

#### GENERAL INFORMATION

We use the term **device** for IP video door stations, access control devices or other peripheral devices that need a network connection. We use the term **firewall** for the 3rd-party firewall mentioned in this document.

# SYSTEM REQUIREMENTS

- DoorBird device
- Sophos Firewall

## ADDITIONAL INFORMATION

The following instructions show how to set up the firewall to allow the device to come online according to our online check: <u>https://www.doorbird.com/checkonline</u>

### INSTRUCTIONS

1) Log into the web interface of the firewall (in the standard configuration, the port is 4444, e.g. https://192.168.x.x:4444)



2) Configure an exception in the web filter settings (Sophos Admin  $\rightarrow$  Protect  $\rightarrow$  Web  $\rightarrow$  Exceptions  $\rightarrow$  Add exceptions)

CONTOR & ANALYZE	Policies	Policy Quota Status	User activities	Categories	URL groups	Exceptions	General settings	File types	Surfing quotes	
Current activities									Add except	
Reports									Add excep	puor
Zero-day protection	Name ar	nd description	•	Selection criteria 🖓			Skip			
Diagnostics		pdate pple Update without c g side effects.	ontent	Matching URLs: ^([A-Za-z0-9]*\.]?ap ^([A-Za-z0-9]*\.]?cdi			HTTPS decryption HTTPS certificate valida Malware and content so			
Rules and policies	Joannin,	g side erreets.		^[[A-Za-z0-9]*\.]?mz			Zero-day protection Policy checks	canning (35		
Intrusion prevention Web	Doorbird	1		Matching URLs:	orbird) pet) 2/		HTTPS decryption	ation		

Set a unique name for the exception and add the following URL matching patterns:

- ^([A-Za-z0-9.-]\*\.)?doorbird\.net\.?/
- api.doorbird.net

#### SOPHOS FIREWALL TROUBLESHOOTING



	e*				
esc	ription		6		
we	b traffic matching these criteria:			Skip the	e selected checks or actions:
	URL pattern matches				HTTPS decryption
	^[[A-Za-z0-9]*\.]?doorbird\.net\.?/	ø 0			HTTPS certificate validation
	api.doorbird.net	10			Malware and content scanning
	Search / Add	+			Zero-day protection Policy checks
	Add new item				
)	Add new item Source IP addresses (end-user's address)				
)					
)	Source IP addresses (end-user's address)				

Set the checkboxes as shown on the screenshot and save the settings to add the exception.

3.1) Configure an exception for the firewall (Sophos Admin  $\rightarrow$  Protect  $\rightarrow$  Rules & Policies  $\rightarrow$  Add Firewall Rule  $\rightarrow$  New Firewall Rule)

tule name *		Description		Rule position	
Enter Rule name		Enter Description		Bottom	· · · · · · · · · · · · · · · · · · ·
ction			1	Rule group	
Accept	-		116	Automatic	-
Log firewall traffic Logs traffic, matching this firewall rule, or default) or on the configured syslog serve				Automatically adds rule to an match with rule type a	n existing group based on fi Ind source-destination zone
OUICE lect the source zones, networks, and e rule applies to traffic from these so		e scheduled time period.			
		Source networks and devices *		During scheduled time	
urce zones *	0	Source networks and devices *	0	During scheduled time All the time	
urce zones *	0		٥	All the time	
ource zones *	٥		0	All the time	
Add new item Add new item Restination and services Restination zones, networks, ne rule applies to traffic to these destin	, devices, and se	Any Add new item	0	All the time Select to apply the rule	to a specific time period an day of the week
AN Add new item estination and services lect the destination zones, networks, e rule applies to traffic to these destin stination zones *	, devices, and se nations.	Any Add new item rvices. Destination networks *		All the time Select to apply the rule	
AN AN Add new item estination and services lect the destination zones, networks, a rule applies to traffic to these desti	, devices, and se	Any Add new item	0	All the time Select to apply the rule Services * HTTP	
AN AN Add new item Add new item estination and services ect the destination zones, networks, e rule applies to traffic to these desti stination zones *	, devices, and se nations.	Any Add new item rvices. Destination networks *		All the time Select to apply the rule	

All companies, logos and product names are registered trademarks of the respective companies. Errors and omissions excepted – Last Update 12/2023 - Copyright © ASSA ABLOY – www.doorbird.com



#### 3.2) Add a new FQDN host to the Destination Networks

Destination zones *		Destination networks *		Services *	
WAN	0	Doorbird	10	HTTP	10
				HTTPS	10
Add new item			Q	Add ne	witem
Match known users		Al types  Any Country of  apple.com box.com bo	it at group FQDN host	Services are cramo type	is based on a combination or protocols and ports

tination zones *		Destination networks *		
AN	0	Doorbird	10	
Add new item		Add new item		
Add FQDN host				
Name *	Doorb	ard		
FQDN *	Use wi	tbird net Idcard *** as a prefix in FQDN to resolve sub-dom imple, * exemple com	sins.	
FQDN host group				
		Add new item		
Security features				
Security features Veb filtering Web policy None Apply web category-based traffic	shaping	Malware and content scanning Scan HITP and decrypted HITPS Use zero-day protection		Filtering common web ports Use web proxy instead of DPI engine DPI engine or web proxy? Web proxy options
Security features Veb filtering Web policy None Apply web category-based traffic		Scan HTTP and decrypted HTTPs		Use web proxy instead of DPI engine
Security features Web filtering Web policy None Apply web category-based traffic and Block QUIC protocol	shaping	Scan HTTP and decrypted HTTP3 Use zero-day protection Scan FTP for malware		Use web proxy instead of DPI engine DPI engine or web proxy? Web proxy options
Security features Web filtering Web policy None Apply web catogory-based traffic Block QUIC protocol Configure Synchronized Secur	shaping	Scan HTTP and decrypted HTTP3 Use zero-day protection Scan FTP for malware		Use web proxy instead of DPI engine DPI engine or web proxy? Web proxy options
Security features Web filtering Web policy None Apply web category-based traffic Block QUIC protocol Configure Synchronized Secur Other security features	shaping îty Heartbe	Scan HTTP and decrypted HTTP3 Use zero-day protection Scan FTP for malware		Use web proxy instead of DPI engine DPI engine or web proxy? Web proxy options
Security features Web filtering Web policy None Apply web category-based traffic Block QUIC protocol Configure Synchronized Secur Other security features	shaping îty Heartbe	Scan HTTP and decrypted HTTP3 Use zero-day protection Scan FTP for malware		Use web proxy instead of DPI engine DPI engine or web proxy? Web proxy options Decrypt HTTPS during web proxy filtering
Security features  Web filtering  Web filtering  None  Apply web category-based traffic to Block QUIC protocol  Configure Synchronized Secur  Other security features dentify and control applications (App on None)	shaping ity Heartbe control)	Scan HTTP and decrypted HTTP3 Use zero-day protection Scan FTP for malware at		Use web proxy instead of DPI engine DPI engine or web proxy? Web proxy options Decrypt HTTPS during web proxy filtering DSCP marking
Security features  Web filtering Web policy None Apply web catogory-based traffic Block QUIC protocol  Configure Synchronized Secur Other security features Identify and control applications (App of	shaping ity Heartbe control)	Scan HTTP and decrypted HTTP3 Use zero-day protection Scan FTP for malware at		Use web proxy instead of DPI engine DPI engine or web proxy? Web proxy options Decrypt HTTPS during web proxy filtering DSCP marking

Configure the security features as shown in the screenshot.



#### SUPPORT INFORMATION

The instructions were tested with Sophos Firewall SFOS 19.5.3 MR-3-Build652 and a standard rule set.

In case further security settings are active, additional steps may be needed. We do not provide further support for the firewall that exceeds the information of this document.

Please contact your responsible IT administrator or the Sophos Support and provide them with the information provided: <u>https://www.doorbird.com/faq-single?faq=168</u>