

## Time Sensitive Information!

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

Check Point Router Configuration  
For Norcom Solutions Group Cloud Telephony  
Deployment  
Document Version 1.0

May 23rd, 2019

## Table of Contents

---

1. Introduction
2. Checklist
3. Disable SIP ALG Inspection
4. Threat Prevention Exception
5. SSL Inspection Exception
6. QoS and Bandwidth Reservation

## ***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 Check Point 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 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 Check Point 730 running Software Version R77.20.86 (990172855).

We recommend loading the latest software version (firmware).

## Firewall Checklist

---

Please provide screen shots to Norcom Solutions Group for verification of settings. This will allow the implementation process to be smooth and ensure quality audio and proper signaling.

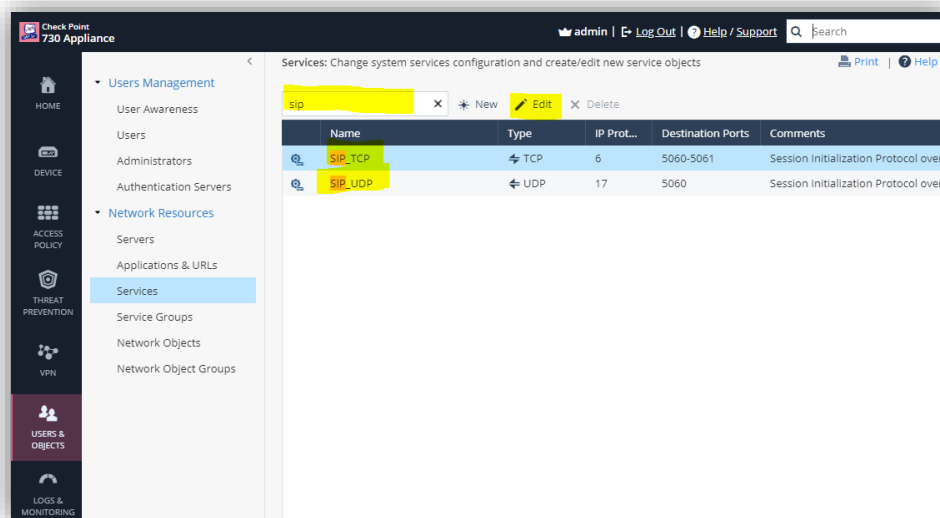
Screen Shot #:	Configuration:	Completed:
1	Users Objects → Network Resources → Services → SIP_UDP → Disable SIP Inspection	
2	Users Objects → Network Resources → Services → SIP_TCP → Disable SIP Inspection	
3	Threat Prevention → Threat Prevention → Exceptions	
4	Access Policy → SSL Inspection → Exceptions	
5	Device → Network → Internet → QoS Tab	
6	Access Policy → QoS → Blade Control → QoS	
7	Access Policy → QoS → Policy	

## Disable SIP Inspection (ALG)

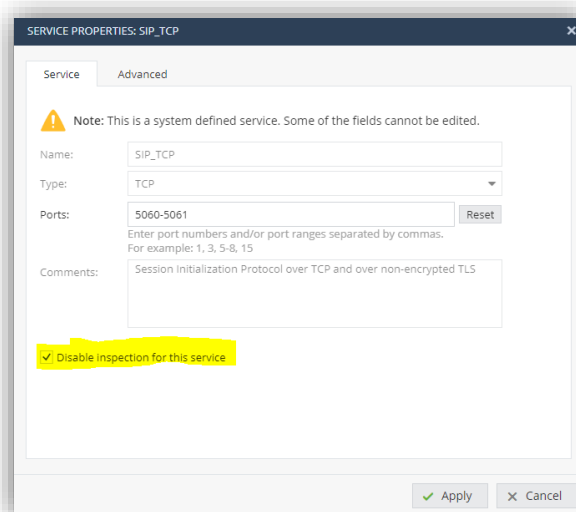
### Users & Objects → Network Resources → Services: SIP\_TCP SIP\_UDP

To disable the SIP inspection, use the search filter to search for the SIP (TCP, UDP) objects and disable the SIP inspection option.

- Please search for “sip” in the search bar
- Select the **SIP\_TCP** object and select “edit”



- Check the “Disable inspection for this service” and click “Apply”



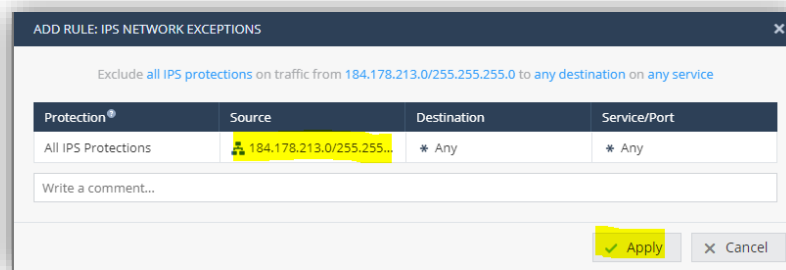
- Once this is complete, select the **SIP\_UDP** object and disable the inspection as well.

## Threat Prevention Exception

### Threat Prevention → Threat Prevention → Exceptions:

To exclude the Crexendo traffic from the Threat Prevention modules please follow the items below:

- Click add/new button
- Add rule that allows all traffic from (Source) the Crexendo subnet
  - (184.178.213.0 255.255.255.0)



ADD RULE: IPS NETWORK EXCEPTIONS

Exclude all IPS protections on traffic from 184.178.213.0/255.255.255.0 to any destination on any service

Protection	Source	Destination	Service/Port
All IPS Protections	184.178.213.0/255.255.255.0	* Any	* Any

Write a comment...

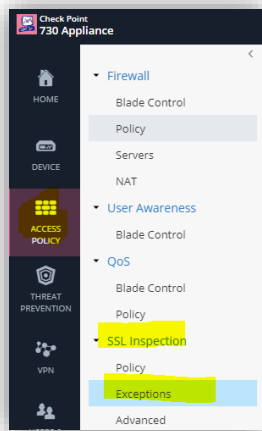
✓ Apply X Cancel

- Click “Apply”

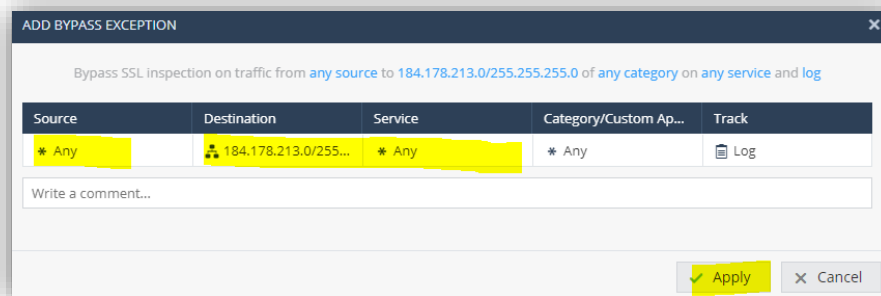
## SSL Inspection Exception

### Access Policy → SSL Inspection → Exceptions:

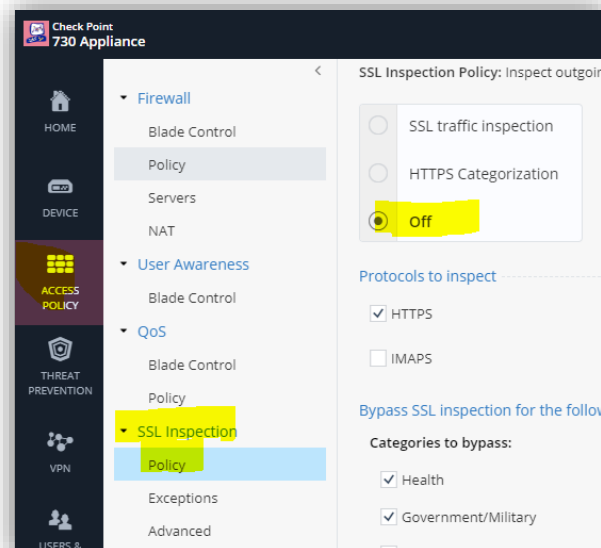
To add the SSL Inspection exception please follow the items below:



- Click add/new button
- Add rule that allows all traffic to (Destination) the Crexendo subnet
  - (184.178.213.0 255.255.255.0)
  - Set "Source" to "Any"
  - Set "Service" to "Any"
- Click "Apply"



**Note:** You may disable this feature also if it causes issues with any other of your network applications.

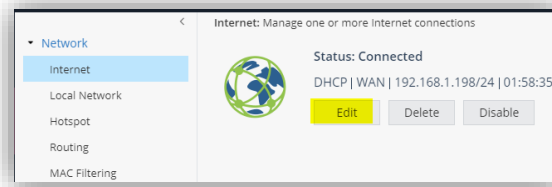


## QoS (Quality of Service) and Bandwidth Reservation

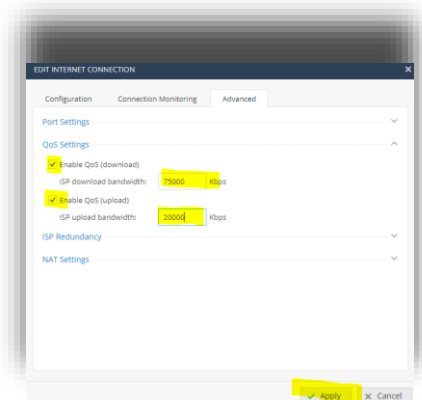
### Device → Network → Internet

To setup QoS on the Check Point firewall you must first set the download/upload speeds on the WAN interface:

- Click the Edit button on the WAN/Internet interface



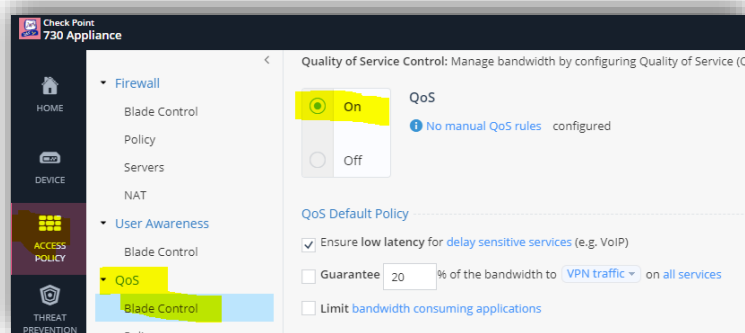
- Click on the “Advanced” tab
- Expand the “QoS Settings” option
- Check/Enable the “download” and “upload” QoS fields and enter the ISP’s contracted bandwidth



- Click “Apply”

### Access Policy → QoS → Blade Control

- Please enable the QoS Module by clicking the radio button under Quality of Service Control:



- Click “Apply”



## Access Policy → QoS → Policy

In the Policy section we will create a rule that gives the Norcom Solutions Group traffic priority and reserves bandwidth for the voice traffic.

- Click on the “New” button
- Edit the following fields:
  - Source: Any
  - Destination: 184.178.213.0/255.255.255.0
  - Service: Any
  - Guarantee/Limit: Guarantee a percentage depending on number of VoIP devices and bandwidth.
  - Comment: Crexendo Traffic

NEW QOS RULE

For traffic from any source to 184.178.213.0/255.255.255.0 on any service, guarantee 20% of bandwidth

Source	Destination	Service	Guarantee/Limit	Weight	Track
* Any	184.178.213.0/...	* Any	20% / -	10	None

Crexendo Traffic

☐ Match only for encrypted traffic

☐ Apply only during this time: 05:00 AM - 05:00 PM

☐ DiffServ mark (1-63): 0

Apply Cancel

- Click “Apply”

## Document Revision History

---

Version	Reason for Change	Date
1.0 Draft	Initial Draft Document	May 23rd, 2019