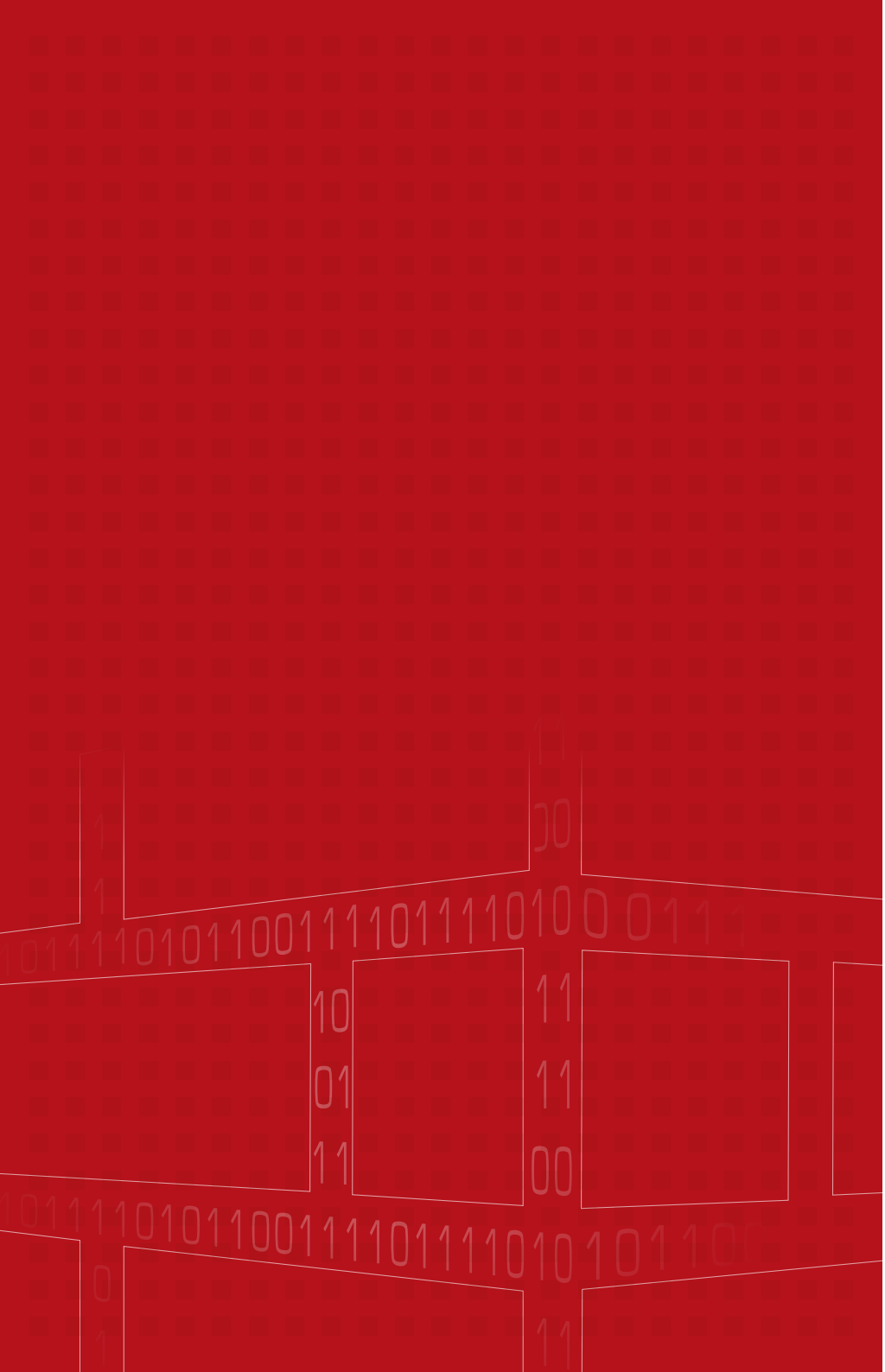


pbxwall

Communicate freely, we've got you protected.

Innovative anti-fraud technology that blocks PBX Hacking and stops Toll Fraud.

THE problem

"Recent reports from the CFCA estimate the Toll Fraud value to be in excess of $4.96bn per annum"

PBX Hacking or otherwise commonly known as Toll Fraud, continues to be the global scourge of the telecommunications sector.

The first symptom of PBX hacking generally occurs when the carrier notifies their client that their network is reporting surges in call volumes to international telephone numbers. At this stage, the carrier advises the enterprise to contact their PBX maintainer and have them lock down or shut off the PBX.

Accountability

The financial consequences of PBX Hacking generally kick off a frantic blame game, ultimately:

- The enterprise will demand that someone should be held accountable.
- The carrier is legally entitled to collect their fees and the enterprise is legally responsible to pay the bill.
- Legal advice sought by the enterprise generally encourages them not to challenge a case that they cannot win.
- The VAR argues that they cannot be held accountable for security breaches because they configured the PBX to their clients specification while also providing self-administration tools & training.
- The police struggle to investigate due to lack of cross border regulation and international language barriers, resulting in zero prosecutions.

The vast majority of reported cases result in:

- Very few prosecutions.
- Accountability is never established.
- Enterprise has to agree a settlement with the carrier.
- The overall experience leaves the enterprise highly frustrated, financially exposed and vulnerable to further attacks.
- Trustworthy relationship established between Carrier, VAR and client are often strained beyond breaking point.

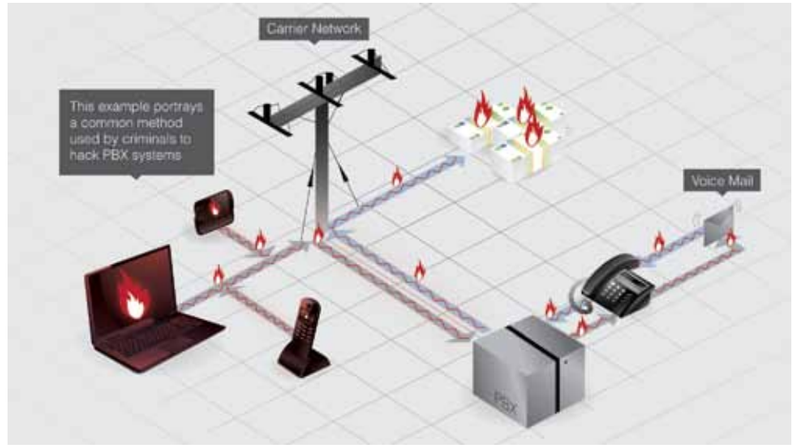
Threat

The open world of unified communications (UC) and mobility applications increases the threat of hackers accessing your PBX system.

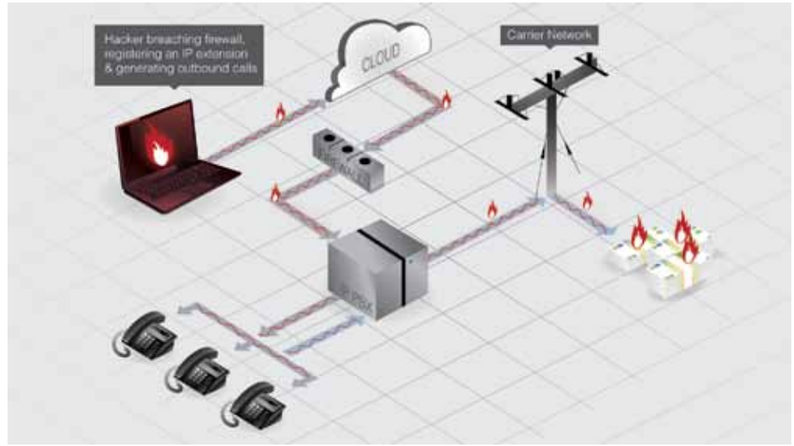
Active PBX system features such as unified mobility, unified messaging, SIP account registration, call divert and conference facilities enhance the overall possibilities for a criminal to hack a PBX system.

Enterprise Under Attack

This example portrays a common method used by criminals to hack PBX systems.



Hackers Accessing an IP Telephony Network



OUR solution

*Protect your business from the threat of Toll Fraud **24x7x365***

Pbxwall is a novel and innovative voice firewall, our intellectual property was designed to automatically identify and stop criminals routing expensive telephone calls across TDM and SIP trunk lines.

Real Time Detection & Blocking

In real time, pbxwall:

- Live monitors the active trunk lines that integrate to a PBX system.
- Continually analyses and compares the audio frames on the active trunk channels.
- Immediately detects fraudulent call activity.
- Automatically blocks the relevant trunk channels.
- Raises an alert for every blocked call and informs our live monitoring centre.
- Continually protects 24x7x365.

Technology Benefits

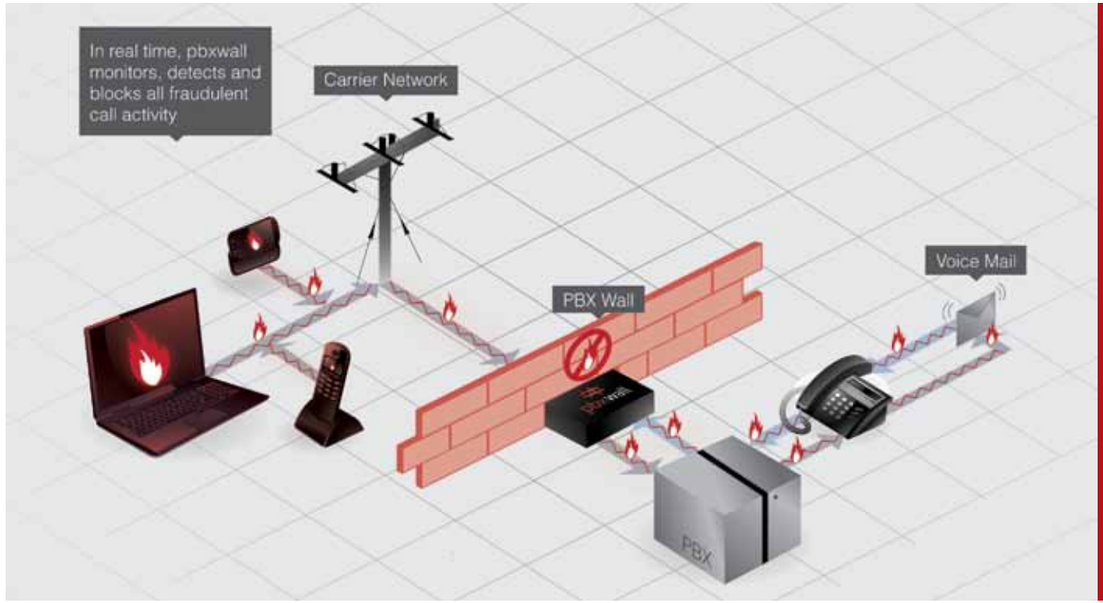
Unlike existing preventative solutions, pbxwall guarantees that all fraudulent call activity is automatically detected and blocked. The major benefits of pbxwall include:

- Carrier and PBX agnostic.
- Simple Deployment.
- Removes the onus from VAR and Enterprise to have PBX user passwords and remote maintenance ports protected.
- Automatically knows when a hacker is on the trunk lines.
- No requirement for PBX integration.
- Does not require a pre-configured "Deny" restriction table.

Summary

Pbxwall is a global solution to a global problem, offering around the clock protection against the threat of Toll Fraud 24x7x365

Pbxwall Protecting the Enterprise



ABOUT pbxwall

Real time anti-fraud solution that automatically stops Toll Fraud

Pbxwall Ltd. is an Irish owned company founded in 2010 by Paul Byrne and is headquartered in Dublin, Ireland.

Paul Byrne
Pbxwall founder & CEO

Our mission is to protect the enterprise from toll fraud and empower the value added resellers (VARs) of PBX systems to retain and gain customers by installing a pbxwall on their customer's voice network.

Backed by our world class R&D division, we have developed the first anti-fraud system of its kind for real time detection and automated blocking of Toll Fraud.

Concept of pbxwall

Pbxwall is both Carrier and PBX agnostic, its design concept was developed from:

- The reality that the basic common functions and features of a PBX system continually expose the enterprise to the threat of Toll Fraud.
- The limited manual protection measures available to secure the enterprise from criminals hacking into their PBX systems.
- The realisation for the enterprise that it is financially/legally. responsible for the charges incurred even though it may feel strongly that the Carrier and VAR should share some of the cost.
- That following a fraud incident, the enterprise still remains vulnerable and financially exposed from further potential attacks as no real prevention exists.

Pbxwall is a novel and innovative voice firewall that live monitors and protects all trunk lines integrated to a PBX system.

Our unique selling proposition is that pbxwall automatically detects a hacker on the trunk lines and blocks their fraudulent call activity.

Pbxwall does not require permit/ deny rules or engineering intervention, or PBX integration to detect and block Toll Fraud.

We would be delighted to talk to you further to see how pbxwall best suits your requirements.

Real Time Detection

In real time, pbxwall continually analyses and compares the audio frames on the active trunk channels for the purposes of detecting fraudulent call traffic.

Automatic Blocking

Pbxwall automatically blocks all fraudulent call activity without the need for engineering intervention, protecting the enterprise 24x7x365. Pbxwall continually protects while the enterprise awaits the arrival of an engineer to plug the breach in the PBX system.

Non Dependency

Our patent protected algorithm provides pbxwall with a unique advantage in that our solution does not depend on rules based configuration or integration to the PBX system to assist in the detection of fraudulent call activity. Continual live monitoring of the active trunk channels insures that pbxwall automatically detects and blocks all fraudulent call traffic.

Carrier & PBX Agnostic

Pbxwall is an independent voice firewall that bridges and protects the trunks that integrate to a PBX system.

Pbxwall is both Carrier and PBX agnostic.

Around the Clock Protection

Pbxwall provides around the clock protection, 24x7x365. Our support centre live monitors all deployments ensuring that all alerts are tracked and dealt with accordingly.

Protect Trusted Relations

Pbxwall protects established trusted relations between vendor and customer.

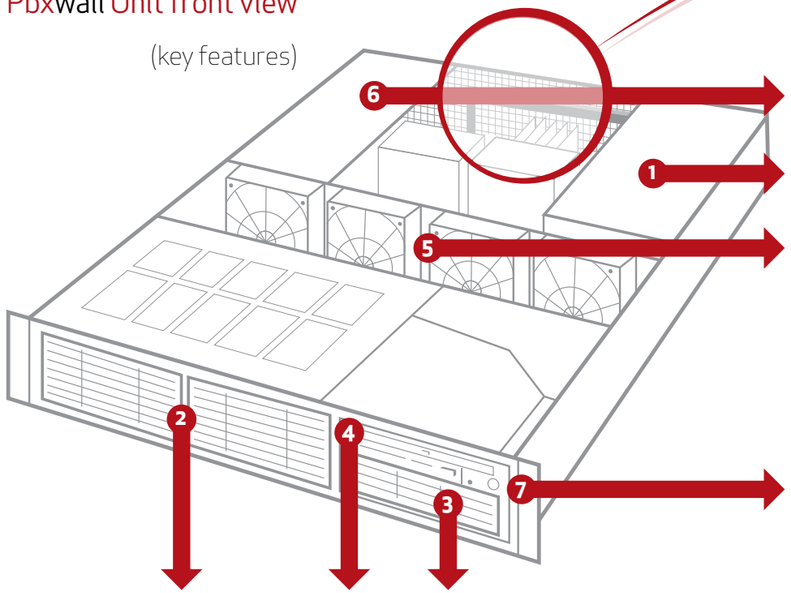
Communicate freely, we've got you protected.

PRODUCT info

The pbxwall product suite includes two solutions, TDMwall™, designed and developed for a pure TDM environment, and SIPwall™ to protect SIP Trunks.

Pbxwall Unit front view

(key features)



6 — 3x PCI Slot via Riser Card (Full Height)

1 — Redundant 500W Power Supply

5 — 4x 80mm Fan Blowers

7 — Power Switch & LED Trunk Indicator

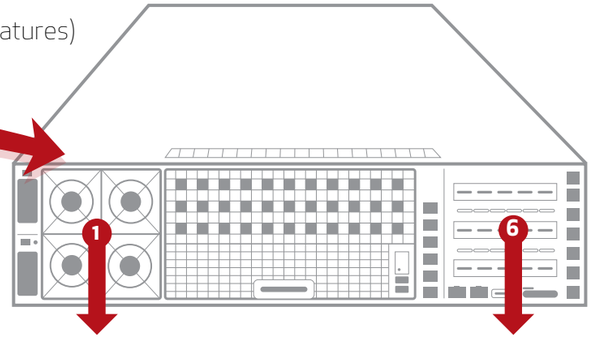
2 — x2.5" HDD Bays

4 — 1x Slim CD-ROM Drive

3 — 1x 5.25" Peripheral Drive Bay

Pbxwall Unit back view

(key features)



1 — Redundant 500W Power Supply

6 — 3x PCI Slot via Riser Card (Full Height)

Chassis	
Form Factor	2U Rackmount
Model	TDMwall
Dimensions	
Height	3.5" (88.9mm)
Width	19" (482.6mm)
Depth	22.5" (571.5mm)
Gross Weight	19Kg
Available Colours	White & Red
Front Panel	
Buttons	▪ Power On/Off ▪ 4x 2.5" HDD Bays

System Cooling	
Fans	4x 80mm Fan Blowers
Environmental	
Temp. Range	Operating 0 - 40
Humidity	▪ Operating: 20%-95% ▪ Non-Operating: 10%-95%
Cooling	Dual 38x38x28mm fans per module
Power Supply	
2U 300W AC Redundant PSU w/ PFC	

AC Voltage	▪ 100-240V, 60-50Hz, 6 amp
DC Output	▪ 5V + 3.3V ≤ 160W ▪ 12V + 5V + 3.3V ≤ 280W
+5V	30.0 amp
+5V standby	2.0 amp
-5V	0.3 amp
+12V	15.0 amp
-12V	0.8 amp
+3.3V	20.0 amp

OUR support *Network Operation Centre (NOC)*

Our NOC provides around the clock support, its responsibilities include:

- Live monitoring and configuration backup for all deployed pbxwall systems.
- Case management for all reported incidents of fraudulent call activity.
- Remote access for the authorisation of permitted call forwarding numbers.
- Communication with on-site technicians, supporting installs and tracking problems through resolution.
- If necessary, our NOC will escalate problems directly with the VAR.
- For severe conditions that are impossible to anticipate – such as a complete system failure, our NOC has procedures in place to immediately dispatch a pre-configured pbxwall system along with an engineer to remedy the problem.

YOUR questions

Q. What is PBX Hacking?
A. PBX hacking is a term used to describe a method used by criminals to illegally breach the security parameters of a PBX system.

Q: Why do criminals hack PBX systems?
A: Criminals hack PBX systems for the purposes of accessing the trunk lines after which they begin generating as many calls as possible to expensive overseas telephone numbers off which the criminal collects 90% of this revenue.

Q. How does a criminal hack a PBX systems?
A. Common methods include:

- Accessing the call divert functions within the voice mail and changing the routing number.
- Log on to the remote maintenance port and re-configure the class of service tables.
- Registering as a SIP account.
- Working with internal staff members to manually divert an extension.

Q. Why do criminals make calls to expensive overseas number?
A. Criminals register international premium rate numbers, all calls made to these numbers generate a significant profit for the criminal.

Q. How much is a call to an international premium rate number?
A. Individual call costs average €2.80 per minute.

Q. Who pays for the calls made to premium rate numbers?
A. The owner of the trunk lines is billed for all calls.

Q. Why should an innocent party have to pay for calls they never made?
A. The Carrier in question is legally entitled to collect their fees and the enterprise is legally responsible to pay the bill.

Q. Who are the perpetrators and why shouldn't they be prosecuted
A. The perpetrators generally reside outside the country. Due to lack of global regulation, language barriers and general cooperation, investigations remain open ended.

Pbxwall Ltd.
Unit E7, North City Business Park,
North Road,
Dublin 11, Ireland

T +353 1 2057999
F +353 1 2057998
E info@pbxwall.com
W www.pbxwall.com