the VoIP challenge

Tadiran Telecom, the leading Israeli telephony provider chose the cutting edge technology of portnox™ by access layers as their OEM security and provisioning software solution.

Tadiran Telecom

What do they know that others might not?

As is well known in the corporate and the business world, the concept and the practice of that service called Telephony has been considered the topmost killer app' any one could find in a working corporate environment. Without the Telephony functioning and secure, the business world might as well shut its doors. Now, giving any ERP, CRM or collaboration architectures the deserved place and importance, the fact remains that 'voice service' plays the central and mandatory role in all business communication, which is an essential element for a successful business performance.

When it comes to VoIP (voice over IP) in the business environment, there are few voices saying it is "running behind". Some are saying that the VoIP solutions are not mature enough; others claim it to be too pricey; there are those who go so far and say that: "… the paradigm shift from the traditional way is far too great for it to succeed". Regardless of what the nay voices claim, fact is that VoIP is here to stay and the question is not if it will replace the conventional Telephony but, how rapid the changeover will be.

The most obvious misgiving folks have with the VoIP-fact is, that it shifts the Telephony from a 'static role of a telephony personal' over to an 'IT personal'. The understanding that VoIP isn't just another IT service is paramount, therefore sending a network manager or administrator for a crash course on IP Telephony will not take the office deployment far. When it comes to VoIP there's something beyond just another new technology generation to be integrated by the IT professional.

Assuming that an organization has managed to run or migrate into a VoIP solution, as the organization has done with all of its IP systems, it needs to manage and secure the VoIP environment. An essential fact to remember is that the VoIP telephone is not just another plain IP device on the network. It's not a web camera or IP based water cooler, it's a Telephone Device and thus it must be considered as important in being secured and properly managed at least as well as any PC workstation. Actually, and as you will soon see, it may be wise to have the IP telephone device even more secured than the common computer workstation.

the voip challenge

A commonality among most VoIP scenarios is that they all rely on one or two telephone device types and at least one central pbx server for a typical office deployment. Unlike a PC workstation, which can be very versatile, in most environments the IP phone device is a static device and its configuration is usually identical to the IP phone device placed on the next table or, in the next door office.

In the corporate environment which deploys a VoIP solution, it might define a designated network number or a network vlan for that VoIP service. **However, can any one person or product constantly ensure that IP phones are physically connected to the right network ports)?** Or verify that a PC device has not been attached to the VoIP network?

Without a positive solution to this problem a probable (and common) mis-plugging scenario is almost guaranteed. And since in such case, neither device is connected to its relevant target network, neither one will receive the required IP service. Chances are that in no time the 'helpdesk team' will receive a call from the distort user, and hopefully point him at the right direction without too many 'man-hours' spent on this easily avoidable problem.

As probable and common as this scenario may sounds, the available Network-Access vendors cannot help. They cannot differentiate between a PC device and a Telephony one (Excluding maybe the uncommon, heterogeneous, single vendor solution). Unlike those technologies portnox™ can identify, authenticate and authorize any IP device at the plug-in port.

portnox™ by access layers, is a unique and cutting edge software solution which identifies the attaching device at the point where the device attaches to the network – at the port level.

The identification of the attaching device is based on several predetermined attributes. Once the device has been identified by portnox™, portnox™ checks the device against its local database and the predetermined security policy and ensures that the attaching device is eligible for access to that specific port. In case the IP device connecting is found to be an illegitimate device, portnox™ will send a command to the local switch, thus allocating the correct network number to the relevant network port.

True, as to migrate into a successful VoIP solution, a corporation may save some wiring and a negligible cost, if they use convergence to deploy the VoIP. However, by doing so the corporation opens the door to major security issues.

The risk of convergence is simple to see and understand as follows:

1. An IP telephone device is assigned a specific network number (e.g. a vlan).
2. A PC device is connected at the back of the telephone and uses another network number (e.g. a default vlan).
3. The PC user manually assign his PC to shift from the data network over to the voice network (e.g. vlan hopping).
4. The corporate VoIP network integrity & security are compromised.

Unlike in the days of plain telephony architecture, nowadays any PC user can manually assign his PC to shift from the data network over to the voice network! And there is NOTHING your switch or voice vendor can do about this manipulation to avert the risk.

No matter how expensive, sophisticated and advanced the network switch is, it cannot tell whether it is a PC or IP telephone which is connecting to the network! Identification and authentication of a device attaching to the network is not part of the switch's 'DNA' design. It is however among the tasks the portnox™ solution was designed to do.

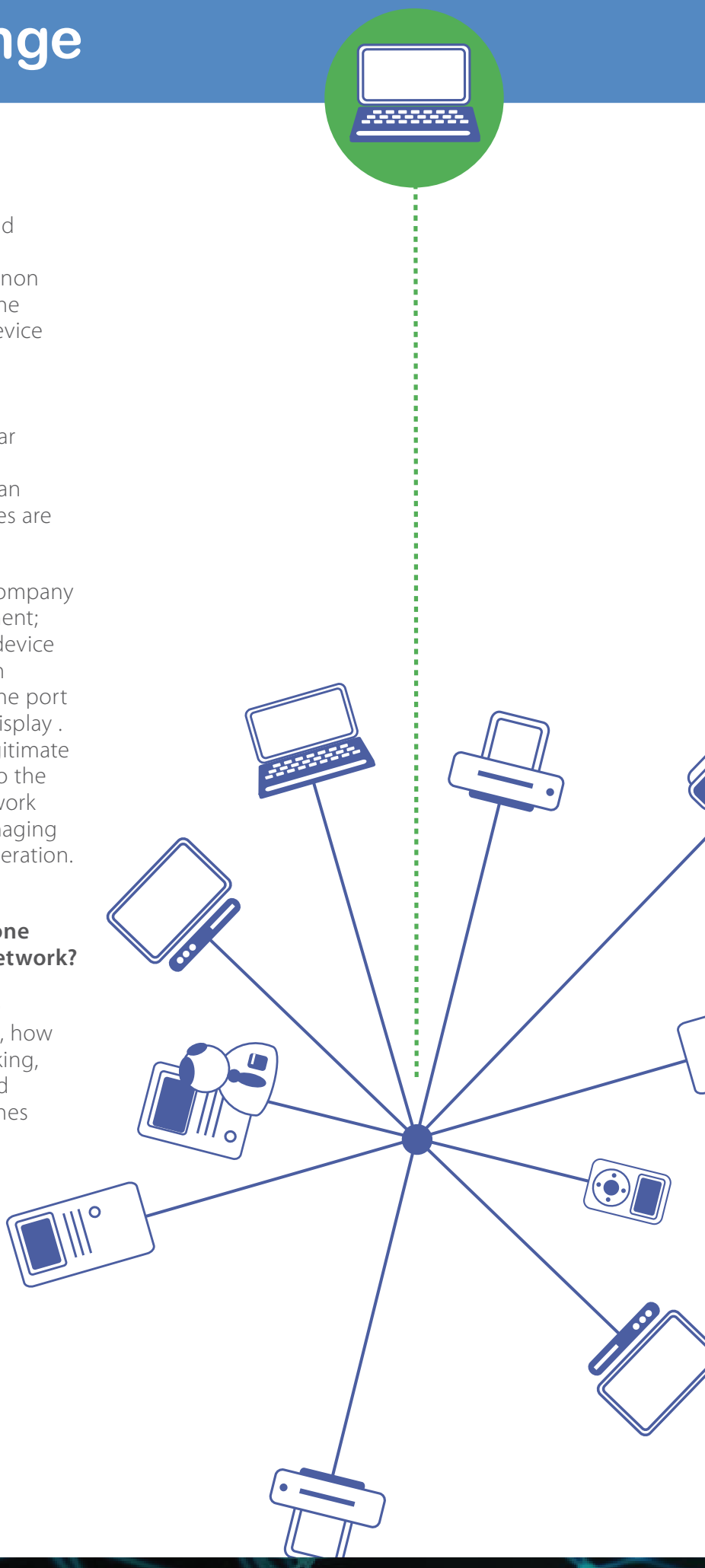
the voip challenge

No matter how expensive, sophisticated and advanced your current network security is, when and in the case when an illegitimate non telephony device succeeds to connect to the corporate VoIP network, that illegitimate device may hijack voice sessions, spoof telephone extensions, perform call enumeration and practically take the pbx down altogether. All that trouble may happen below the radar screen of the current and available security products. None of the available products can guarantee that the only legitimate IP phones are participating in your voice network.

Only with the portnox™ protection can a company safely manage and secure its VoIP deployment; each IP telephone is in clear sight; each IP device can be tracked, traced and monitored; each logged-on device is a legitimate one and the port location where it logged on is constantly display . portnox™ allows no other device than a legitimate and authenticated IP telephone to attach to the voice network. portnox™ provides the network with the absolute integrity needed for managing and securing a corporate voice network operation.

How can a company assure that only a legitimate and authenticated IP telephone device attaches to its corporate voice network?

How can a company tell the number of the working and operational IP phones it owns, how can it assure that the IP phones are all working, identify each one of them, authenticate and provide the physical location of the IP phones using the service altogether?



Version 2 | 二版
www.version-2.com

Hong Kong
Tel : (852) 2893 8860
Email : sales@version-2.com.hk

Taiwan
Tel : (886) 02 7722 6899
Email : sales@version-2.com.tw

Singapore
Tel : (65) 6296 4268
Email : sales@version-2.com.sg

portnox™