Patton Electronics Co. | www.patton.com
7622 Rickenbacker Drive, Gaithersburg, MD 20879, USA
tel: +1 301-975-1000 | fax: +1 301-869-9293

Application Note

Patton® SmartNode in combination with a CheckPoint® Firewall for Multimedia security

Document version	2.0
Date of creation	25.01.2012
Contact	**Patton Support** http://patton.com/support support@patton.com

Table of contents

Document revisions

Date	Name	Content
25.01.2012	MM	Document creation
19.06.2012	MZ	Revision to document V2.0

1 Introduction

Security is in the today communication systems a key element required to have a stable and reliable IT service. This includes not only data security however also written and mutual communication.
Open VoIP networks are attackable using different methods such as brute-force search. VoIP attacks leads often in fast growing costs; therefore, VoIP networks must be protected such as data networks. Using the Patton SmartNode eSBC as Session-Border-Controller, SBC, together with a firewall covers the customer's requirements concerning multimedia network security. One of the firewall products is provided by Checkpoint.
The document provides you information, how a SmartNode can be used as SBC in a small/medium size installation in combination with a Checkpoint Firewall.

2 Network

The data network infrastructure is often split into three main networks, WAN, LAN and DMZ. The three networks are in our example physically connected through a CheckPoint firewall. Introducing VoIP several components and entities can be added to all three network segments:

DMZ Network

- SmartNode Session-Boarder-Controller
- UCS / IP-PBX

LAN Network

- Local VoIP users

WAN Network

- SIP Trunk / SIP Provider
- Remote / Home Office
- Nomadic users

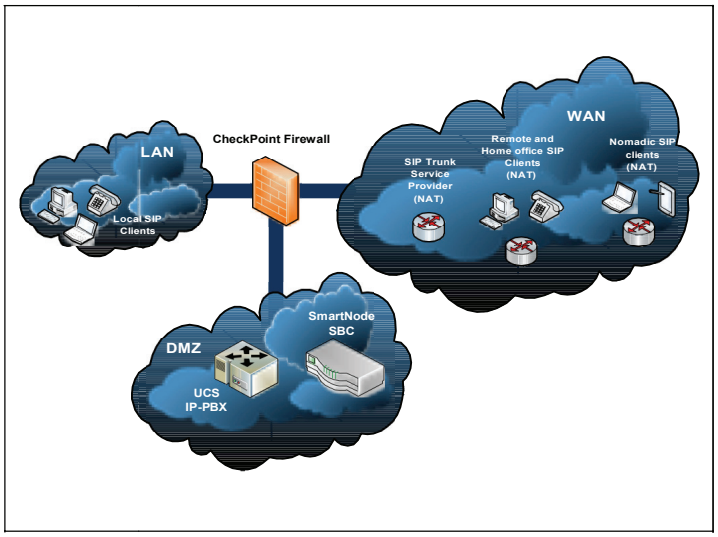


Figure 1: Network diagram

Optional, instead of using the SmartNode as SBC in combination with an UCS/IP-PBX system it may be used as VoIP to TDM/Analogue gateway towards a legacy telephony system.

3 Solution

In a probable solution the CheckPoint firewall is used as TCP/IP filter to limit in a first step the range of entities accessing the VoIP network based on TCP and IP addresses.

Therefore, the following Layer4 ports need to be opened to setup a SIP call from, to a defined range of IP addresses:

- UDP Port 5060, SIP default signaling port
- TCP Port 5060, required depending on the UCS
- UDP Port for RTP traffic, depending on the used equipment (SmartNode: 4864-5119 except 5060`)

In a second step the SmartNode used as SBC takes over the VoIP security of the SIP networks. Multiple filters, e.g. SIP domain, SIP from/to header, etc. allow limiting the access to the SIP Networks for authorized users and entities only. Optional inbound registration and authentication enhances the security of the VoIP network.

The TransCoding functionality available in a selected range of SmartNode allows converting the RTP voice stream to the most efficient codec for each connection. E.G. G.711 for the SIP/RTP leg LAN – PBX – SN codec G./26 for the SIP/RTP call leg SN – SIP-Provider.

The diagram below show that all external SIP/RTP VoIP traffic path the SBC filter of the SmartNode. VoIP traffic between the save LAN and DMZ networks has direct access to the PBX.

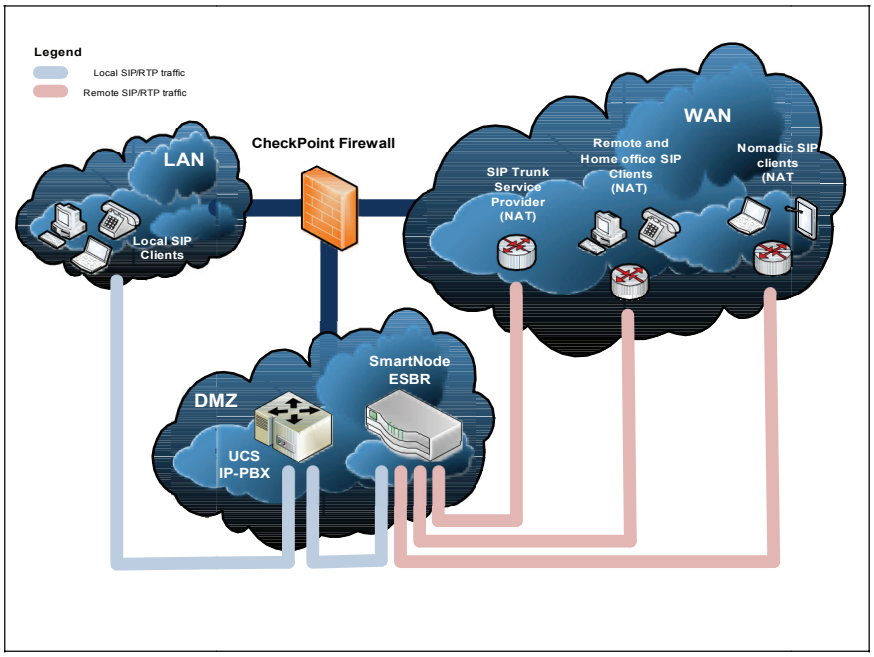


Figure 2: Network Diagram including VoIP call flow

4 Conclusion

With the proposed network configuration the communication system is protected for many different attacks on all OSI layers required for VoIP.

The PBX is not direct reachable from the WAN, the barrier for misuse of the system gets higher. Due to the higher security the reliability of the communication network increases.

5 Configuration

5.1 CheckPoint Firewall

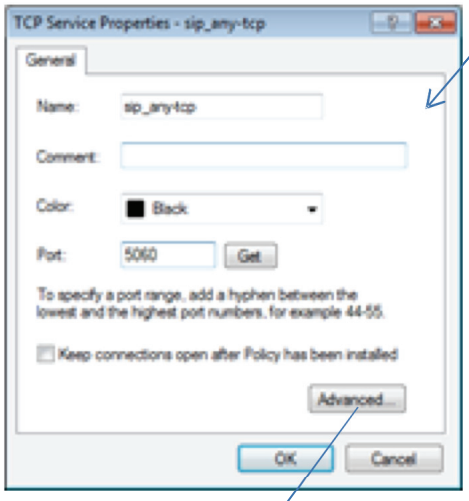
Different settings needs to be covered **t**hat the CheckPoint Firewall is open for SIP sign**a**ling and RTP traffic. These settings must be made for all SIP users or networks, which are allowed to access the pr**o**tected VoIP system. That's includes as well as traffic from t**h**e local VoIP network installed in LAN toward the UCS/IP-PBX server.

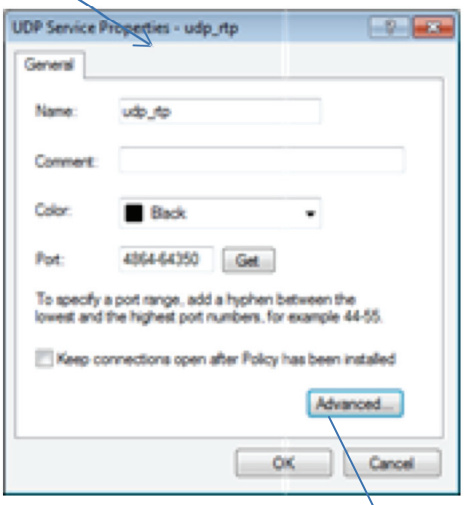
The below configuration guide line hel**p**s you configuring the CheckPoint Firewall for voi**c**e

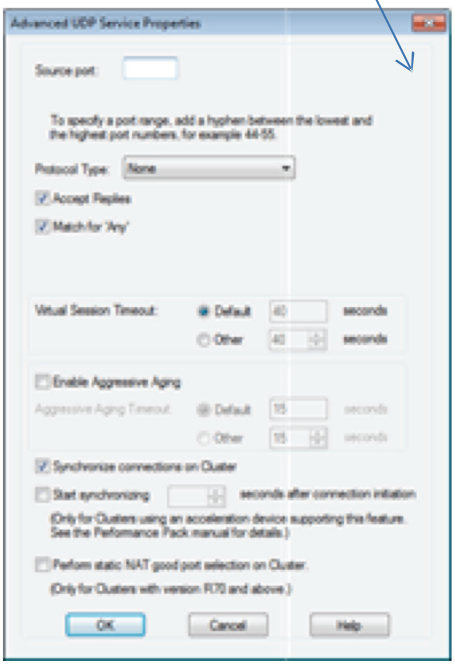
5.1.1 Firewall Panel

For each entity that access the VoIP s**y**stem, a separate rule for incoming and a separa**t**e rule for outgoing traffic is required. To follow to the proposed sol**u**tion the target of the SIP/RTP stream coming fr**o**m the WAN is the IP address of the SmartNode. The target **o**f the SIP/RTP stream coming from the LAN will **b**e the

NAME	SOURCE	DESTINATION	SERVICE	ACTION	TRACK
<name>	<range or ip>	<r**a**nge or ip>	sip_any-tcp udp_rtp	accept	log







5.1.2 NAT panel

To avoid one way voice communication the CheckPoint firewall must keep the original UDP port address for the RTP stream. Therefore Port Address Translation needs to disabled for all authorized RTP traffic in the NAT panel.

ORIGINAL PACKET			TRANSLATED PACKET		
SOURCE	DESTINATION	SERVICE	SOURCE	DESTINATIO	SERVICE
<range or ip>	<range or ip>	udp-rtp	Original	Original	Original

5.2 Patton SmartNode

The SmartNode configuration depends on the connected endpoints. Each UCS/IP-PBX system and each SIP service provider has its own SIP configuration that needs to be adapted into the SmartNode configuration.

Patton provides many configuration examples for different VoIP system in the knowledge base. The Patton knowledge base is accessible on the Patton home page for free and around the clock.

http://www.patton.com/support/kb.asp?cat=100

Figure 3: Patton Knowledge Base