NORCOM Solutions Group powered by crexendo

Time Sensitive Information!

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

Sophos Router Configuration For Norcom Solutions Group Cloud Telephony Deployment

Document Version 1.2

March 17th, 2017

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 Sophos 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 (SG105, etc…) and UTM 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 Sophos SG105 running UTM 9.315-2.

We recommend loading the latest Sophos UTM OS (firmware).

Note: Default access address to Sophos https://192.168.2.1:4444

Firewall Checklist

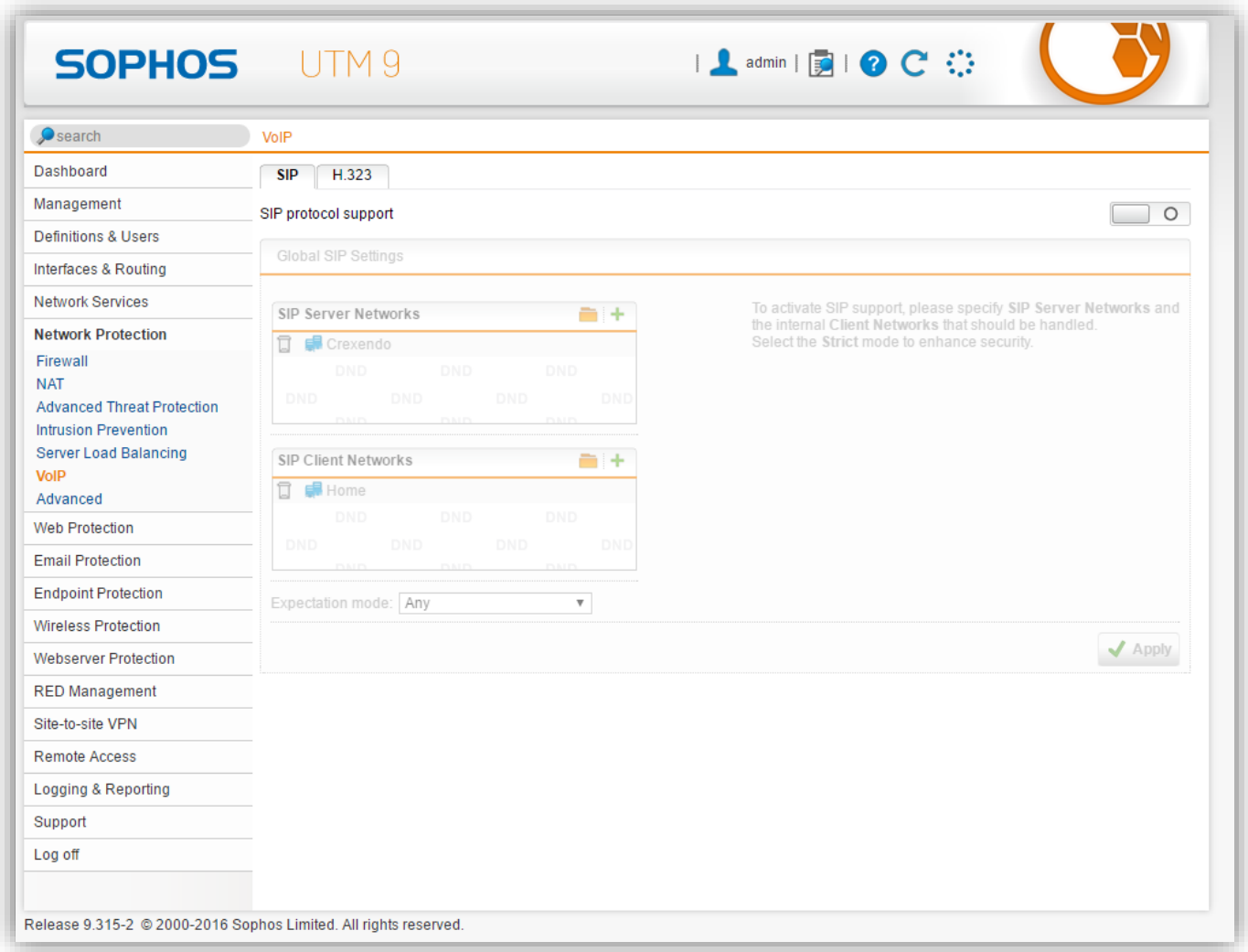
After applying the GUI configurations in this document, please take the appropriate screen shots to provide the firewall "verification" to Norcom Solutions Group.

Screen Shot #:	Configuration:	Completed:
1	Network Protection → VoIP → SIP tab	
2	Network Protection → Firewall → Policies → showing rules for at minimum "Crex Traffic, NTP"	
3	Interfaces & Routing → Quality of Service → Traffic Selector → show "Crex Traffic" details	
4	Interfaces & Routing → Quality of Service → Bandwidth Pool → showing guaranteed bandwidth for the Crexendo traffic	
5	Networking Protection → Intrusion Preventions → Exceptions Tab showing Crexendo subnet excluded "Coming from..." and "Going to…"	

Disable SIP ALG

SIP ALG is used to try and avoid configuring Static NAT on a router. Its implementation, however, varies from one router to another, often making it difficult to inter-operate a router with SIP ALG enabled with a PBX. In general, you would want to disable SIP ALG and configure one to one port mapping on the router.

Network Protection → VoIP

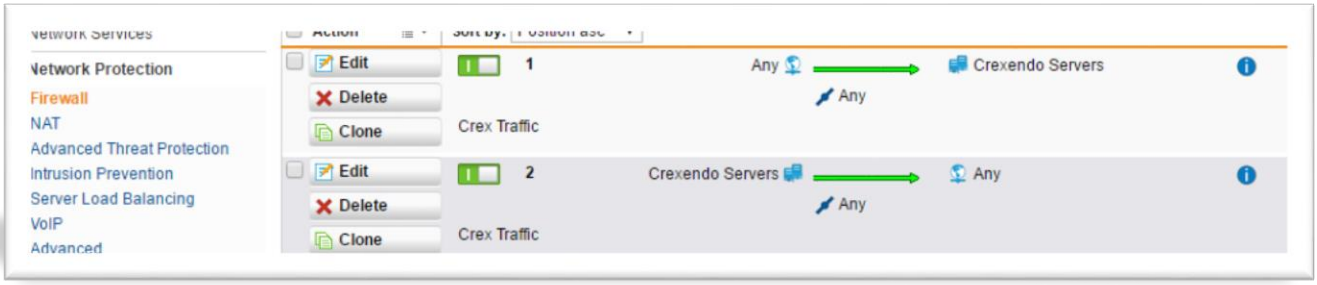


- Select the "SIP" Tab
- Set the "SIP Protocol Support to OFF or "O"

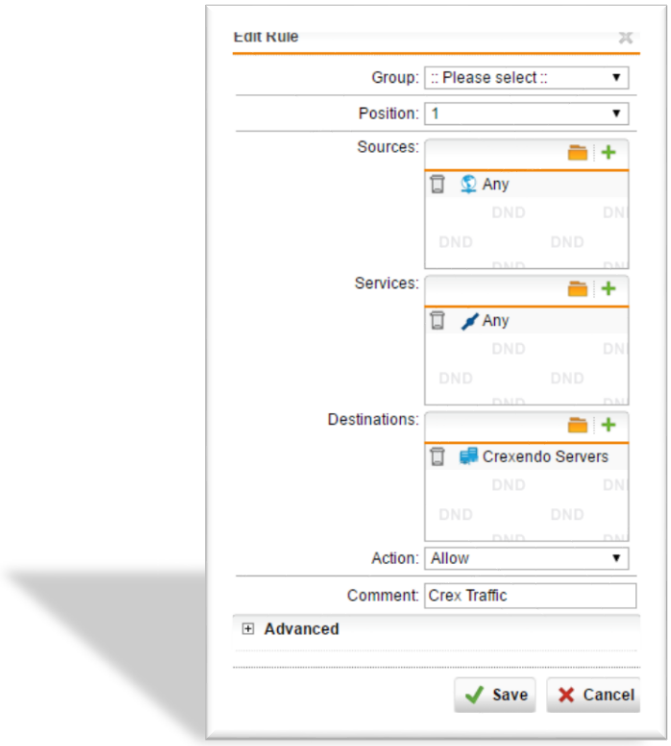
Note: SIP ALG Can be disabled using command line: *system system_modules sip unload*

Create Firewall Rules

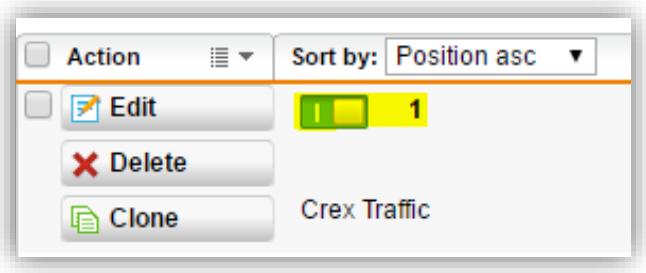
Network Protection → Firewall



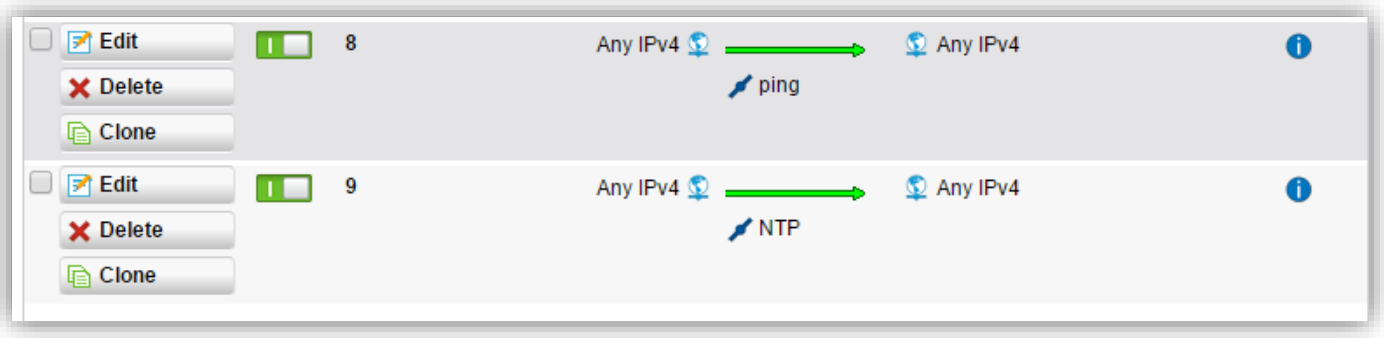
- Click on “New Rule”
- Position: Top
- Sources: Any
- Services: Any (Can specify ports UDP – 5060, 16000-16999, 11780-11800, 80, 443)
- Destination: Crexendo Servers object (184.178.213.0/24)
- Comment: Crex Traffic



- Click Save
- Once rule is save ensure it is enabled by clicking the enable/disable slider:



- Create additional “Allow” rules for any other network services such as “NTP, Ping, etc…”

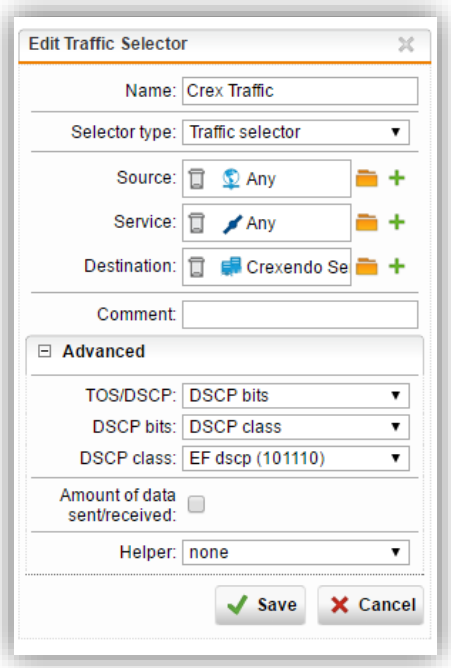


Create Traffic Selector

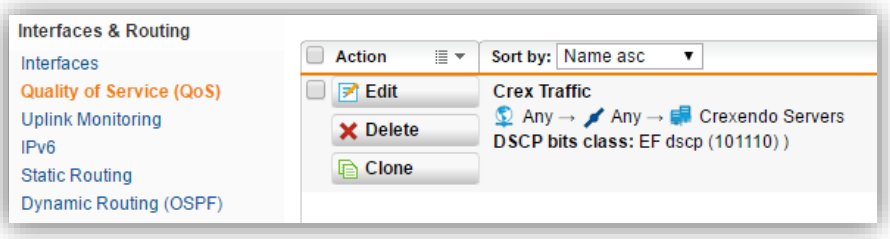
Interfaces & Routing → Quality of Service → Traffic Selector

The Traffic Selectors tab is where you specify the type of packet that you would like to control. Generally speaking, traffic classification is based on IP address and service type, or by choosing the application type you wish to control.

- Click "New Traffic Selector"



- Name: Crex Traffic
- Selector type: Traffic Selector (default)
- Source: Any
- Service: Any
- Destination: Crexendo Servers object (184.178.213.0/24)
- Advanced
  - TOS/DSCP: DSCP bits
  - DSCP bits: DSCP class
  - DSCP class: EF dscp
- Click Save

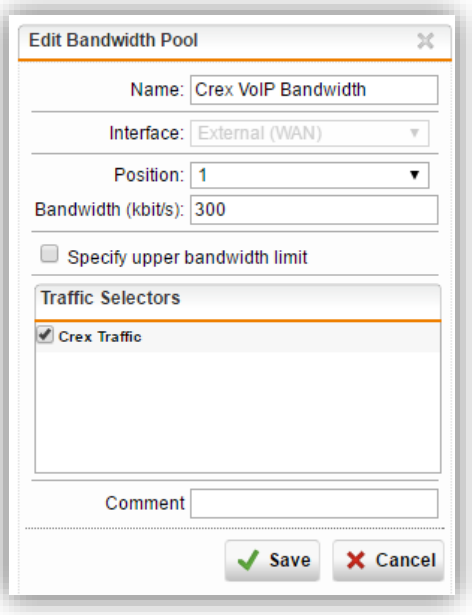


Create Bandwidth Pool

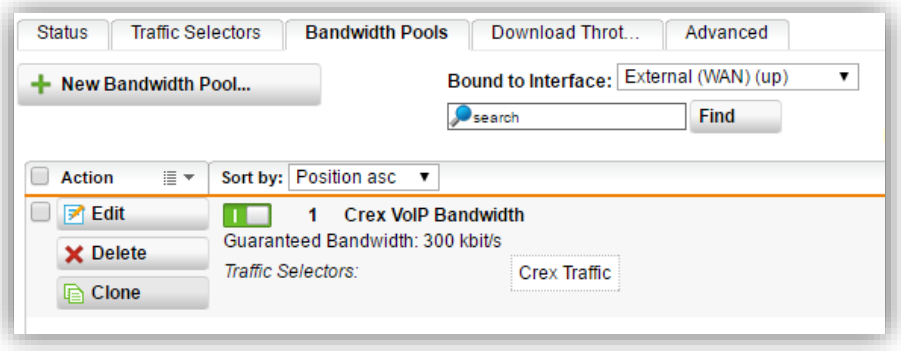
Interfaces & Routing → Quality of Service → Bandwidth Pool

With a bandwidth pool, you reserve a guaranteed bandwidth for a specific outgoing traffic type, optionally limited by a maximum bandwidth limit.

- Click “New Bandwidth Pool”



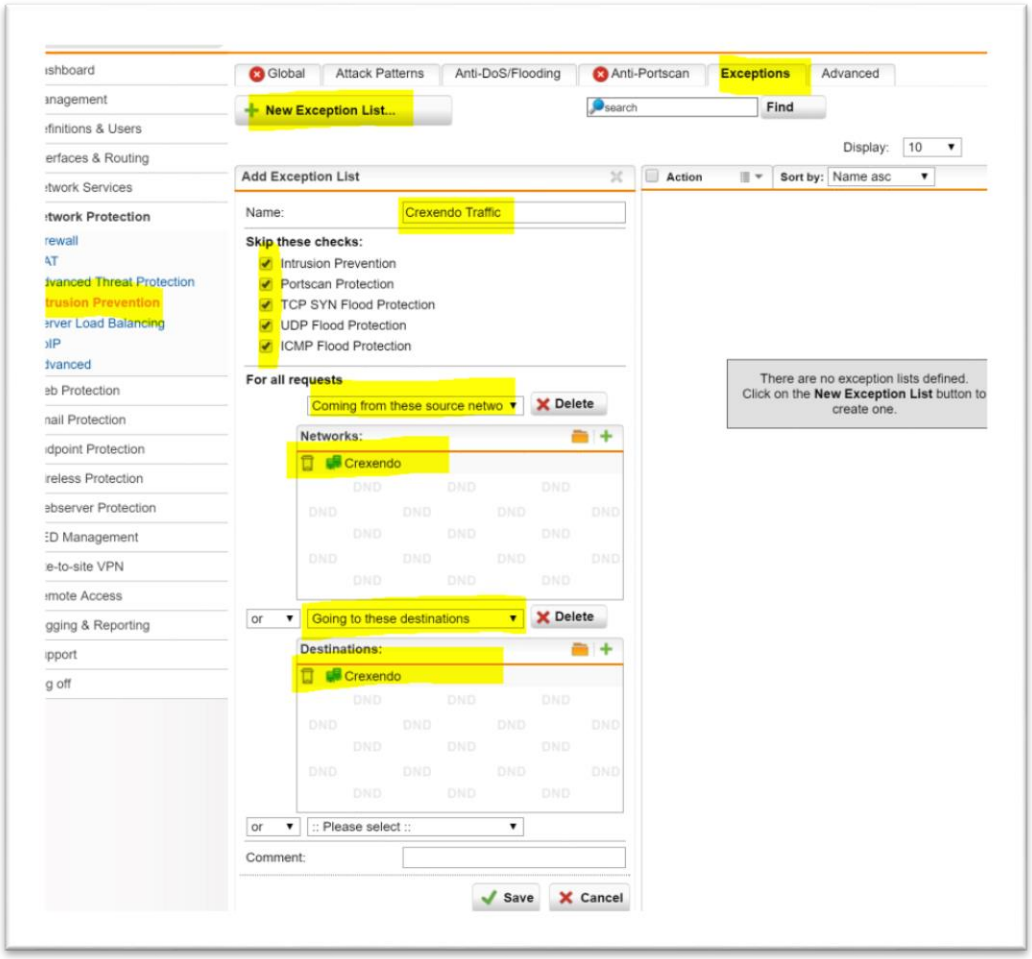
- Name: Crex VoIP Bandwidth
- Interface: External (WAN)
- Position: 1
- Bandwidth: 300Kbps (see note below)
  - Note: please use the following formula for the minimum bandwidth
    - 30% of total # of phones x 100Kbps = minimum bandwidth reservation
  - I.E. 100phones – 30phones x 100Kbps= 3000Kbps
- Traffic Selector: Check “Crex Traffic”
- Click Save



Create Exception for Crexendo Traffic (IPS)

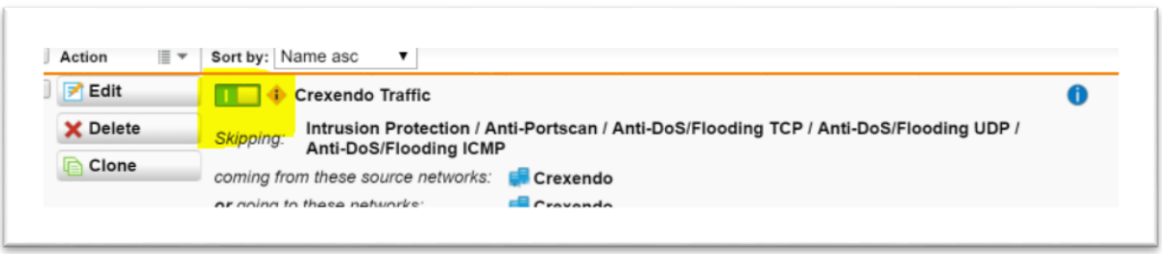
Networking Protection → Intrusion Prevention → Exceptions Tab

- Click the "New Exception List"



- Enter the following information:
  - Name: Crexendo Traffic
  - Skip these Checks: Intrusion Prevention, Portscan, TCP SYN, UDP Flood, ICMP Flood
  - For all requests: Coming from and going to Crexendo network group (184.178.213.0/24)

- Click "Save"
- Click the "power" icon to turn the rule on



Document Revision History

Version	Reason for Change	Date
1.0 Draft	Initial Draft Document	June 27, 2016
1.1	Add IPS Exception list for Crexendo traffic	September 12, 2016
1.2	Verification checklist added	March 17th, 2017