Gear up your PBX
Cut Costs, Boost Profits

Version 20160226

Configure the Firewall

3CX

Goal of this Module

- Correctly Setup the Firewall for 3CX
- Concepts of:
    - NAT & Port Preservation
    - SIP ALG
    - Setup for Provider
    - Setup for 3CX Client, SBC & Bridges
    - Setup Remote IP Phone (Stun)
    - Validation

Firewall Configuration - Why?

- Voice Calls need to pass through the firewall to reach your PBX
- Voice calls use several ports (SIP for signaling and RTP for audio)
- Firewall will block traffic by default
- Need to configure firewall / router to forward calls to PBX

Prerequisites for this Module

- Fundamental Knowledge of routing required
- Configurable Firewalls:
  - pfSense
  - Watchguard
  - Sonicwall (req. hotfix)
- Good knowledge of the Firewall Device
- **Note**: 3CX will not configure your Firewall!

http://www.3cx.com/docs/manual/firewall-router-configuration/
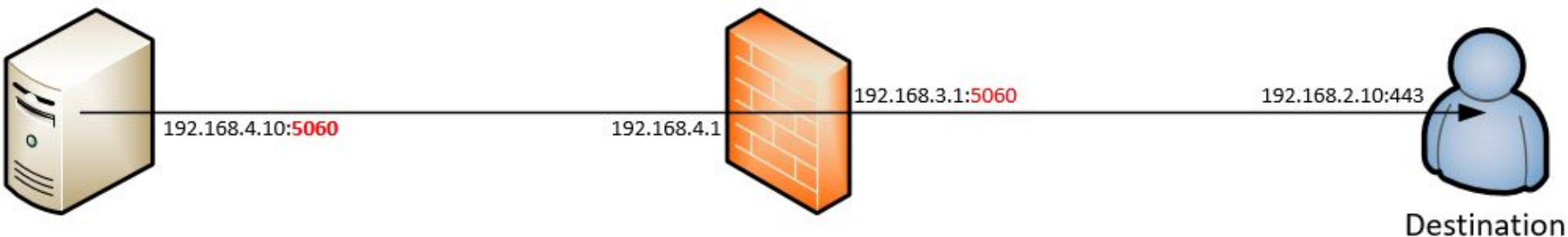
Concept: NAT & Ports

- Translates Public (IPv4) to Private IP Addresses (NAT/PAT)
- Allows Access or Restricts it (ACLs)
- Required to allow connections to 3CX from:
  - Provider(s)
  - 3CX Clients
  - Supported IP Phones
  - 3CX SBC

Concept: Full Cone NAT

- 3CX PBX requires Full Cone NAT
- Allows Incoming Traffic from uncontacted sources
  - Required for
    - VoIP Provider (Multiple IPs)
    - Mobile Devices (Routed IPs)
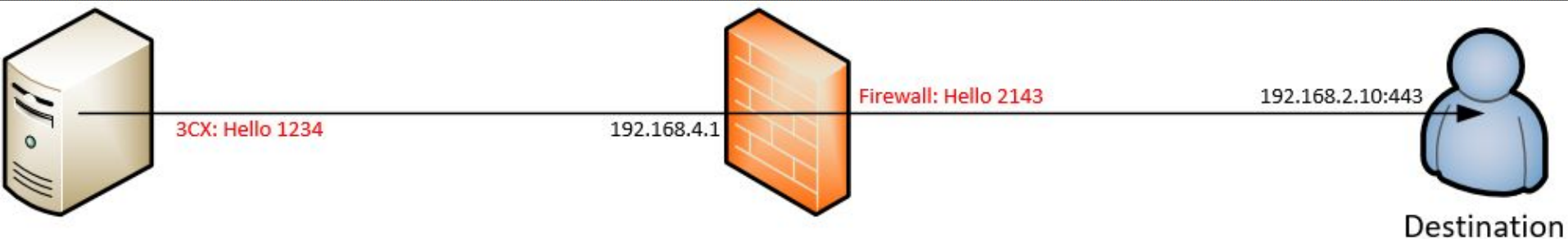   - Home Offices (Dynamic IPs)

Concept: Port Preservation

- Internal source Port = External source Port
- Protocol (SIP/SDP) defines the Port → Not the Transport Header (unique to VoIP)
  - Ensures Connectivity
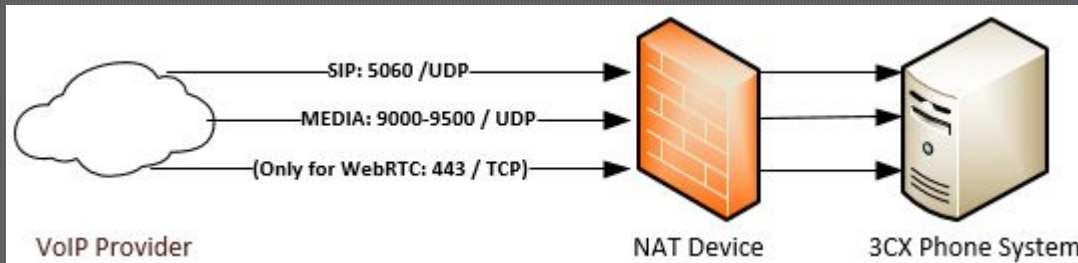 - Eliminates Destination Implementations

Concept: Disable SIP ALG

- ALG = Application Layer Gateway (Firewall)
  - Inspects Content of Packages
  - Tampers Uncontrolled with Content (and you can't see it)
  - Made for Clients NOT Servers
  - Google: e.g.: "Cisco ASA disable SIP ALG"

3CX: Hello 1234   192.168.4.1   Firewall: Hello 2143   192.168.2.10:443
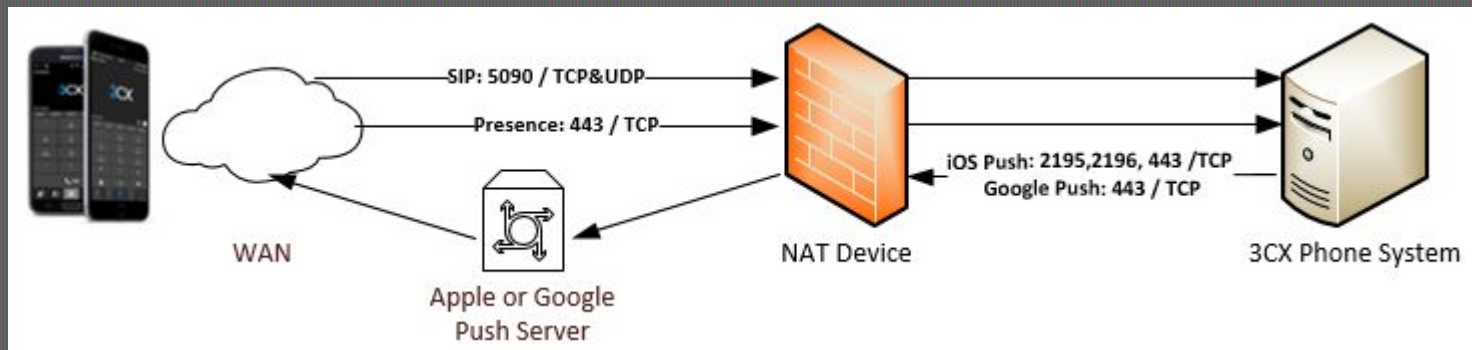
Destination

Prereq: Setup for Provider

- Inbound NAT Ports Required:
  - SIP Port
    - 5060 UDP
    - 5060 TCP
  - Audio Ports (incl. Video & Fax)
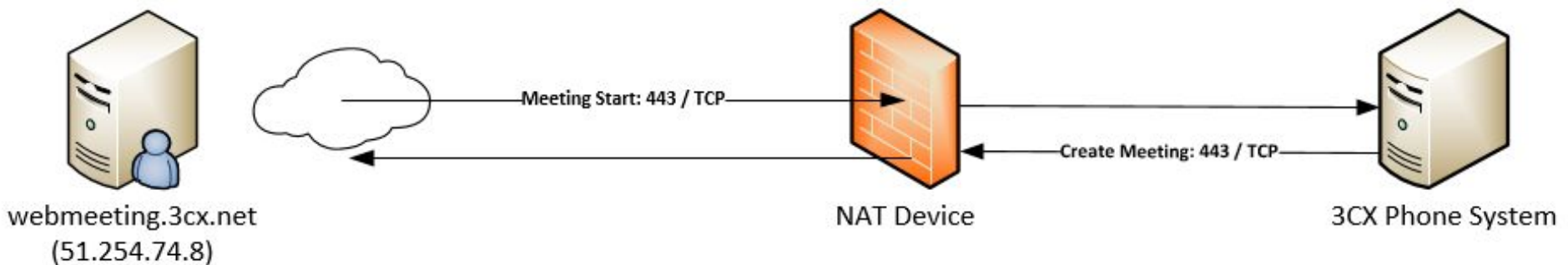   - Range: 9000-9500 UDP

Prereq: Setup for 3CX Client & SBC

- Inbound NAT Ports Required:
    - Tunnel Port (combines SIP & Audio):
        - 5090 TCP + UDP
    - HTTPs Port (Presence):
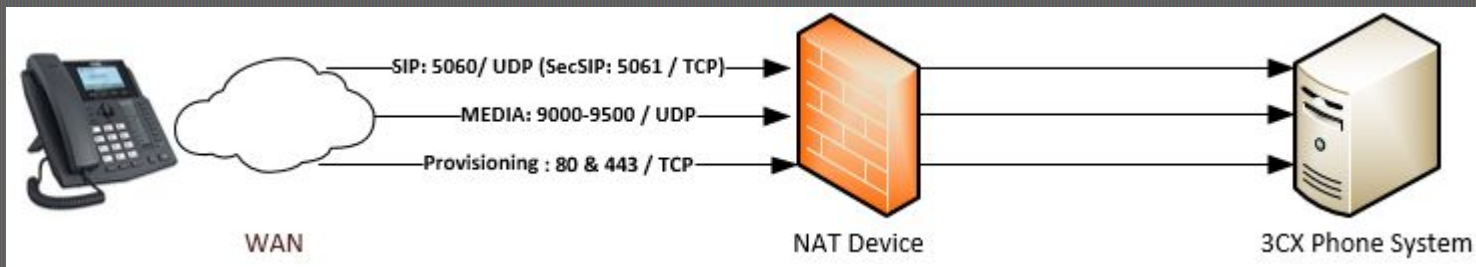   - 5001 TCP (or 443 depending on installation)

Prereq: Setup for 3CX Client (3CX WebMeeting)

- Allow Outbound ACL:
  - Host: webmeeting.3cx.net:443
- Inbound NAT Ports Required:
  - HTTPs Port (Logo and Notifications) :
    - 443 (5001) TCP
- Enables:
  - Starting of Web Meetings
  - Notifications of Waiting User in Meeting Room

webmeeting.3cx.net
(51.254.74.8)

Meeting Start: 443 / TCP

Create Meeting: 443 / TCP

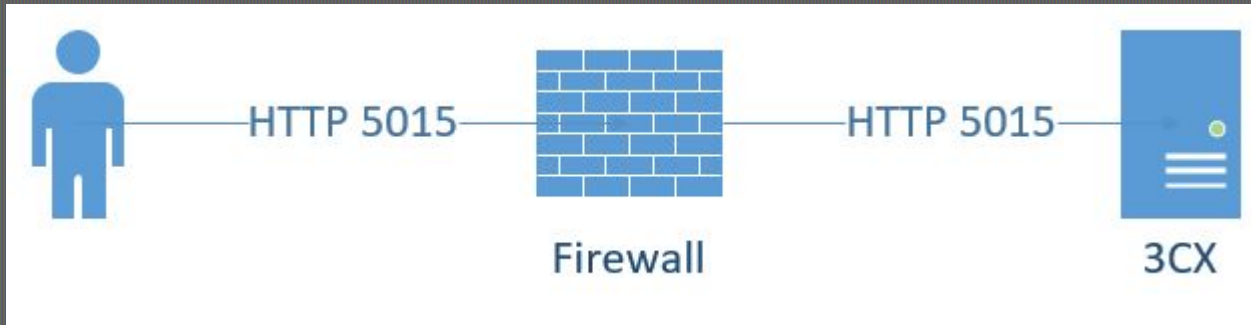NAT Device

3CX Phone System

Prereq: Remote IP Phone (Stun)

- Uses a Mix from (so maybe already opened)
  - VoIP Providers
  - 3CX client
- Inbound NAT Ports Required:
  - SIP: 5060 UDP + TCP
  - Audio: 9000-9500 UDP
  - Provisioning: 5001 TCP (or 443 depending on installation)

Prereq: Remote Configuration Wizard

- Inbound NAT Ports Required:
    - HTTP: 5015 TCP
      (Only for the duration of the host setup)

Concept: Validation

- Management Console > Dashboard > Firewall Checker
  - GREEN is pass
  - RED is FAIL
  - One RED = Fail = Reconfigure Firewall
    Note: Firewall Checker only tests UDP Ports!
  - No HTTPs Port
  - No Tunnel TCP Port

PBX Status	
Trunks Up	1/3
Extensions Up	1/30
Number of calls in use	0/8
Blacklisted IPs	0
Event log	Purge
Call history	Purge 152 calls
Chat logs	Disabled
Automatic Backups	OFF
Firewall Check	Firewall test failed
✓ Services	✓ System Extensions

Using: Validation - All Failed

Firewall Check

3CX Services will be stopped until the test is complete. Services will be started automatically after.

▶ Run   ■ Stop

resolving 'stun.3cx.com'... **done**
resolving 'stun2.3cx.com'... **done**
resolving 'stun3.3cx.com'... **done**
testing 3CX SIP Server... **failed** (How to resolve?)
   stopping service... **done**
   testing port 5060... **full cone test failed**
   starting service... **done**
testing 3CX Tunneling Proxy... **failed** (How to resolve?)
   stopping service... **done**
   testing port 5090... **full cone test failed**
   starting service... **done**
testing 3CX Media Server... **canceled**
   stopping service... **done**
   testing ports [9000..9255]...
      testing port 9000... **full cone test failed**
      testing port 9001... **full cone test failed**
      testing port 9002... **full cone test failed**
      testing port 9003... **full cone test failed**
      testing port 9004... **full cone test failed**

Validation: Part 1

- Firewall configuration does not work or has not been made
- Contact firewall manufacturer support if needed
- Do not call 3CX Support for assistance configuring your firewall
- Do not attempt to create SIP Trunks, Bridges or Remote Extensions
- Remote Extensions or SIP Trunks won't register

Using: Validation - nearly there = still a fail

Firewall Check

3CX Services will be stopped until the test is complete. Services will be started automatically after.

▶ Run   ▮ Stop

resolving 'stun.3cx.com'... **done**
resolving 'stun2.3cx.com'... **done**
resolving 'stun3.3cx.com'... **done**
testing 3CX SIP Server... **done**
　　stopping service... **done**
　　testing port 5060... **done**
　　starting service... **done**
testing 3CX Tunneling Proxy... **done**
　　stopping service... **done**
　　testing port 5090... **done**
　　starting service... **done**
testing 3CX Media Server... **failed** (How to resolve?)
　　stopping service... **done**
　　testing ports [9000..9255]... **failed**
　　　　testing port 9000... **full cone test failed**
　　　　testing port 9001... **full cone test failed**
　　　　testing port 9002... **full cone test failed**
　　　　testing port 9003... **full cone test failed**
　　　　testing port 9004... **full cone test failed**

Validation: Part 2

- Review and fix your firewall configuration
- Contact firewall manufacturer support if needed
- Do not call 3CX support for assistance configuring your firewall
- Do not attempt to create SIP Trunks, Bridges or Remote Extensions
- In this example Remote Extensions will register but not have audio

Using: Validation - Well Done - Success

Firewall Check

3CX Services will be stopped until the test is complete. Services will be started automatically after.

▶ Run   ■ Stop

resolving 'stun.3cx.com'... **done**
resolving 'stun2.3cx.com'... **done**
resolving 'stun3.3cx.com'... **done**
testing 3CX SIP Server... **done**
　　stopping service... **done**
　　testing port 5060... **done**
　　starting service... **done**
testing 3CX Tunneling Proxy... **done**
　　stopping service... **done**
　　testing port 5090... **done**
　　starting service... **done**
testing 3CX Media Server... **done**
　　stopping service... **done**
　　testing ports [9000..9255]... **done**
　　　　testing port 9000... **done**
　　　　testing port 9001... **done**
　　　　testing port 9002... **done**
　　　　testing port 9003... **done**
　　　　testing port 9004... **done**

Recap

- Full Cone NAT has been correctly configured and tested
- Port Preservation has been correctly configured and tested
- SIP ALG can not be tested by the firewall checker
- TCP Ports can not be tested from within the PBX

Gear up your PBX
Cut Costs, Boost Profits

3CX