

Time Sensitive Information!

These Configuration Changes Must Be Applied Ten Days Prior to Norcom Solutions Group Cut-Over

Watchguard Router Configuration For Norcom Solutions Group Cloud Telephony Deployment Document Version 2.2

May 6th, 2020

www.Norcom.tech



Table of Contents

- 1. Introduction
- 2. Enable Traffic Management & QoS Gobally
- 3. Enable QoS Marking on interfaces
- 4. Traffic Management
- 5. Create Firewall Policies (Inbound Outbound)
- 6. Whitelist Crexendo Servers

Read Me!

- 1. These changes must be applied before client implements their Norcom Solutions Group hosted telephony solution.
- 2. If you are <u>experienced</u> with business class firewalls and routers, please have your IT staff/contractor perform these changes for you.
- 3. Please read this entire document before attempting to make any changes.
- 4. If you have questions about this document, you can call 877-667-2661 to schedule an appointment with one of our firewall support specialists. We will attempt schedule your appointment within 24- 48 hours of your call to us so please allow adequate time.
- 5. After changes are completed please let your client or Norcom Solutions Group Customer Support specialist know.
- 6. Once completed, a Norcom Solutions Group technician will be requesting access or a collaborative web session to verify settings prior to customer cut over.

Introduction

This document is for IT administrators and illustrates configuration changes required on Watchguard firewall & router appliances to support Norcom Solutions Group's cloud communications telecommunications platform. This document assumes a basic network deployment consisting of one internal LAN network containing the IP phones and one WAN network connected to the Internet. While we strongly recommend a dedicated network for VoIP traffic, the instructions below can be used for a "converged" network whereby both VoIP and non-VoIP traffic share one physical WAN network. With basic modifications (such as adding access rules for additional interfaces); this configuration can be extrapolated for other network layouts. The screenshots below may vary slightly from what is displayed while configuring the device depending on model and OS software version. Setting values not mentioned may be left at default or changed as required for specific purposes.



Please call Norcom Solutions Group Customer Support at 877-667-2661 if you need any further information. Firewall changes can be in depth and you will need to schedule time with one of our specialists if you need assistance.

Screenshots and instructions are based on XTM25 running version 11.8.B432340.

We recommend loading the latest XTM OS (firmware).



Firewall Checklist

After applying the GUI configurations in this document, please take the appropriate screen shots to provide the firewall "verification" to Norcom Solutions Group.

Screen Shot #:	Configuration:	Completed:
1	System \rightarrow Global Settings \rightarrow Networking Tab (Traffic Management)	
2	Network \rightarrow Interfaces \rightarrow External \rightarrow Advanced Tab (Prioritize based on QoS Marking)	
3	Firewall \rightarrow Traffic Management \rightarrow Crexendo Traffic	
4	Firewall \rightarrow Firewall Policies (overview screen)	
5	Firewall → Firewall Policies → Crex Inbound Policy → Settings Tab	
6	Firewall → Firewall Policies → Crex Inbound Policy → Traffic Management Tab	
7	Firewall \rightarrow Firewall Policies \rightarrow Crex Inbound Policy \rightarrow Advanced Tab	
8	Firewall \rightarrow Firewall Policies \rightarrow Crex Outbound Policy \rightarrow Settings Tab	
9	Firewall → Firewall Policies → Crex Outbound Policy → Traffic Management Tab	
10	Firewall \rightarrow Firewall Policies \rightarrow Crex Outbound Policy \rightarrow Advanced Tab	
11	Firewall \rightarrow Blocked Sites \rightarrow Blocked Sites Exceptions Tab	



Enable Traffic Management & QoS

Note: default log in to Watchgaurd devices is: <u>https://xxx.xxx.1:8080</u> UN: admin PW: readwrite

System \rightarrow Global Settings \rightarrow Networking tab

NETWORK IREWALL SUBSCRIPTION SERVICES AUTHENTICATION VPN SYSTEM Information Feature Key NTP SNMP Managed Device Logging Diagnostic Log Global Settings Certificates Upgrade OS Backup Image Restore Image USB Drive Passphrase Configuration File About Traffic Management and QoS Image End Provide and SNAT action changes, clear active connections that use that SNAT action	SYSTEM STATUS	Global Settings	
FIREWALL The changes were saved successfully SUBSCRIPTION SERVICES AUTHENTICATION VPN SYSTEM Information Feature Key NTP SNMP Managed Device Logging Diagnostic Log Global Settings Upgrade OS Backup Image Restore Image USB Drive Passphrase Configuration File About TCP maximum segment size control About Traffic Management and QoS Capible all Traffic Management and QoS features Traffic Flow When an SNAT action changes, clear active connections that use that SNAT action	NETWORK	Giobal Octaings	
AUTHENTICATION VPN SYSTEM Information Feature Key NTP Signal General Networking Feature Key NTP Tr Signal General Networking Centrificates Copy General CCP Settings Certificates CCP Settings Certificates CCP Settings Certificates CCP Settings Certificates CCP Settings CConfiguration File About CCP maximum segment size control About CCP maximum segment size control About CCP maximum segment and QoS Feature All Copy Copy Center Copy Copy Copy Copy Copy Copy Copy Copy		The changes were saved successfully	
SYSTEM Information Feature Key Fragmentation req (PMTU) ✓ NTP ✓ Fragmentation req (PMTU) ✓ SNMP ✓ Time exceeded ✓ Port unreachable Managed Device ✓ Network unreachable ✓ Protocol unreachable Coging Diagnostic Log ✓ Restore Image ✓ Protocol unreachable Certificates Upgrade OS Enable TCP SyN checking TCP connection idle timeout 1 Hours ▼ USB Drive Pasphrase Configuration File Auto adjustment No adjustment No adjustment No adjustment Imit to 1460 Traffic Management and QoS ✓ Enable all Traffic Management and QoS features Traffic Flow When an SNAT action changes, clear active connections that use that SNAT action		General Networking	
Internation Importance Feature Key Importance NTP Importance SNMP Importance Managed Device Importance Logging Importance Diagnostic Log Importance Global Settings Importance Certificates Importance Upgrade OS Enable TCP SYN checking Backup Image TCP connection idle timeout Restore Image Importance USB Drive Passphrase Configuration File About About Importance Importance Importance Importance Importance Configuration File About About Importance Importance Importance Importance Importance Importance Importance Importance Importance Importance Importance Importance Importance About Importance Importance Importance Importance Importance	SYSTEM	ICMP Error Handling	
NTP SNMP Managed Device Logging Diagnostic Log Global Settings Certificates Upgrade OS Backup Image Restore Image USB Drive Passphrase Configuration File About TCP maximum segment size control Auto adjustment Limit to 1460 Traffic Management and QoS Enable all Traffic Management and QoS features Traffic Flow When an SNAT action changes, clear active connections that use that SNAT action 	Feature Key	Fragmentation req (PMTU)	Host unreachable
Managed Device Logging Logging Image Network unreachable Image Protocol unreachable Diagnostic Log Certificates Image Protocol unreachable Certificates Image Protocol unreachable Image Protocol unreachable Diagnostic Log Enable TCP Settings Image Protocol unreachable Certificates Image Protocol unreachable Image Protocol unreachable Restore Image Image Protocol unreachable Image Protocol unreachable USB Drive Enable TCP SYN checking Image Protocol unreachable VSB Drive Passphrase Image Protocol unreachable Configuration File About Image Protocol unreachable About Image Protocol unreachable Image Protocol unreachable Image Protocol unreachable Image Protocol unreachable Image Protocol unreachable USB Drive Passphrase Image Protocol unreachable Image Protocol unreachable VB Drive Passphrase Image Protocol unreachable Image Protocol unreachable About Image Protocol unreachable Image Protocol unreachable Image Protocol unreachable About Image Protocol unreachable Image Protocol unrea	SNMP	✓ Time exceeded	Port unreachable
Cartificates Upgrade OS Backup Image Enable TCP SYN checking Restore Image TCP connection idle timeout USB Drive Passphrase Configuration File TCP maximum segment size control About About Image No adjustment Limit to 1460 Traffic Management and QoS Image Enable all Traffic Management and QoS features Traffic Flow Image When an SNAT action changes, clear active connections that use that SNAT action	Managed Device Logging Diagnostic Log	Network unreachable	Protocol unreachable
Certificates TCP settings Wpgrade OS Backup Image Restore Image USB Drive Passphrase Configuration File About 1 Hours • About • Image • About • Image • Image • About • Image • Imag	Global Settings	TCD Settings	
Backup Image TCP connection idle timeout 1 Hours USB Drive Passphrase Configuration File TCP maximum segment size control About • Auto adjustment • No adjustment • Limit to 1460 Traffic Management and QoS ✓ Enable all Traffic Management and QoS features. Traffic Flow • When an SNAT action changes, clear active connections that use that SNAT action	Upgrade OS	Enable TCP SYN checking	
Configuration File About TCP maximum segment size control Auto adjustment No adjustment Limit to 1460 Traffic Management and QoS Enable all Traffic Management and QoS features Traffic Flow When an SNAT action changes, clear active connections that use that SNAT a 	Backup Image Restore Image USB Drive Passphrase	TCP connection idle timeout	Hours
Auto adjustment No adjustment Limit to 1460	Configuration File	TCP maximum segment size control	
 No adjustment Limit to 1460 Traffic Management and QoS Enable all Traffic Management and QoS features Traffic Flow When an SNAT action changes, clear active connections that use that SNAT a 	About	Auto adjustment	
 □ Limit to 1460 Traffic Management and QoS ✓ Enable all Traffic Management and QoS features Traffic Flow □ When an SNAT action changes, clear active connections that use that SNAT a 		 No adjustment 	
Traffic Management and QoS Enable all Traffic Management and QoS features Traffic Flow When an SNAT action changes, clear active connections that use that SNAT a		Limit to 1460	
 Enable all Traffic Management and QoS features Traffic Flow When an SNAT action changes, clear active connections that use that SNAT a 		Traffic Management and QoS	
Traffic Flow When an SNAT action changes, clear active connections that use that SNAT a		Enable all Traffic Management and Q	oS features
When an SNAT action changes, clear active connections that use that SNAT a		Traffic Flow	
		When an SNAT action changes, clear	r active connections that use that SNAT ac

- Click (check) the "Enable all Traffic Management and QoS features
- Click Save



Enable QoS Marking on WAN and LAN Interfaces

Network → Interfaces

- Select on the interface 0 (External/WAN)
 - This will also need to be configured on the X1 (or Active LAN port).
 - Please repeat on the LAN port
- Click "edit"

Configure Interfaces in	Mixed Routing Mode	¥			
Interface ≑	Туре	Name (Alias)	IPv4 Address	IPv6 Address	NIC Config
o	External	External	DHCP		Auto Negotiate
1	Trusted	Trusted	10.0.1.1/24		Auto Negotiate
2	Trusted	Optional-1	10.0.3.1/24		Auto Negotiate
3	Bridge	Optional-2			Auto Negotiate
4	Trusted	Optional-3	10.0.4.1/24		Auto Negotiate



• Click on the "Advanced" tab

	Interfaceo (Edit	
SYSTEM STATUS	Interfaces / Edit	
Interfaces Link Aggregation	Interface Name (Alias)	External
VLAN Bridge Multi-WAN	Interface Description	
Dynamic DNS NAT	Interface Type	External •
Dynamic Routing Gateway Wireless Controller	IPv4 IPv6 Secondary	/ Advanced
FIREWALL	NIC Softings	
SUBSCRIPTION SERVICES	Nic Settings	
AUTHENTICATION	Link Speed	Auto Negotiate 🔹
/PN SYSTEM	MTU	1500
		Override MAC Address
	Dente Fragmant (DE) Dit Catting	r for IDSoc (External only)
	Don't Fragment (DF) Bit Setting) for the sec (External only)
	Copy - Original DF bit setting) of the IPSec packet is copied to the encapsulating header
	Set - Firebox cannot fragmen	It IPSec packets regardless of the original bit setting
	 Clear - Firebox can tragment 	IPSec packets regardless of the original bit setting
	PMTU Setting for IPSec (Extern	nal only)
	Minimum MTU	576
	Aging time of learned PMTU	10 minutes
	QoS	
	Marking type	IP Precedence v
	Marking method	Preserve v
	Value	0 (Normal)
	Value	0 (Normal) Prioritize traffic based on QoS Marking
	Value Static MAC/IP Address Binding	0 (Normal) ▼ ✓ Prioritize traffic based on QoS Marking
	Value Static MAC/IP Address Binding	0 (Normal)
	Value Static MAC/IP Address Binding Add Remove	0 (Normal)
	Value Static MAC/IP Address Binding Add Remove Only allow traffic sent from or	0 (Normal)

- Click "Prioritize traffic based on QoS Marking
- Click Save



Traffic Management

Firewall → Traffic Management

DA SHBOARD SYSTEM STATUS	Traffic Management	
ETWORK	Enable Traffic Management	
Firewall Policies Mobile VPN Policies	Policies Interfaces	
Proxy Actions Traffic Management	Traffic Management Actions	
SNAT		Name 🗢
Default Packet Handling Blocked Sites	Add Edit Remove	
Blocked Ports	Traffic Management Policies	Select action 🔻
JESCRIPTION SERVICES	Policy Name	Traffic Mana
	FTP	
STEM	WatchGuard Web UI	
	Ping Ping	
	WatchGuard	
	Outgoing	

- Click the "Add" button
- Create a Crexendo Traffic Management scope
 - <u>Name</u>: Crexendo Traffic
 - Click the "Add" button under "Guaranteed Bandwidth for Outgoing traffic"

Interfac	e		Ŧ	
Minimu	m <mark>500</mark>	Kpbs		
Maximu	m 1000	Kpbs		

- A "guaranteed Bandwidth" pop-up window will appear. Enter the following:
 - o <u>Interface</u>: External
 - Minimum: Enter the minimum speed in Kpbs that you would like to reserve for voice Traffic. As a rule of thumb I would use this formula:
 <u>1/2</u> Total number of phones * 100K
 - <u>Maximum</u>: Enter the max bandwidth needed using: <u>Total number of phones *100K</u> Note: Value of "0" (this will allow the traffic management to burst if needed)
- Click "OK"
- Click "Save"



Create Firewall Policies

Firewall → click "Add Policy"

ASHBOARD											
YSTEM STATUS	Po	licies									
ETWORK											
REWALL	Act	ion 🗸	Add Pol	licy				Filt	ter None		
Firewall Policies Mobile VPN Policies		Actio	Policy Nam	Туре	From	To	Port	PBR	Application	Tags	
Aliases Draws Actions		1	E FTP	FTP	Any-Trusted	Any-Extern	tcp:21				1
Fraffic Management		1	WatchGu	WG-Firewa	Any-Trusted	Firebox	tcp:8080				1
Scheduling SNAT		1	Ping	Ping	Any-Trusted	Any	ICMP (type:				1
Default Packet Handling		1	WatchGu	WG-Firebox	Any-Trusted	Firebox	tcp:4105 tc				
Blocked Sites Blocked Ports		1	Outgoing	TCP-UDP	Any-Trusted	Any-Extern	tcp:0 udp:0				
UBSCRIPTION SERVICES	Dis	able p	olicy Auto-Or	rder mode							
UTHENTICATION											
Blocked Ports UBSCRIPTION SERVICES UTHENTICATION	Dis	able p	olicy Auto-Or	rder mode	Any-Irusted	Any-Extern	tcp:0 udp:0				

STEM STATUS	Firewall Policies /	Add Firewall Pol	licy				
ETWORK	Policy Name Crexe	ndoPorts					
irewall Policies Aobile VPN Policies Viases	Select a policy type						
rafic Management	- racket ritter	Allow Hotsp	ot Session Mgmt	*			
Scheduling SNAT	Proxies	DNS-proxy			DNS-I	ncoming	
)efault Packet Handling Nocked Sites	Custom	CrexendoP	orts	•	Add	Edit	Remove
JBSCRIPTION SERVICES	Po	rt *		Protoc	ol		
UTHENTICATION	16000-17999	it v	UDP	11000			
PN	11780-11800	UDP				_	
rstem	5060		UDP				
	9000 UDP						

- Select the "Custom" Policy Type
- Select "Add"
 - Enter the following information:
 - <u>Policy Name</u>: Crexendo Ports
 - Ports:
 - 16000-17999 UDP
 - 11780-11800 UDP
 - 5060 UDP
 - 9000 UDP
- Click Add Policy



Create the Inbound Policy

Once the custom policy type is created you can create the Inbound and Outbound Policies.

Inbound Policy:

- Click "Add Policy"
- <u>Name Policy</u>: Crexendo Inbound
- Select "Custom" radio button
- Choose "Crexendo Ports" in drop down
- Click "Add Policy"

Name Crexendo Inbound	Enable	
Settings Traffic Management Scheduling Advanced		
Connections are Allowed •	Policy Type Cre	xendoPorts
	Port 🗇	Protocol
	16000-17999	UDP
	11780-11800	
	5060	
From *	Any	To 👙
Add Remove	Add Remo	ve
Auto-block sites that attempt to connect		
Specify custom idle timeout 180 seconds		

- Enter the following:
 - Ensure Policy Name is: Crexendo Inbound
 - Connections are:

Allowed 184.178.213.0/24

Change From network: 184.1
 Change To network: Any

www.Norcom.tech



Continue Inbound Policy Creation

- Click on the "Traffic Management" tab

 Select "Crexendo Traffic" from the drop down box

Firewall Policies / Add				10
Name	Crexendo Inbound	Enable		ľ
Settings Traffic Management	Scheduling Advanced			I
Fraffic Management Action	٣			I
Traffic Management Acti	on Settings			U
Name	Crexendo Traffic			Ľ
Description	Description			U
Guaranteed Bandwidth 1	for Outgoing Traffic			U
Outg	oing Interface 🐡	Minimum bandwidth (Kbps)	Maximum bandwidth (Kbps)	ш
External		500	1000	ш
Add Edit Remove				l
Save				J



Continue Inbound Policy Creation

- Click on the "Advanced" tab
 - Uncheck the 1-to-1 NAT
 - o Check QoS "Override per-interface settings" DSCP
 - Marketing type:
 - Marking Method: • Assign
 - Value:
 - Proritize traffic based on: QoS Marking

46 (ĔF)

Click Save

WatchGuard Firew	are XTM Web UI
DASHBOARD	
SYSTEM STATUS	Firewall Policies / Edit
NETWORK	
FIREWALL	Name Crexendo Inbound
Firewall Policies	
Aliases	
Proxy Actions Traffic Management	Settings Traffic Management Scheduling Advanced
Scheduling	
SNAT	Comment
Blocked Sites	Policy added on 2016-09-009T14:56:00-07:00.
Blocked Ports	
SUBSCRIPTION SERVICES	ΝΔΤ
AUTHENTICATION	1 to t NAT takes preventiones if the traffic qualifies for both rules
VPN	1 to 1 NAT (Hes Network MAT estime)
SYSTEM	
	Use Network NAT settings
	All traffic in this policy
	Set source IP 0.0.0.0
	Sticky Connection
	Override Multi-WAN sticky connection settings
	Enable sticky connection 3 minutes
	ICMP Error Handling
	Use policy-based ICMP error handling
	Fragmentation Req(PMTU) Host unreachable
	Network unreachable
	Connection Rate (per second)
	Specify Connection Rate 100
	Qo S
	Override per-interface settings
	Marking Type DSCP v
	Marking method Assign
	Value 46 (EF)
	Prioritize traffic based on QoS Marking
	Value 0 (Normal)
	Save Cancel



Create Outbound Policy

• Click "Add Policy"

DASHBOARD											
SYSTEM STATUS	Polic	cies									
NETWORK											
FIREWALL	Actio	n -	Add Policy						Filter	None	*
Firewall Policies Mobile VPN Policies		Action	Policy Name	Туре	From	То	Port	PBR	Application Cont	n Tags	
Proxy Actions		/	र्देश <u>FTP</u>	FTP	Any-Trusted Any-O	Any-External	tcp:21				
Traffic Management		/	WatchGuard We	WG-Fireware-XTM	Any-Trusted Any-O	Firebox	tcp:8080				
SNAT		~	Ping	Ping	Any-Trusted Any-O	Any	ICMP (type: 8, cod				
Default Packet Handling		~	WatchGuard	WG-Firebox-Mgmt	Any-Trusted Any-O	Firebox	tcp:4105 tcp:4117				
Blocked Sites Blocked Ports		⁄₽	Crexendo Inbo	CrexendoPorts	Any	184.178.213.0/24	udp:16000-16999				
SUBSCRIPTION SERVICES		~	Outgoing	TCP-UDP	Any-Trusted Any-O	Any-External	tcp:0 udp:0				
AUTHENTICATION	Disa	ble polic	v Auto-Order mode								

- Enter the following:
 - Policy Name:Policy Type:
- Crexendo Outbound
- Customer \rightarrow Crexendo Ports (in drop down)
- Click Add Policy
- Enter the following:
 - Ensure Policy Name is: Crexendo Outbound
 - Connections are:
- Allowed
- Change From network: Any
- Change To network:

184.178.213.0/24

DASHBOARD	Firewall Dollaise / Add					
SYSTEM STATUS	Firewaii Policies / Add					
	Name Crevendo Outbound					
Firewall Policies Mobile VPN Policies Aliases Proxy Actions Traffic Management	Settings Traffic Management Scheduling Advanced					
Scheduling	Connections are Allowed Policy Type CrexendoPorts					
Default Packet Handling	Port * Protocol					
Blocked Sites	16000-17999 UDP					
	11780-11800 UDP					
	5060 UDP					
/PN	9000 UDP					
SYSTEM						
	From the					
	Any 2,184,176,213.0/24					
	Add Remove Add Remove					
	Specify custom idle timeout 180 seconds					



Continued Outbound Policy

• Click "Traffic Management" tab

 $_{\odot}$ $_{\odot}$ Choose the "Crexendo Traffic" from the drop down

	Name	Crexendo Outbound	Enable					
ttings	Traffic Management	Scheduling A	Advanced					
c Manage	ment Action							
exendo Tra	affic	Y						
Traffic Management Action Settings								
	Name	Crexendo Traffic						
		Description						
	Description	Description						
Guarant	Description eed Bandwidth	for Outgoing Trat	ffic					
Guarant	Description eed Bandwidth Outgoing Inte	for Outgoing Trat	ffic Minimum bandwidth (Kbps)	Maximum bandwidth (Kbps)				
_	Description	Description						



Continued Outbound Policy

- Click on the "Advanced" tab
 - Uncheck 1-to-1 NAT
- Click "Save"

Name			
	Crexendo Outbound		•
Sottings Traffic Managem	ant Schoduling Advanced		
	Auvanceu		
Comment			
Policy added on 2016-09-009T1	15:07:12-07:00.		
NAT			2
1-to-t NAT takes precedence if th	e traffic qualifies for both rules.		
1-to-1 NAT (Use Network NA	T settings)		
Dynamic NAT			
All traffic in this policy			
Set source IP 0.0.0.0			
Sticky Connection	apartian acttings		
Enable sticky connection	minutes		
Enable slicky connection	minutes		
CMP Error Handling			
Use policy-based ICMP error	handling		
Fragmentation Req(PMTU)) e Host unreachable		Time Exceeded
Network unreachable	Port unreachable		Protocol unreachable
Connection Rate (per second)		
Connection Rate (per second))		
Connection Rate (per second)	0		
Connection Rate (per second) Specify Connection Rate))0		
Connection Rate (per second) Specify Connection Rate 10 Qo S Override per-interface setting))0 s		
Connection Rate (per second) Specify Connection Rate 10 Qo S Override per-interface setting Marking Type) s DSCP	¥	
Connection Rate (per second) Specify Connection Rate 10 Qo S Override per-interface setting Marking Type Marking method	0 s DSCP Preserve	•	
Connection Rate (per second) Specify Connection Rate 10 Qo S Override per-interface setting Marking Type Marking method) S DSCP Preserve 0 (Rest Effort)	•	
Connection Rate (per second) Specify Connection Rate 10 Qo S Override per-interface setting Marking Type Marking method Value) s DSCP Preserve 0 (Best Effort)	* *	
Connection Rate (per second) Specify Connection Rate 10 Qo S Override per-interface setting Marking Type Marking method Value Prioritize traffic based on) DSCP Preserve 0 (Best Effort) Custom Value	* * *	
Connection Rate (per second) Specify Connection Rate 10 Qo S Override per-interface setting Marking Type Marking method Value Prioritize traffic based on Value	DSCP Preserve 0 (Best Effort) Custom Value 0 (Normal)	* * *	
Connection Rate (per second) Specify Connection Rate 10 Qo S Override per-interface setting Marking Type Marking method Value Prioritize traffic based on Value) S DSCP Preserve 0 (Best Effort) Custom Value 0 (Normal)	* * *	
Connection Rate (per second) Specify Connection Rate 10 Qo S Override per-interface setting Marking Type Marking method Value Prioritize traffic based on Value) S DSCP Preserve 0 (Best Effort) Custom Value 0 (Normal)	* * *	



Whitelist Crexendo Servers

Firewall → Blocked Sites → Blocked Sites Exceptions tab

WatchGuard Firew	User: admin Help Logout	
DASHBOARD SYSTEM STATUS NETWORK FIREWALL Firewall Policies Mobile VPN Policies Aliases	Blocked Sites Blocked Sites Exceptions Auto Blocked Blocked Site Exceptions	
Proxy Actions Traffic Management Scheduling SNAT	Blocked Site Exceptions 184.178.213.0/24	Description Cexendo Servers
Default Packet Handling Blocked Sites Blocked Ports SUBSCRIPTION SERVICES	Add Remove	

- Add the Crexendo Servers/subnet to the "Exclusion" list
 184.178.213.0/24
- Click "Save"

Note: This will prevent the Watchguard from accidentally blocking SIP traffic based on the port scan IPS policies.



Document Revision History

Version	Reason for Change	Date
1.0 Draft	Initial Draft Document	October 18, 2013
2.0 Draft	Updated to reflect new web GUI and white list Crexendo subnets to resolve port scan scenario.	August 8, 2016
2.1	Firewall Checklist added	March 17 th , 2017
2.2	Added Addition RTP UDP ports	May 6 th , 2020