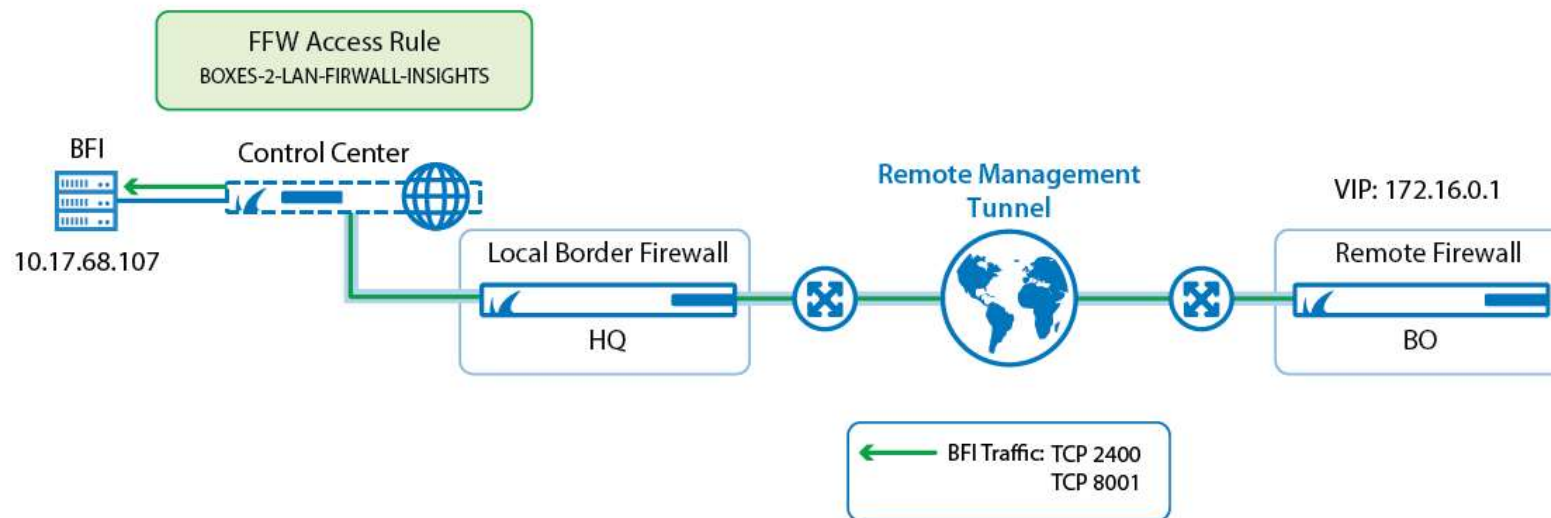




# Remote Management Tunnel



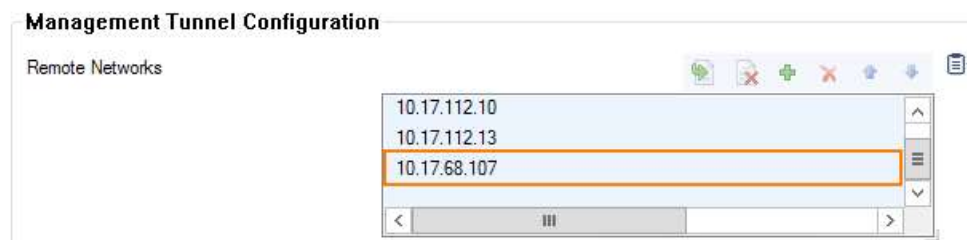
- Newly deployed CC with firmware 7.2.4 or higher
- Migrate a CC to firmware 7.2.4 or higher



# 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'

-FIREWALL-INSIGHTS [Rule]

Pass

BOXES-2-LAN-FIREWALL-INSIGHTS

Allows limited LAN access from managed firewalls to Firewall Insights.

☐ Bi-Directional ☐ Dynamic Rule ☐ Deactivate Rule

Source VR Instance default Destination VR Instance default

Source	Service	Destination
Any	FIREWALL-INSIGHTS	Firewall Insights
0.0.0.0/0	TCP 8001	10.17.68.107
	TCP 2400	





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





# Firewalls Insights Login



## Barracuda Firewall Insights

Username

Password

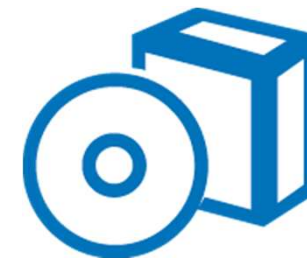
SIGN IN



# 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





**Firewall Insights**

BASIC

DASHBOARD

REPORTS

LOG VIEW

ADVANCED

General

IP Configuration

Administration

## Dashboard ?

### System Status

Uptime	5d 21h 59m
System Load	6.25
Memory	0.00%

### Firewall Insights Storage

16.6GB used

### Subscription Status

Energize Updates

### Connected Devices

Show Devices by Status: All (9) Connected (8) Disconnected (1) Error (0)

Device	Model	Firmware	Status	Last Log Received
CloudGen Firewall				







- 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

DASHBOARD

REPORTS

LOG VIEW

ADVANCED

General

IP Configuration

Administration

Administration ?

Password Change

Current Password

New Password

Re-enter New Password

Email Notification

SMTP Host

SMTP Port

Connection Security

Username

Password

System Alerts Email Address

From Email

Test SMTP Configurations

Time

Current Date and Time

Time Zone

NTP Server

Enable NTP Sync

NTP Servers

Manual NTP Sync

Web Interface Settings

Web Interface Certificate

Session Expiration Length

Update Dashboard Every 30 Minutes

Connected Devices

Log Retention Period

Shared Secret

System Management

Shutdown

Restart

2019-07-29 14:23:26

(UTC+1:00) Amsterdam, Berlin, Bern, Ro...

pool.ntp.org

Hostnames and/or IP addresses of NTP servers to use, in order of precedence. One server per line.

Sync Now

Trigger NTP Sync manually

Default certificate

60 minutes

Minimum: 1 minute

Yes No

12 months

.....

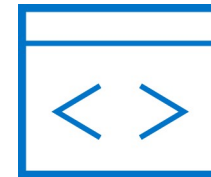
ry device you want to connect to this Barracuda Firewall Insights, enter this same Shared Secret.



# BASIC – IP Configuration



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



# BASIC – IP Configuration



Firewall Insights

admin

BASIC

DASHBOARD

REPORTS

LOG VIEW

ADVANCED

General

IP Configuration

Administration

IP Configuration ?

CANCEL

SAVE CHANGES

TCP/IP Configuration

IP Address

192.168.222.2

Subnet Mask

255.255.255.252

Default Gateway

192.168.222.1

DNS Configuration

Primary DNS Server

9.9.9.9

Secondary DNS Server

1.1.1.1

Domain Configuration

Default Host Name

bfi

Default Domain

training.com

DNS Configuration

Primary DNS Server

9.9.9.9

Secondary DNS Server

1.1.1.1

Domain Configuration

Default Host Name

bfi

Default Domain

training.com

Proxy Server Configuration (Optional)

Server Name/IP Address:

Port

0

Username

Password



# Insights - DASHBOARD Features



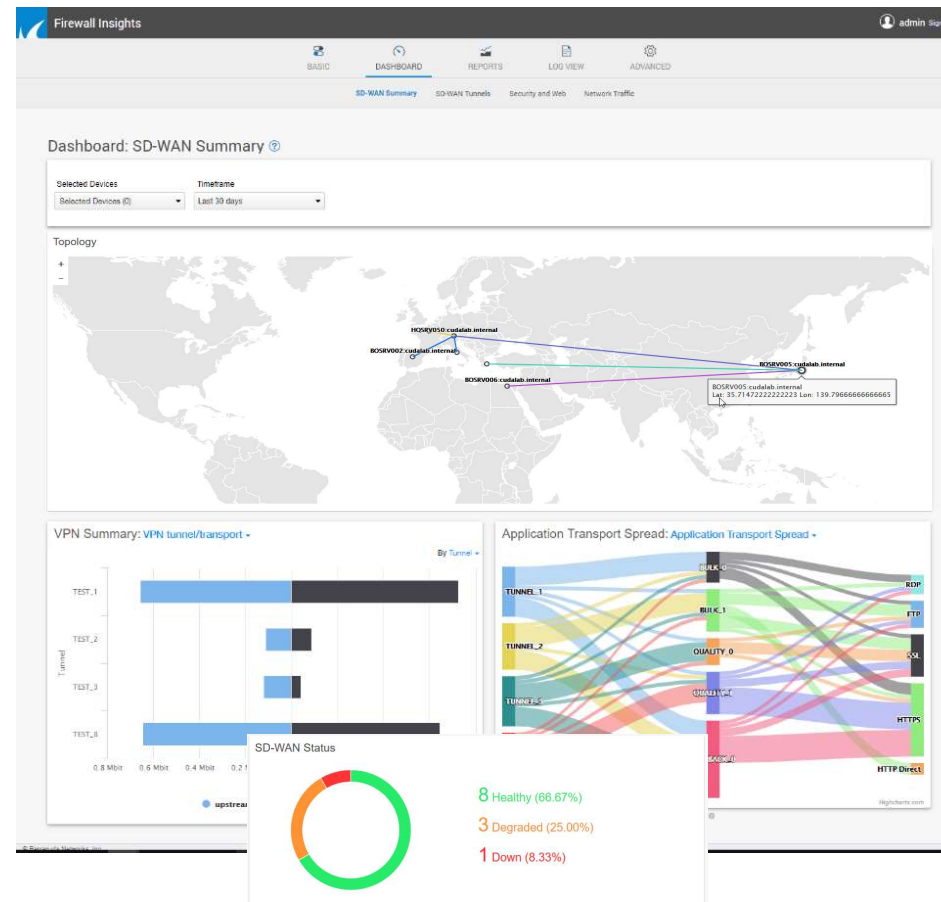
- SD-WAN / VPN
- Security & web
  - Top 10 applications
  - URL categories
  - Web requests, ...
- Firewall traffic
  - Network Discovery graph
  - Bandwidth used by web traffic, ...



FW

Barracuda  
CloudGen Firewall

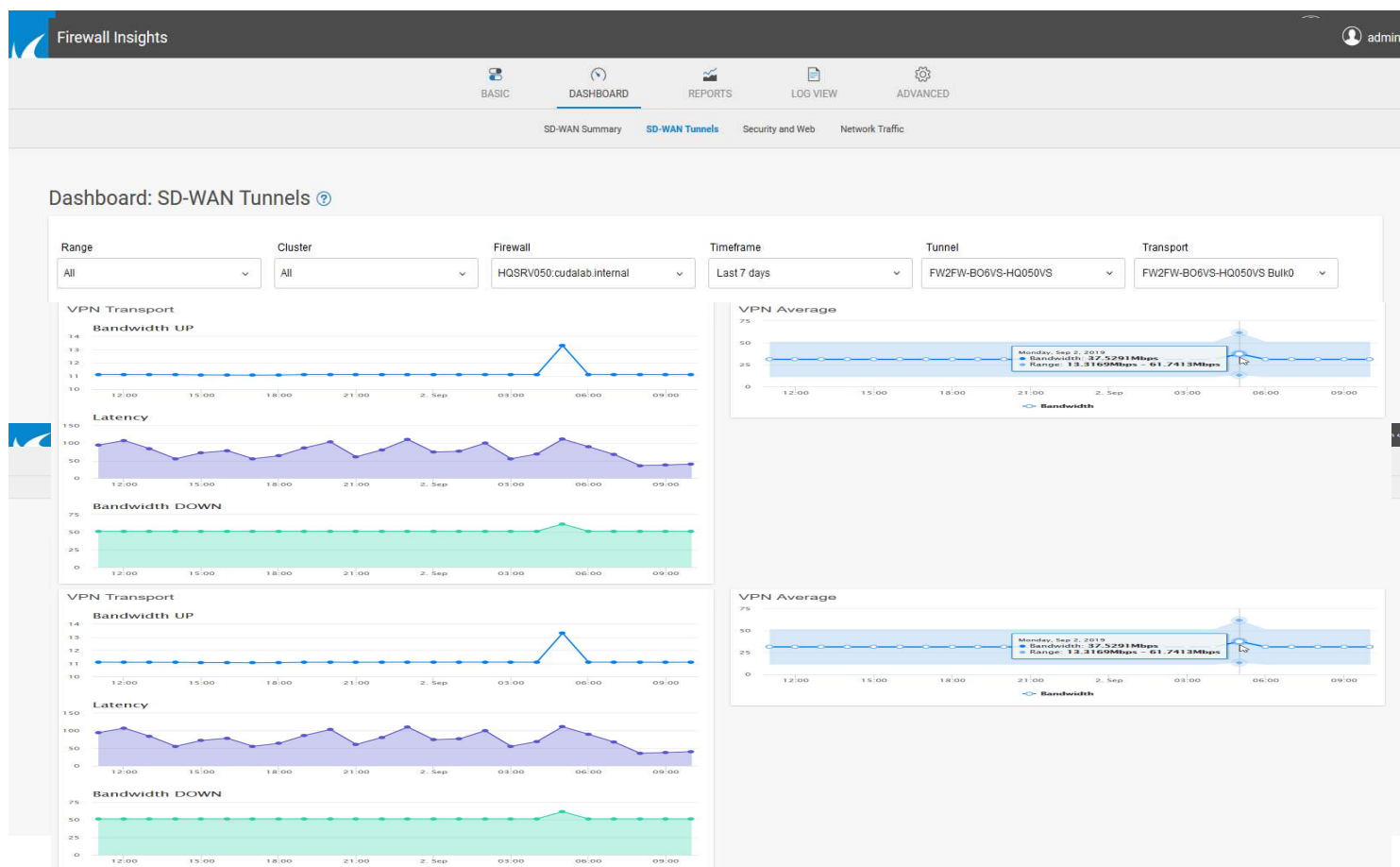
# Insights – Dashboard – SD-WAN



FW

Barracuda  
CloudGen Firewall

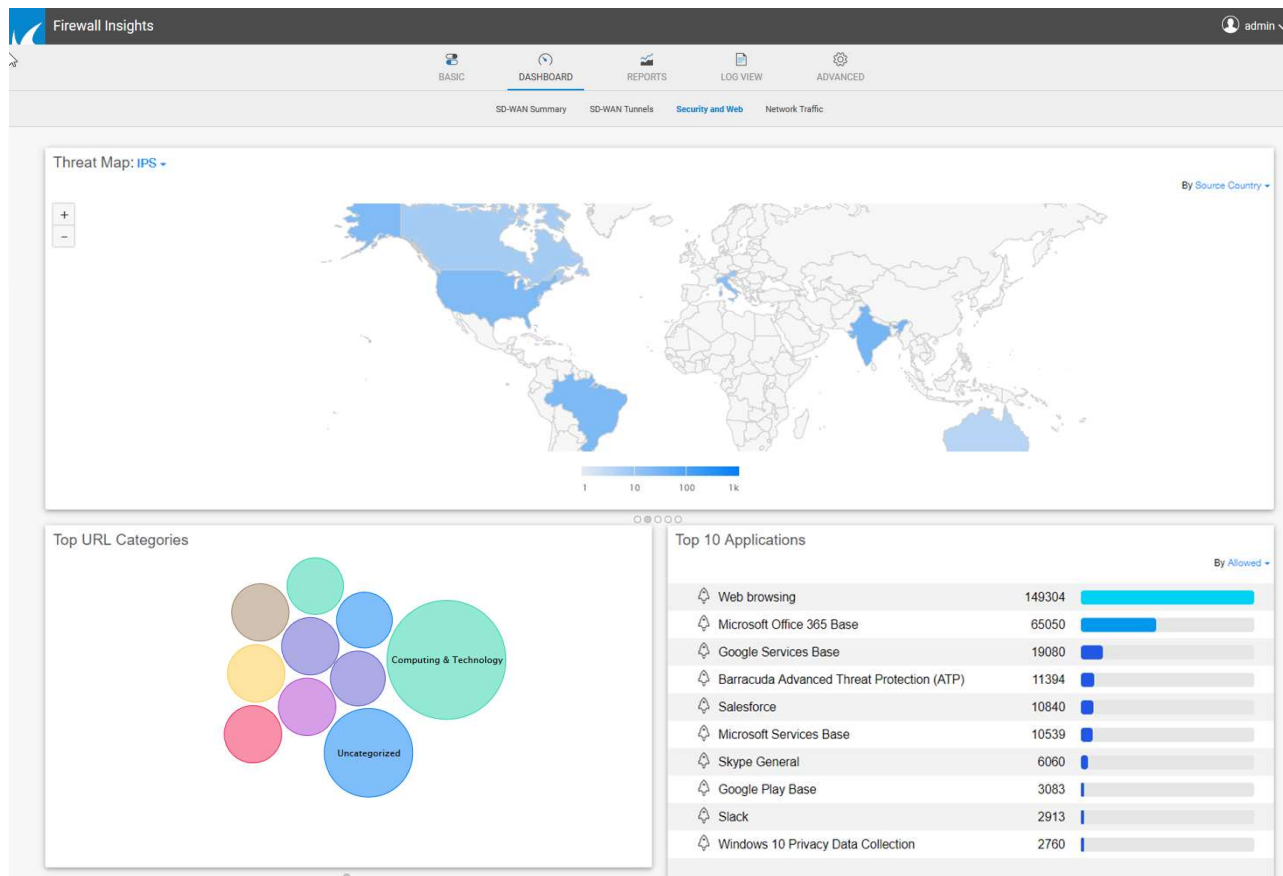
# Insights – Dashboard – SD-WAN



FW

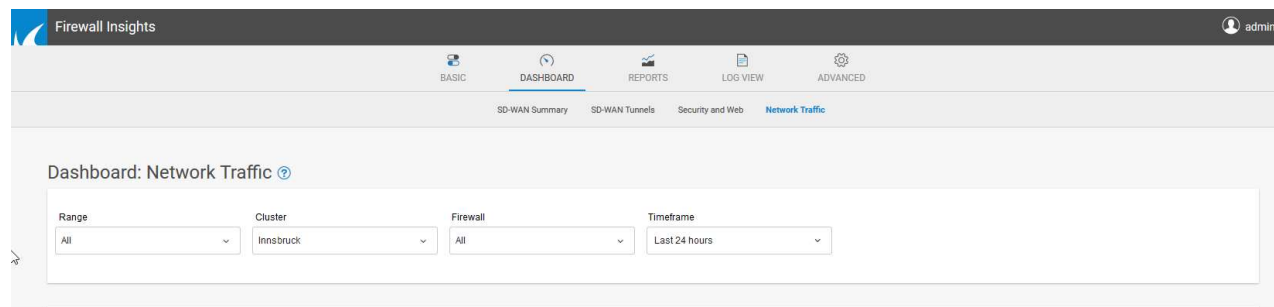
Barracuda  
CloudGen Firewall

# Insights – Dashboard – Security and Web

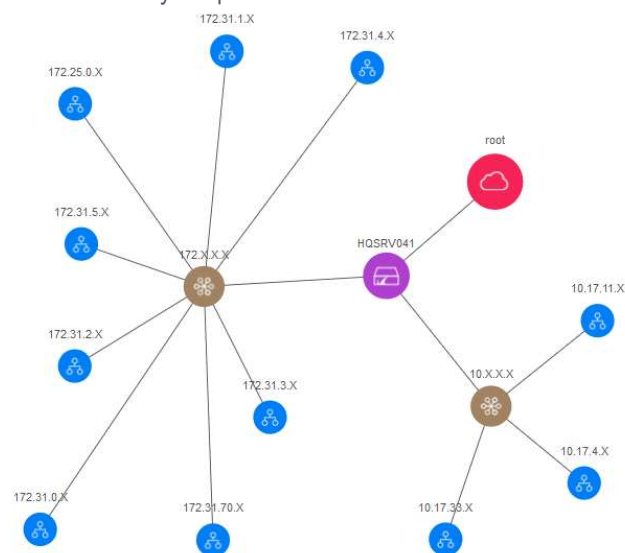




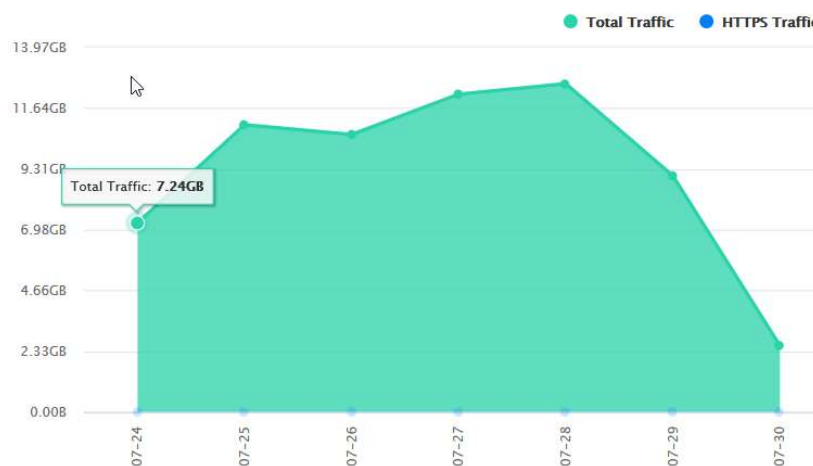
# Insights – Dashboard – Network Traffic



Network Discovery Graph



Bandwidth used by Web 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



Reports: CloudGen Firewall ?

Filtering Options

Time Frame: Today

Start: 2019-07-30 00:00

End: 2019-07-31 00:00

Output Format: HTML

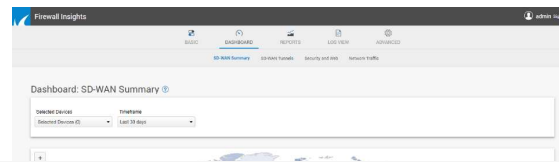
Report On: HTML

Selected Devices (1)

Today  
Custom  
Yesterday  
**Today**  
Last 7 Days  
Last 30 Days  
Last 60 Days  
Last 90 Days  
Last 120 Days  
Last Week  
This Week  
This and Last Week  
Last Month  
This Month  
This and Last Month  
Last 3 Months  
Last 6 Months



# Insights – Reports – Advanced Options



## Advanced Options

Destination

☒ Domain ☐ Category

Filter by either domain or by category.

IP Anonymize

☐

IP Anonymize, e.g. 10.0.0.xx

Serial Number Bucketing

☐

Serial Number Bucketing

Domains

☐ Exclude specified domains

Specify up to five domains to include in the report, one per line.

Exclude Timeframe

From  To

☐ Sunday ☐ Monday ☐ Tuesday ☐ Wednesday ☐ Thursday ☐ Friday ☐ Saturday

Enter a timeframe in the format HH:MM and/or check the days of the week for which to exclude data collected when preparing reports.

Action

☒ Allow ☒ Block ☒ Deny ☒ Drop ☒ Detect

Requests with the selected actions will be included in the reports.

Chart Type

☒ Horizontal Bar ☐ Vertical Bar ☐ Pie Chart

Drill-Down Limit Levels

1:  2:  3:  4:  5:





## Schedule Report

Report Name

Delivery Option

☒ Email ☐ External Server

Recipients

*Separate multiple email addresses with commas.*

Frequency

☒ Once ☐ Hourly ☐ Daily ☐ Weekly ☐ Monthly

Disable

☒ Enabled ☐ Disabled

Schedule Report





- Filtering options

Filtering Options

Time Frame: Today (dropdown) Start: 2019-07-30 00:00 End: 2019-07-31 00:00 Devices: Selected Devices (9) (dropdown)

Log Type: Firewall Connection History (dropdown)

Connection History Filters: Select field (dropdown) - +

Apply

Select field

- Select field
- Type
- Operation
- Severity
- Firewall Info
- Protocol
- Firewall Rule
- Source IP
- Source Port
- Source Interface
- Source NAT
- Destination IP
- Destination Port
- Destination NAT
- Destination Interface
- Application
- User
- Source MAC





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

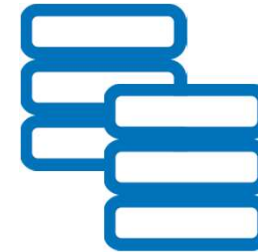
## Network Connectivity Test

*Enter a hostname or IP address in the text field and click on the appropriate button to perform a network test*





- 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 !







BASICDASHBOARDREPORTSLOG VIEWADVANCED

BackupsEnergize UpdatesFirmware UpdatesExternal ServersTroubleshootingSupport

### Backups ?

#### Configuration Backup

Backup Now

Status: The last successful manual backup was on **2019-07-30 at 02:10:44 PM.**

#### Restore Configuration

Restore From:  No file selected.

#### Data Backup

External Server for data backup:

Backup data from:

Backup data until:

Backup Data Now

#### Data Restore

External Server for data backup:

Restore Data



## Add external server

BASICDASHBOARDREPORTSLOG VIEWADVANCED

BackupsEnergize UpdatesFirmware UpdatesExternal ServersTroubleshootingSupport

### External Servers ?

Add External Server

Server Type

☒ FTP ☐ SMB

Hostname/IP Address

Username

FolderPath

/

Alias

Port

21

Password

Add ServerTest Server

Alias	Hostname/IP Address	Type	Port	FolderPath	Actions
BFI	MyBackupSrvSMB	SMB	445	/bfi/	<a href="#">Remove</a> <a href="#">Edit</a>





- Energize Updates

## Security Definition Updates

Current Installed Version: 2.1.27267 (2017-09-25 18:49:46)  
[\(view release notes\)](#)

Latest Version: 2.1.27267 (2017-09-25 18:49:46)

Previous Version: 2.1.17395

Automatic Updates: ☒ On ☐ Off

## Reports Definition Updates

Current Installed Version: 1.0.009 (2019-07-03 14:38:55)  
[\(view release notes\)](#)

Latest Version: 1.0.009 (2019-07-03 14:38:55)

Automatic Updates: ☐ On ☒ Off

- Firmware updates

## Current Firmware Version

Current Installed Version: 1.0.0.232 (2019-07-11)  
[\(view release notes\)](#)

## Firmware Download

No updates available.





- 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

### Warning

Barracuda Firewall Insights has not received any data from one or more of your connected devices. Check your connections for the following device(s):

Name	Type	Serial	Last Data Received
BOSRV001:cudalab.internal	CloudGen Firewall	57c2b2b8b95404346fb12e281db5cdf5	20 minutes
BOSRV003:cudalab.internal	CloudGen Firewall	379511666296927b762d848af6e44048	38 minutes
BOSRV002:cudalab.internal	CloudGen Firewall	e5a1854625371d6a1cf6da50c305d373	81 minutes

Dismiss



# 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