NORCOM Solutions Group powered by crexendo® ride the cloud

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

Read Me!

1. These changes must be applied before client implements their Norcom Solutions Group hosted telephony solution.
2. If you are experienced 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

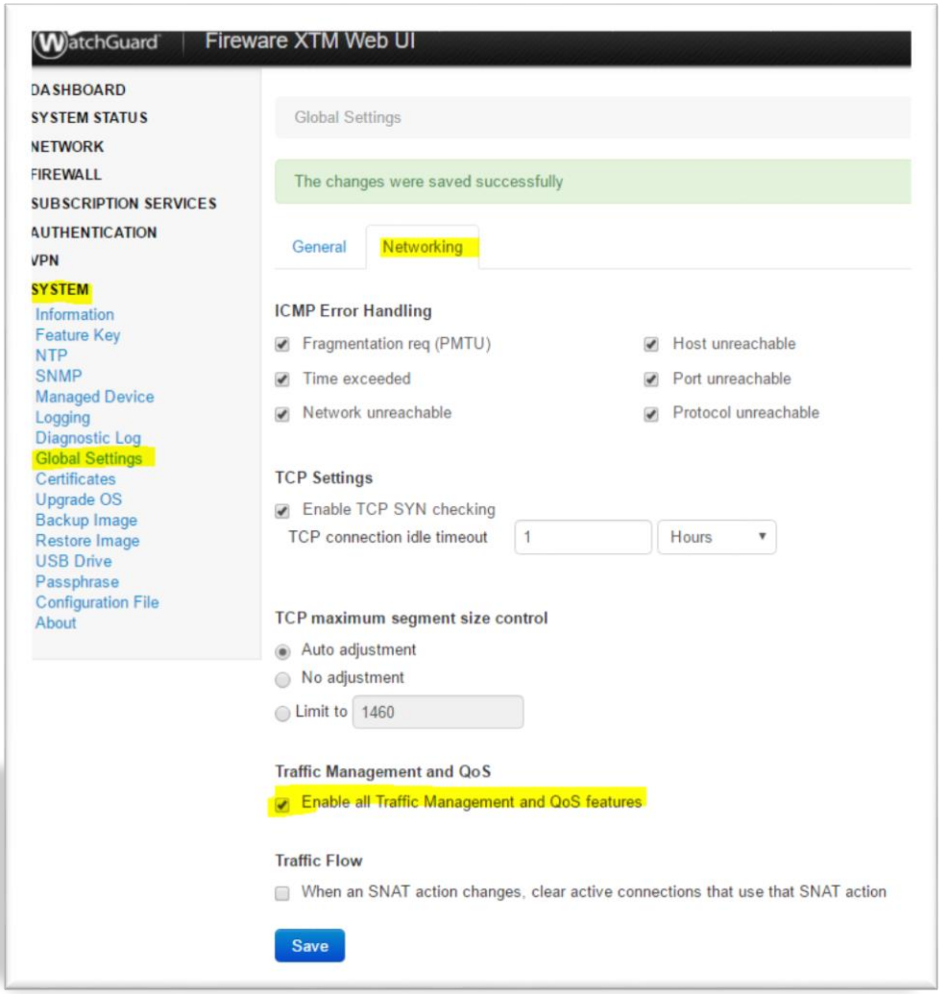
After applying the GUI configurations in this document, please take the appropriate screen shots to provide the firewall “verification” to Norcom Solutions Group.

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

Enable Traffic Management & QoS

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

System → Global Settings → Networking tab



Global Settings

The changes were saved successfully

General | Networking

ICMP Error Handling

☑ Fragmentation req (PMTU) ☑ Host unreachable
☑ Time exceeded ☑ Port unreachable
☑ Network unreachable ☑ Protocol unreachable

TCP Settings

☑ Enable TCP SYN checking
TCP connection idle timeout: 1 Hours ▾

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 action

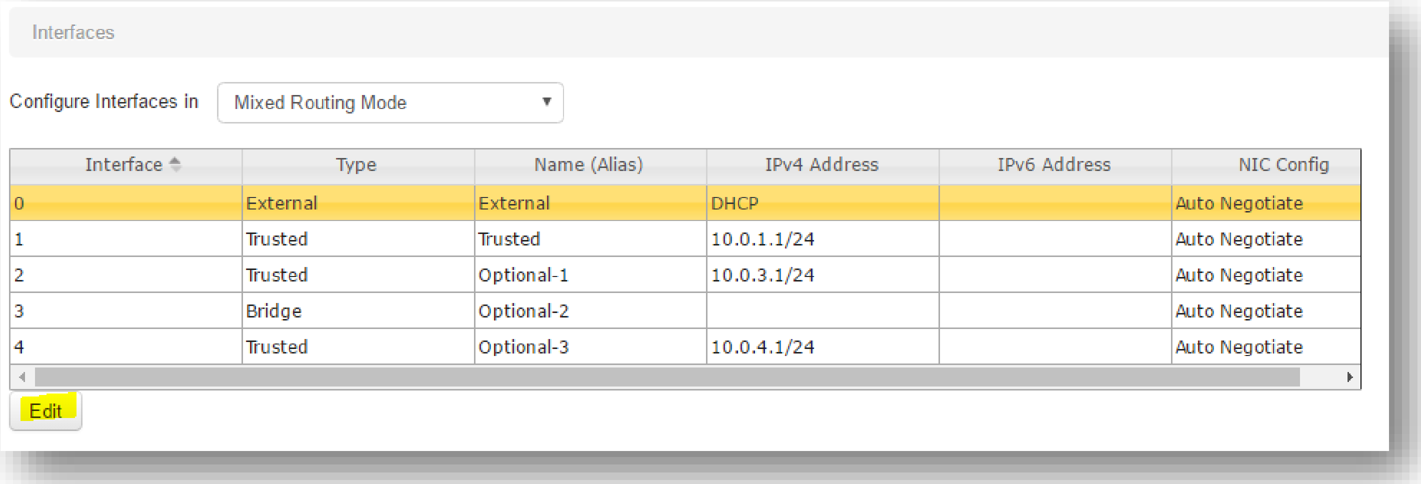
Save

- 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”

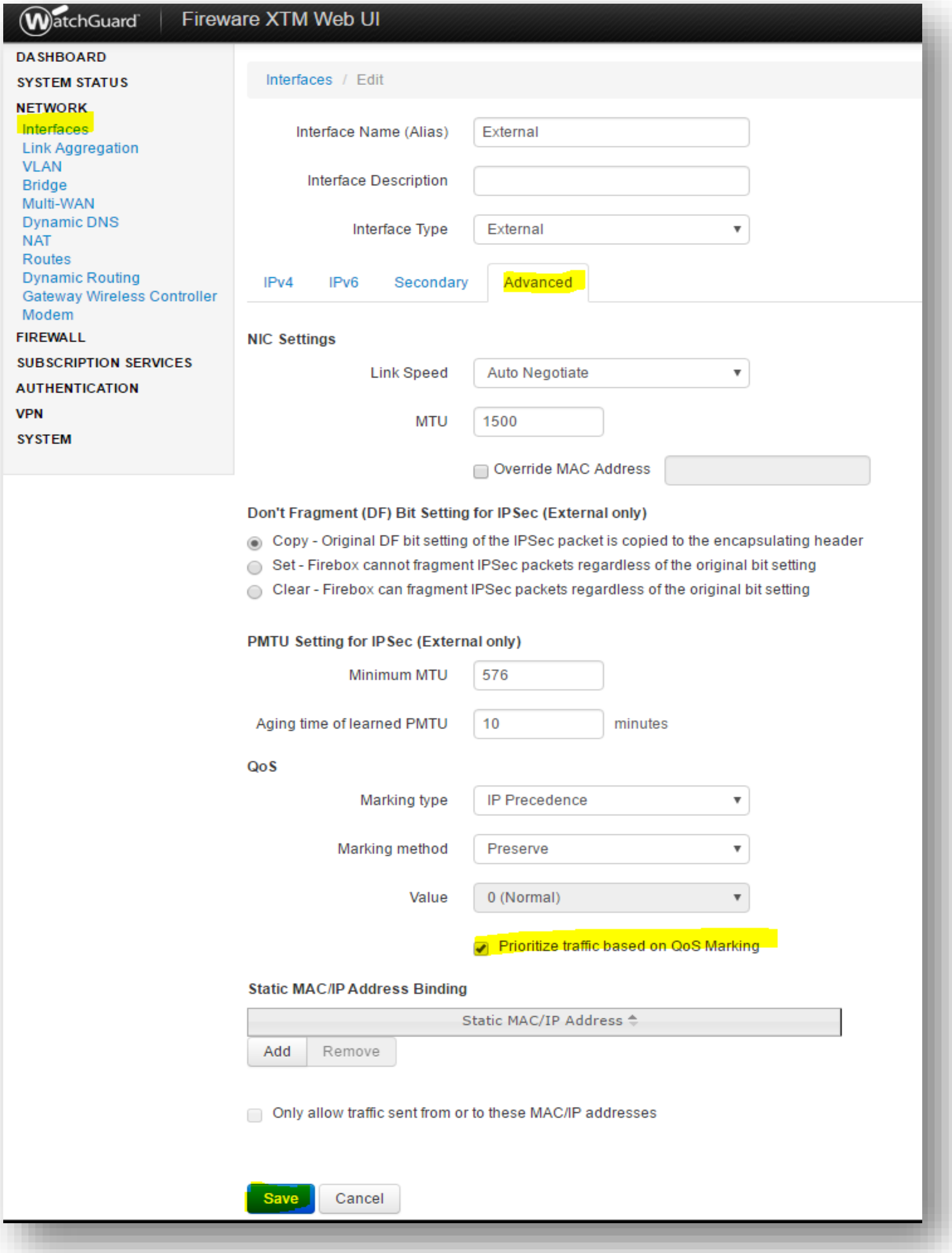


Interfaces

Configure Interfaces in Mixed Routing Mode ▾

Interface ▲	Type	Name (Alias)	IPv4 Address	IPv6 Address	NIC Config
0	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



Interface Name (Alias): External

Interface Description:

Interface Type: External

NIC Settings

Link Speed: Auto Negotiate

MTU: 1500

☐ Override MAC Address

Don't Fragment (DF) Bit Setting for IPSec (External only)

● Copy - Original DF bit setting of the IPSec packet is copied to the encapsulating header
○ Set - Firebox cannot fragment IPSec packets regardless of the original bit setting
○ Clear - Firebox can fragment IPSec packets regardless of the original bit setting

PMTU Setting for IPSec (External only)

Minimum MTU: 576

Aging time of learned PMTU: 10 minutes

QoS

Marking type: IP Precedence

Marking method: Preserve

Value: 0 (Normal)

☑ Prioritize traffic based on QoS Marking

Static MAC/IP Address Binding

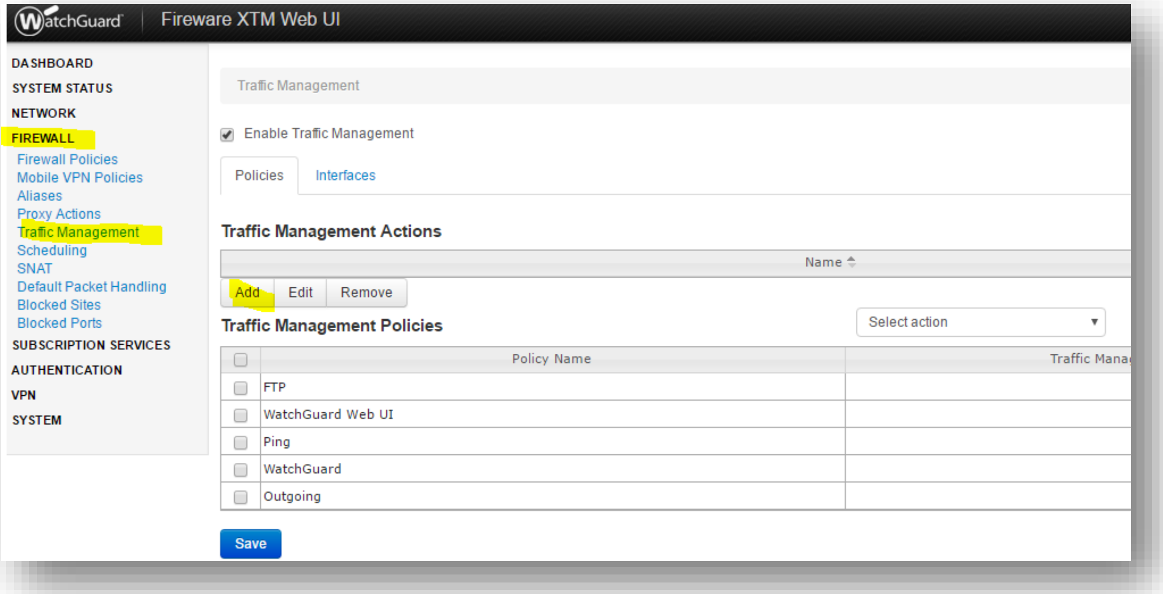
Static MAC/IP Address

☐ Only allow traffic sent from or to these MAC/IP addresses

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

Traffic Management

Firewall → Traffic Management



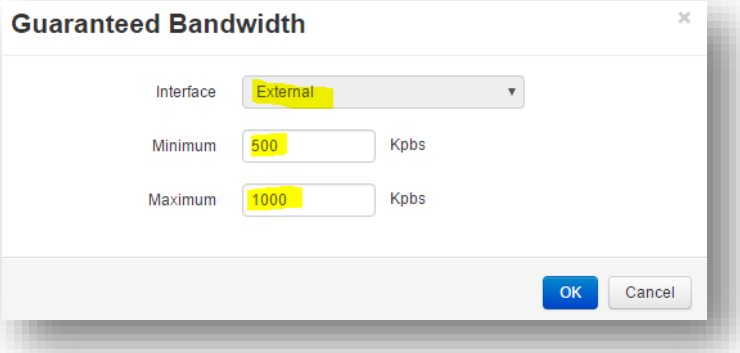
☑ Enable Trafic Management

Traffic Management Actions

Traffic Management Policies

□	Policy Name	Traffic Mana
□	FTP	
□	WatchGuard Web UI	
□	Ping	
□	WatchGuard	
□	Outgoing	

- Click the “Add” button
- Create a Crexendo Traffic Management scope
  - Name: Crexendo Traffic
    - Click the “Add” button under “Guaranteed Bandwidth for Outgoing traffic”



Interface: External

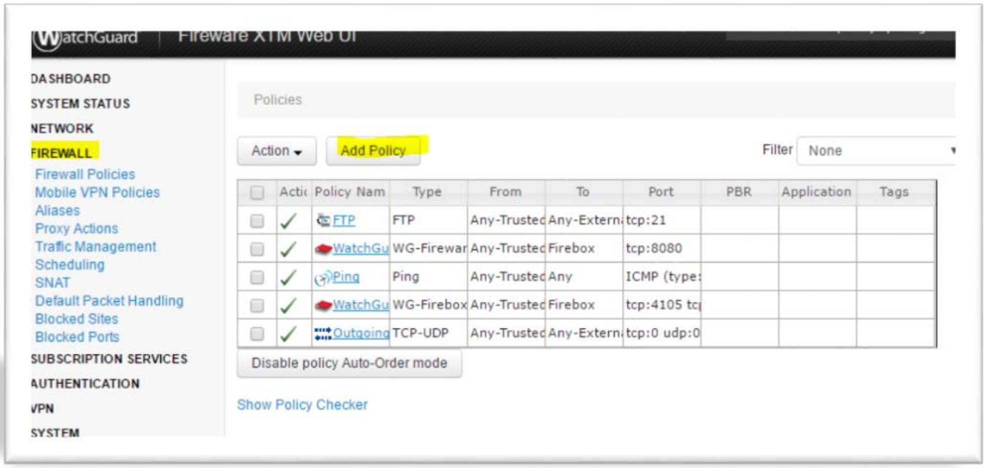
Minimum: 500 Kpbs

Maximum: 1000 Kpbs

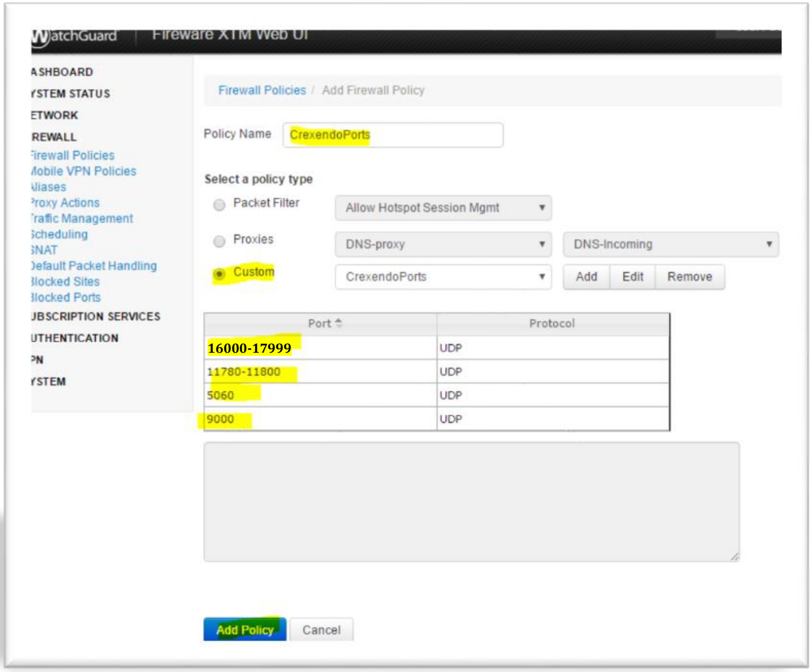
- A “guaranteed Bandwidth” pop-up window will appear. Enter the following:
  - Interface: External
  - Minimum: Enter the minimum speed in Kpbs that you would like to reserve for voice Traffic. As a rule of thumb I would use this formula:
    ½ Total number of phones * 100K
  - Maximum: Enter the max bandwidth needed using:
    Total number of phones *100K
    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”



□	Actic	Policy Nam	Type	From	To	Port	PBR	Application	Tags
□	✓	FTP	FTP	Any-Trusted	Any-Extern	tcp:21			
□	✓	WatchGu	WG-Firewar	Any-Trusted	Firebox	tcp:8080			
□	✓	Ping	Ping	Any-Trusted	Any	ICMP (type:			
□	✓	WatchGu	WG-Firebox	Any-Trusted	Firebox	tcp:4105 tc			
□	✓	Outgoing	TCP-UDP	Any-Trusted	Any-Extern	tcp:0 udp:0			



Policy Name: CrexendoPorts

Select a policy type

○ Packet Filter — Allow Hotspot Session Mgmt

○ Proxies — DNS-proxy — DNS-Incoming

● Custom — CrexendoPorts

Port	Protocol
16000-17999	UDP
11780-11800	UDP
5060	UDP
9000	UDP

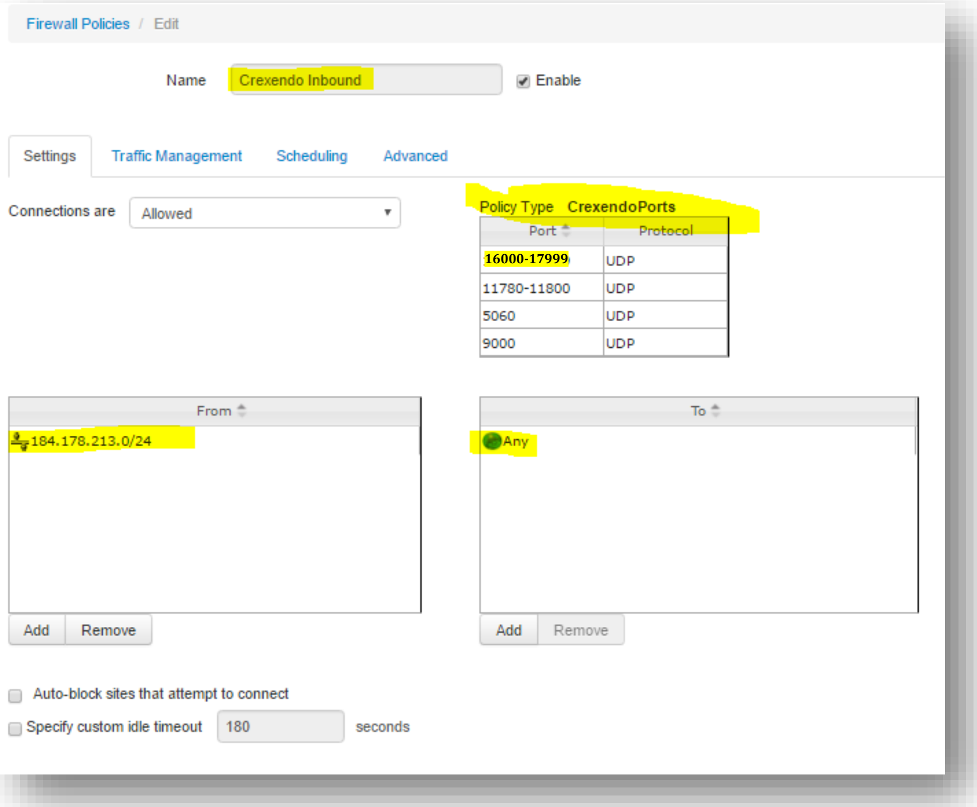
- Select the “Custom” Policy Type
- Select “Add”
  - Enter the following information:
    - Policy Name: Crexendo Ports
    - Ports:
      - 16000-17999 UDP
      - 11780-11800 UDP
      - 5060 UDP
      - 9000 UDP
- Click Add Policy

Create the Inbound Policy

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

Inbound Policy:

- Click “Add Policy”
- Name Policy: Crexendo Inbound
- Select “Custom” radio button
- Choose “Crexendo Ports” in drop down
- Click “Add Policy”



Name: Crexendo Inbound ☑ Enable

Connections are: Allowed

Policy Type: CrexendoPorts

Port	Protocol
16000-17999	UDP
11780-11800	UDP
5060	UDP
9000	UDP

From: 184.178.213.0/24

To: Any

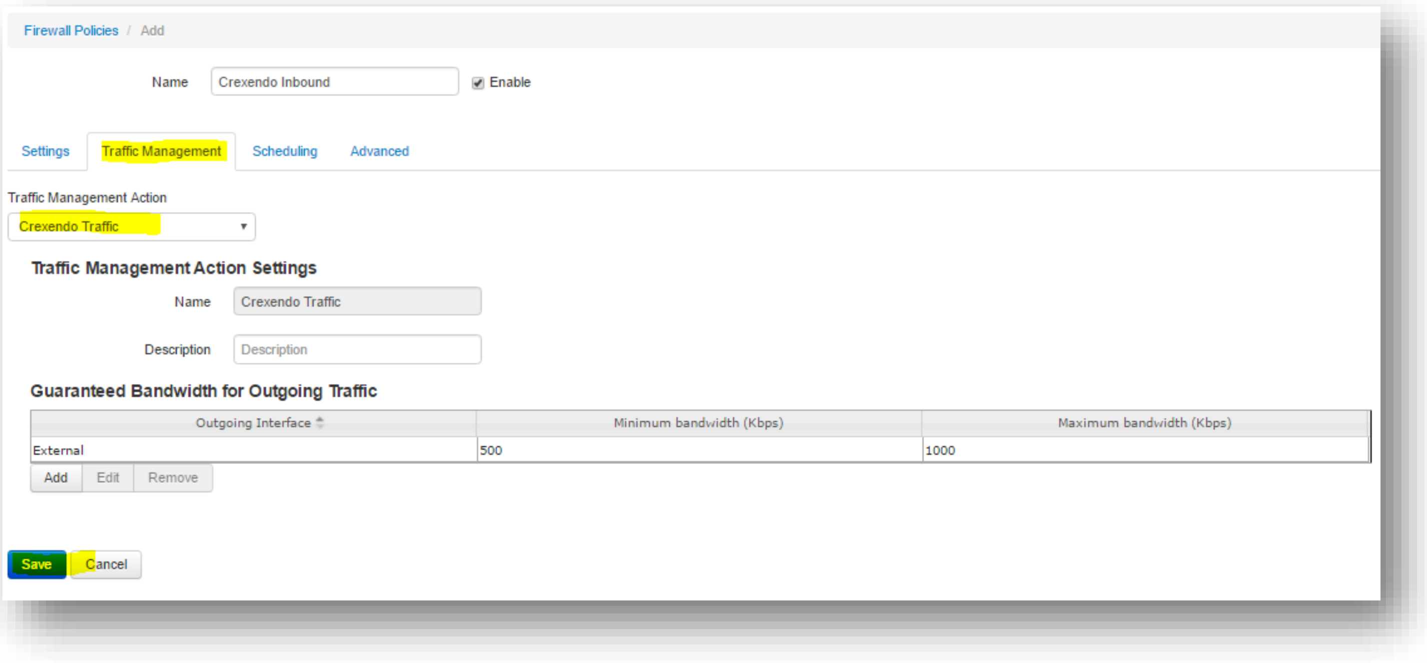
□ Auto-block sites that attempt to connect

□ Specify custom idle timeout 180 seconds

- Enter the following:
  - Ensure Policy Name is: Crexendo Inbound
  - Connections are: Allowed
  - Change From network: 184.178.213.0/24
  - Change To network: Any

Continue Inbound Policy Creation

- Click on the “Traffic Management” tab
    - Select “Crexendo Traffic” from the drop down box



Firewall Policies / Add

Name: Crexendo Inbound ☑ Enable

Traffic Management Action: Crexendo Traffic

Traffic Management Action Settings

Name: Crexendo Traffic

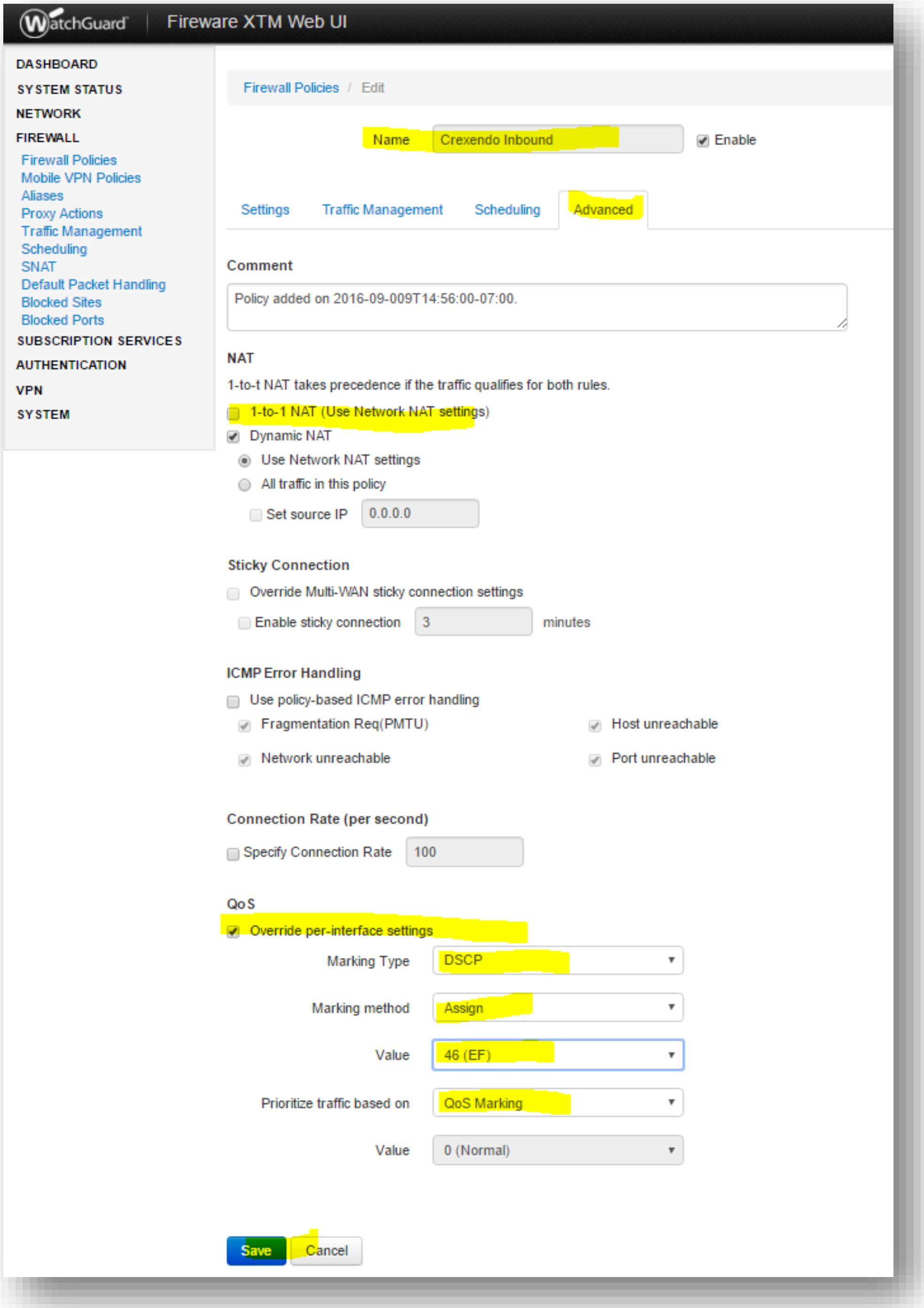
Description: Description

Guaranteed Bandwidth for Outgoing Traffic

Outgoing Interface	Minimum bandwidth (Kbps)	Maximum bandwidth (Kbps)
External	500	1000

Continue Inbound Policy Creation

- Click on the “Advanced” tab
  - Uncheck the 1-to-1 NAT
  - Check QoS “Override per-interface settings”
    - Marketing type: DSCP
    - Marking Method: Assign
    - Value: 46 (EF)
    - Proritize traffic based on: QoS Marking
- Click Save



Name: Crexendo Inbound ☑ Enable

Comment

Policy added on 2016-09-009T14:56:00-07:00.

NAT

1-to-t NAT takes precedence if the traffic qualifies for both rules.

☐ 1-to-1 NAT (Use Network NAT settings)

☑ Dynamic NAT

● 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 ☑ Port unreachable

Connection Rate (per second)

☐ Specify Connection Rate 100

QoS

☑ Override per-interface settings

Marking Type: DSCP

Marking method: Assign

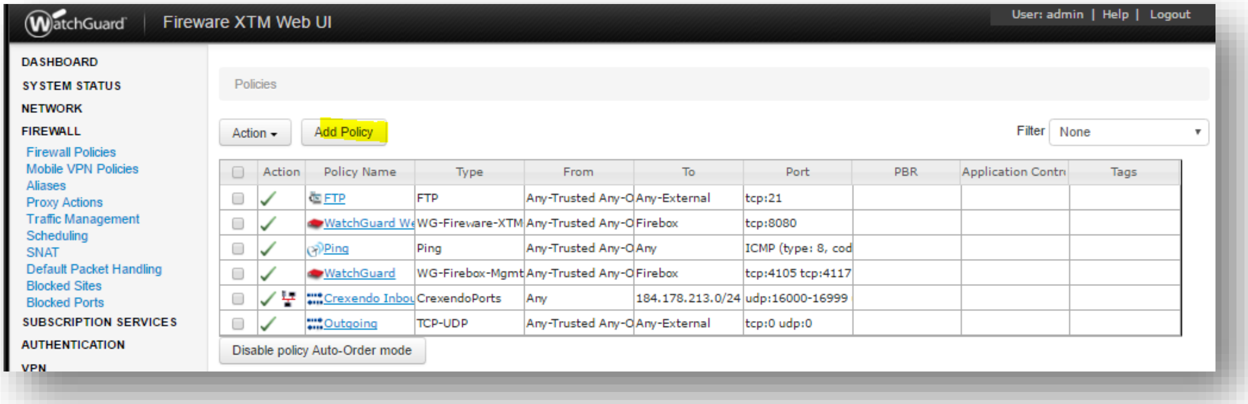
Value: 46 (EF)

Prioritize traffic based on: QoS Marking

Value: 0 (Normal)

Create Outbound Policy

- Click “Add Policy”

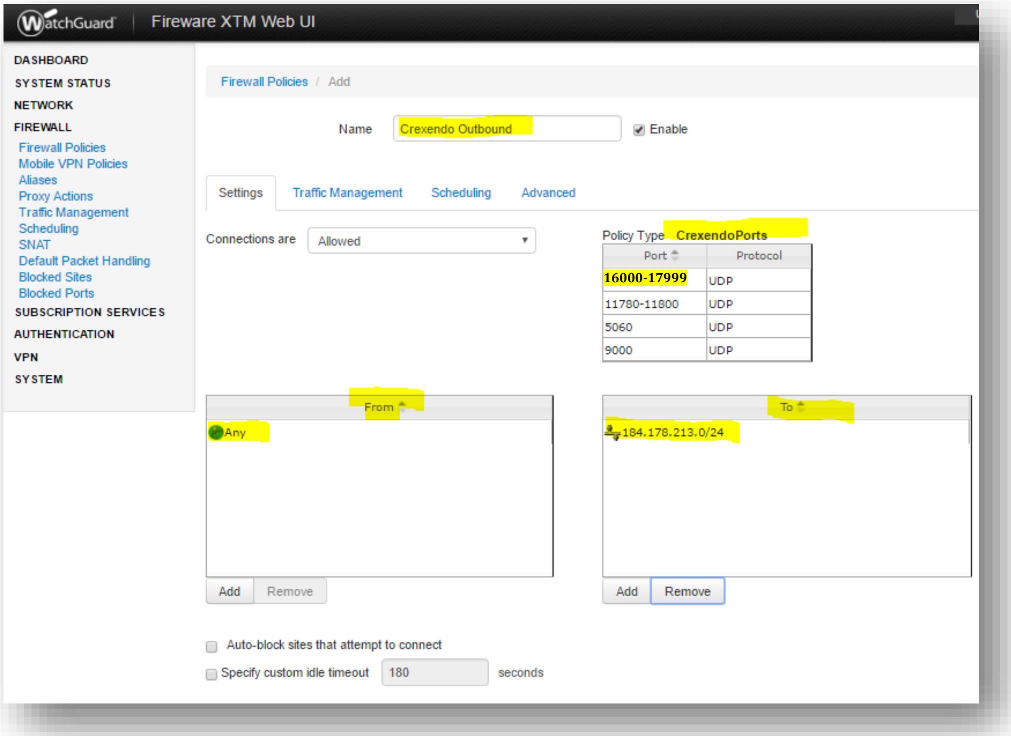


Filter: None

□	Action	Policy Name	Type	From	To	Port	PBR	Application Contr	Tags
□	✓	FTP	FTP	Any-Trusted Any-O	Any-External	tcp:21			
□	✓	WatchGuard We	WG-Fireware-XTM	Any-Trusted Any-O	Firebox	tcp:8080			
□	✓	Ping	Ping	Any-Trusted Any-O	Any	ICMP (type: 8, cod			
□	✓	WatchGuard	WG-Firebox-Mgmt	Any-Trusted Any-O	Firebox	tcp:4105 tcp:4117			
□	✓	Crexendo Inbou	CrexendoPorts	Any	184.178.213.0/24	udp:16000-16999			
□	✓	Outgoing	TCP-UDP	Any-Trusted Any-O	Any-External	tcp:0 udp:0			

- Enter the following:
  - Policy Name: Crexendo Outbound
  - Policy Type: Customer → 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



Name: Crexendo Outbound ☑ Enable

Connections are: Allowed

Policy Type: CrexendoPorts

Port	Protocol
16000-17999	UDP
11780-11800	UDP
5060	UDP
9000	UDP

From: Any

To: 184.178.213.0/24

□ Auto-block sites that attempt to connect

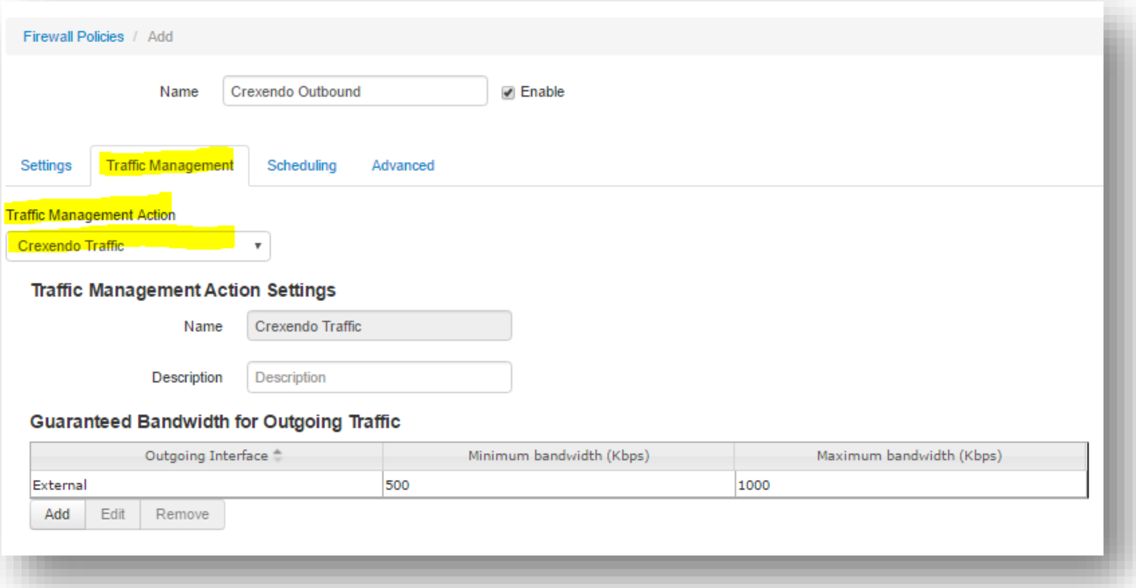
□ Specify custom idle timeout 180 seconds

Continued Outbound Policy

- Click “Traffic Management” tab

    ○

    - Choose the “Crexendo Traffic” from the drop down



Firewall Policies / Add

Name: Crexendo Outbound ☑ Enable

Settings | Traffic Management | Scheduling | Advanced

Traffic Management Action

Crexendo Traffic ▾

Traffic Management Action Settings

Name: Crexendo Traffic

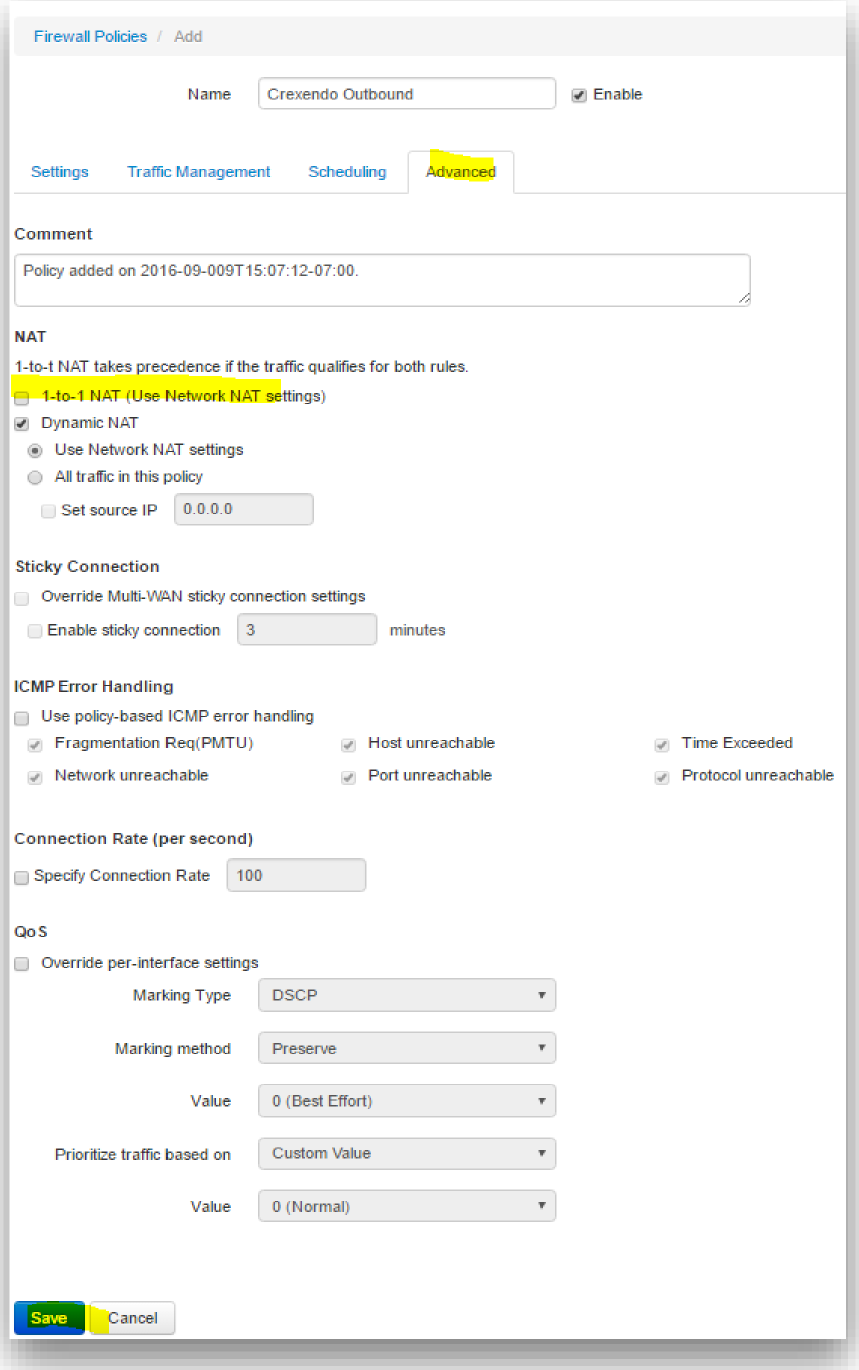
Description: Description

Guaranteed Bandwidth for Outgoing Traffic

Outgoing Interface	Minimum bandwidth (Kbps)	Maximum bandwidth (Kbps)
External	500	1000

Continued Outbound Policy

- Click on the “Advanced” tab
    - Uncheck 1-to-1 NAT
- Click “Save”



Firewall Policies / Add

Name Crexendo Outbound ☑ Enable

Comment

Policy added on 2016-09-009T15:07:12-07:00.

NAT

1-to-t NAT takes precedence if the traffic qualifies for both rules.

☐ 1-to-1 NAT (Use Network NAT settings)

☑ Dynamic NAT

● 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 ☑ Time Exceeded

☑ Network unreachable ☑ Port unreachable ☑ Protocol unreachable

Connection Rate (per second)

☐ Specify Connection Rate 100

QoS

☐ Override per-interface settings

Marking Type DSCP

Marking method Preserve

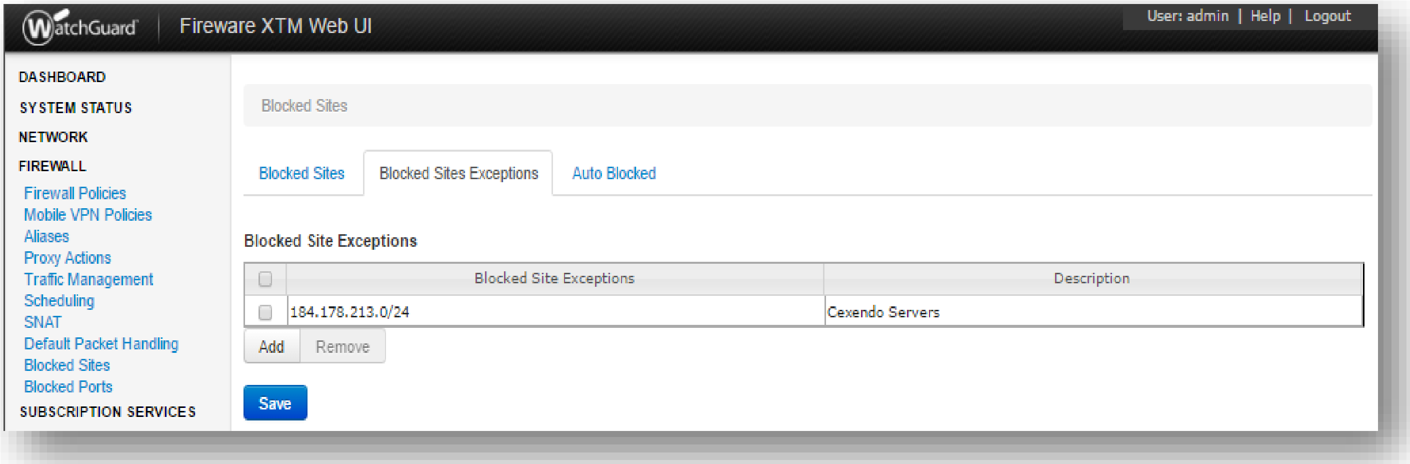
Value 0 (Best Effort)

Prioritize traffic based on Custom Value

Value 0 (Normal)

Whitelist Crexendo Servers

Firewall → Blocked Sites → Blocked Sites Exceptions tab



Blocked Site Exceptions

□	Blocked Site Exceptions	Description
□	184.178.213.0/24	Cexendo Servers

- 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 17th, 2017
2.2	Added Addition RTP UDP ports	May 6th, 2020