

Incident Response For VOICE Services

***Lee Sutterfield
President
SecureLogix Corporation***

***13750 San Pedro
San Antonio, TX 78232
lsutt@securelogix.com
www.securelogix.com***

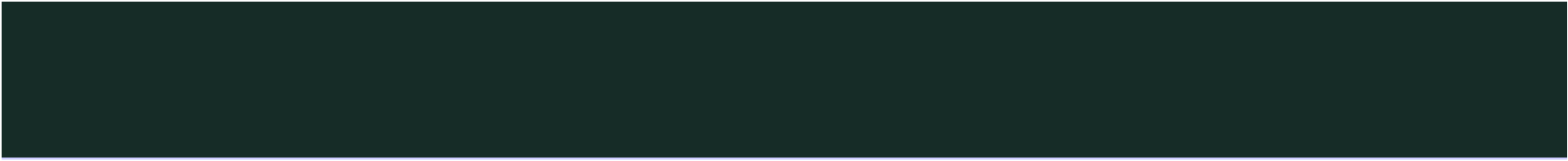
The Voice Service has long been a useful and lucrative attack vector into the Enterprise data network.

Voice Firewall technology provides the Enterprise with the other half of “360 degree” visibility and control over the enterprise electronic perimeter.

Voice Incident Response is increasingly needed to address both the obvious impact to costs and operations of attacks against the voice service itself and the security risks that rise from the logical and physical interconnectivity of voice and data services.

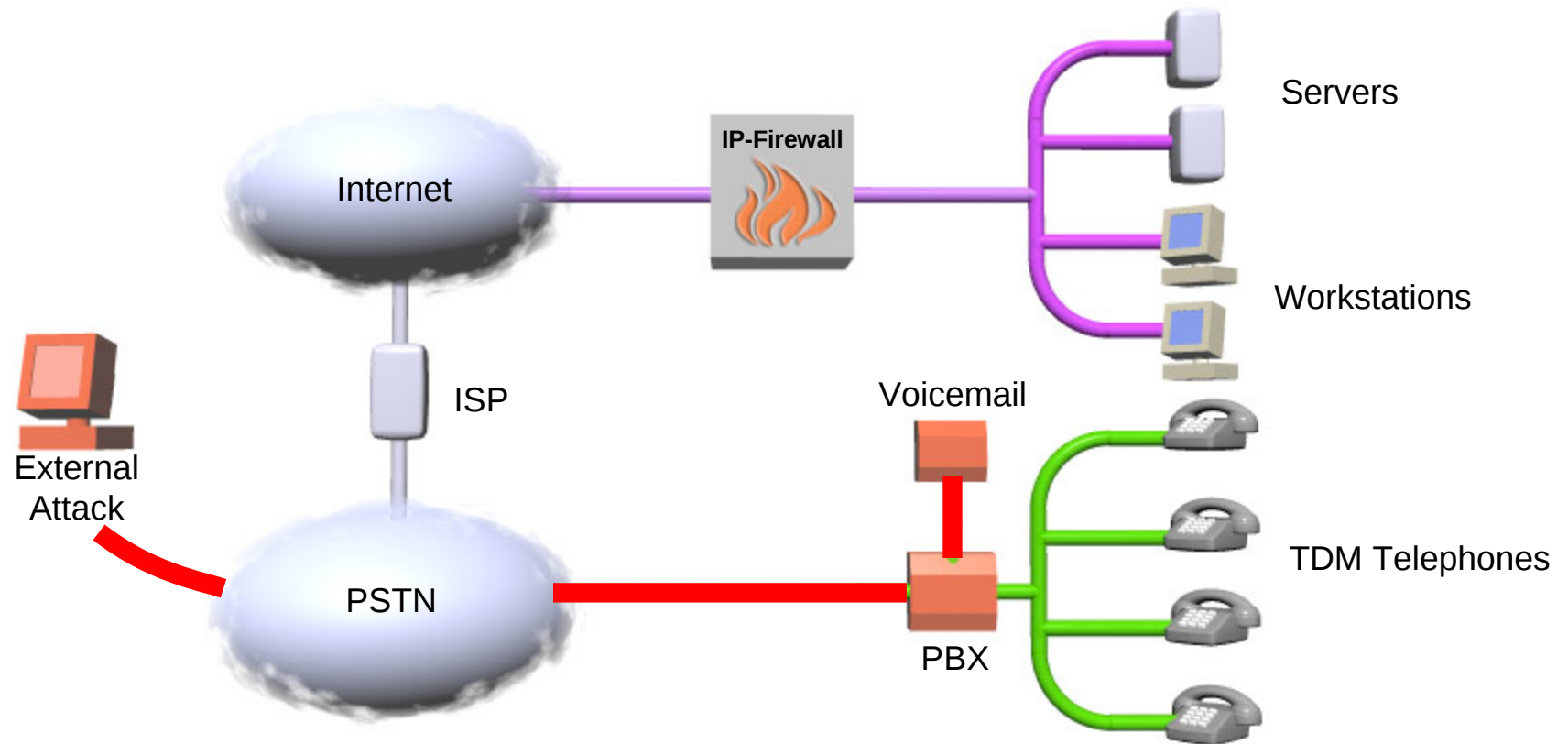
Overview

- Legacy Voice Security
- *Voice Firewall* Technology Base (circuit switched)
- Campus VoIP Security
- IP Trunk Security
- *Voice Firewall* Technology Base (packet switched)
- ***Incident Response for VOICE Services***



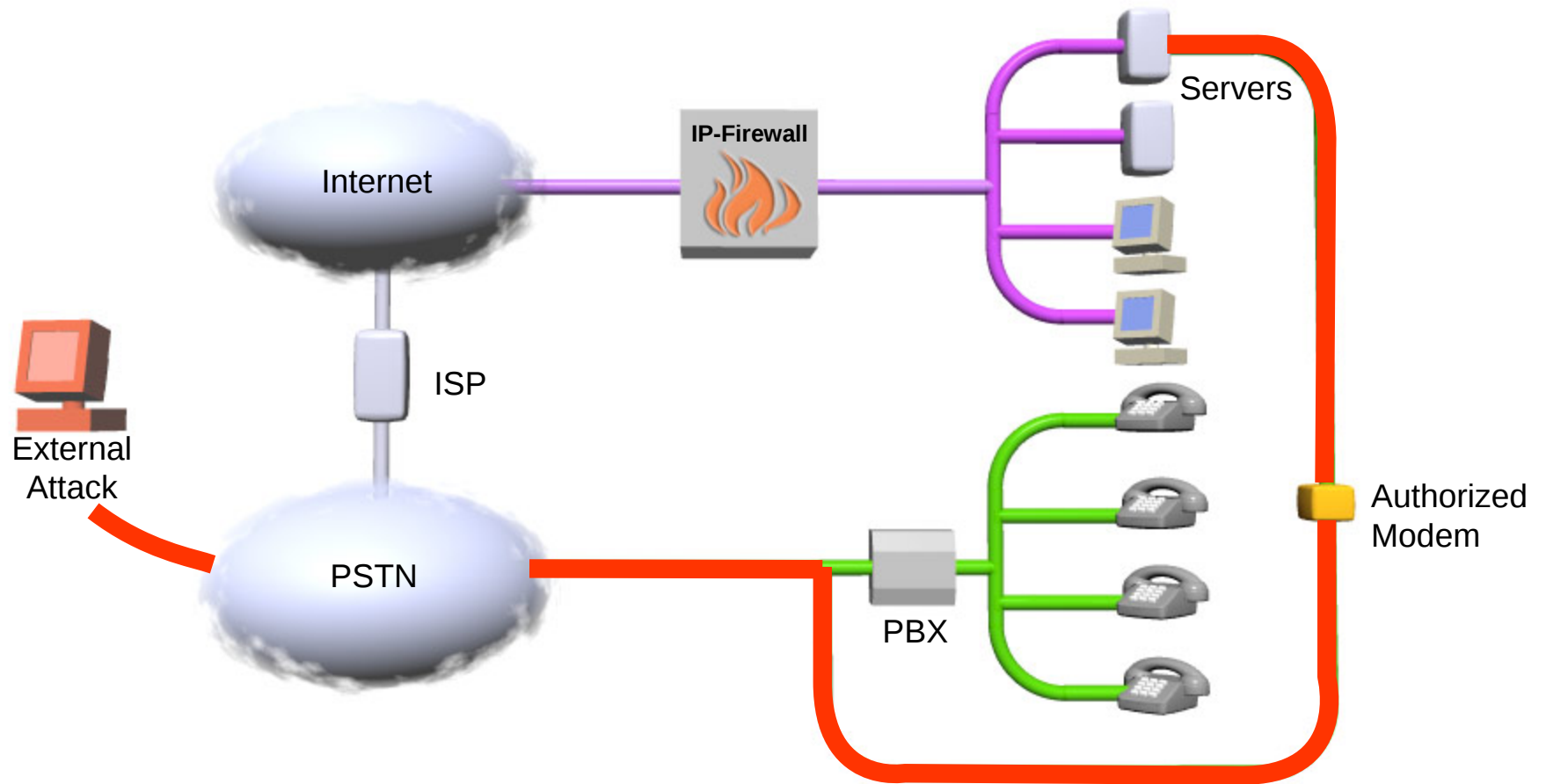
Legacy Voice and Data Network Security Issues

Voice Service Availability / Theft

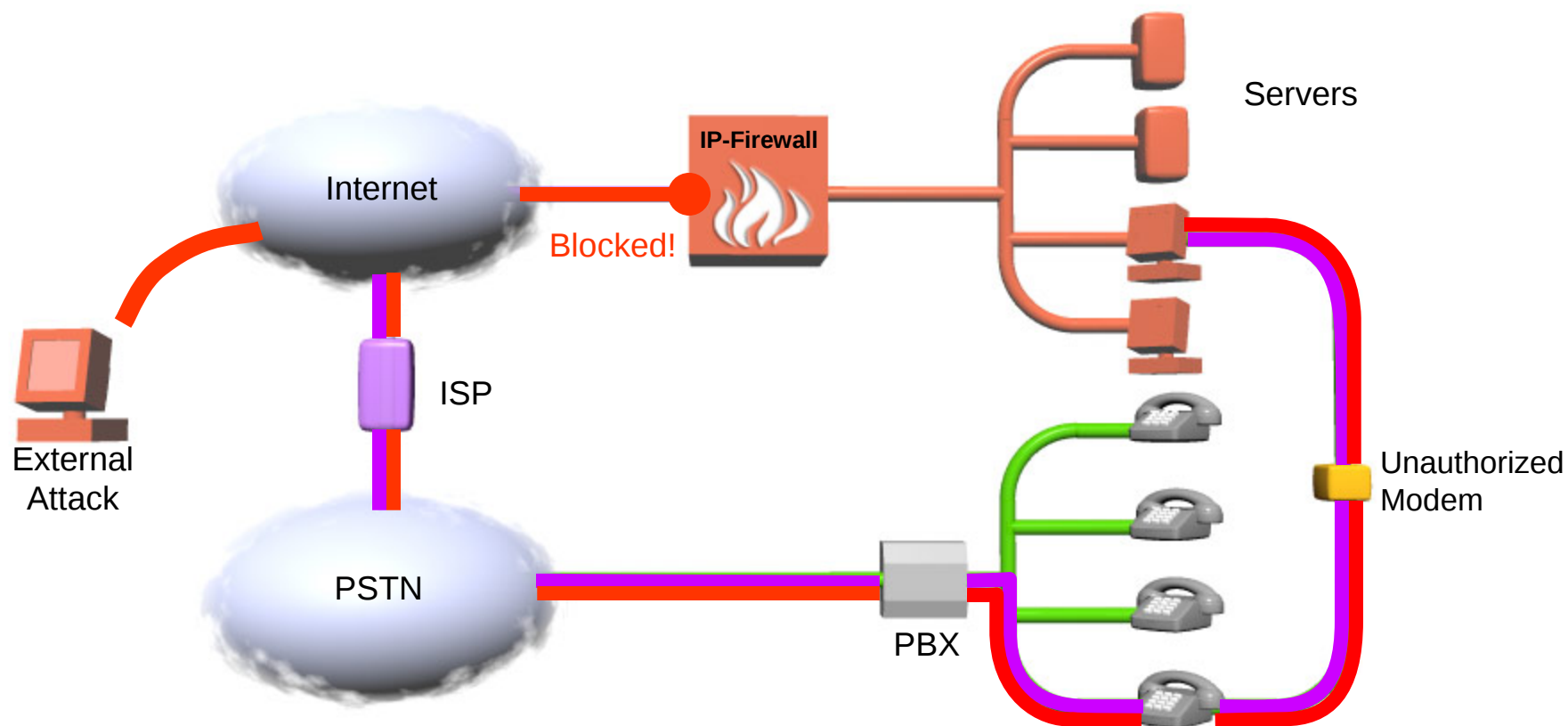


Significant increase in reported TOLL FRAUD in the last three years.

Cross Network Attacks - Authorized Modems



Cross Network Attacks - Unauthorized Modems

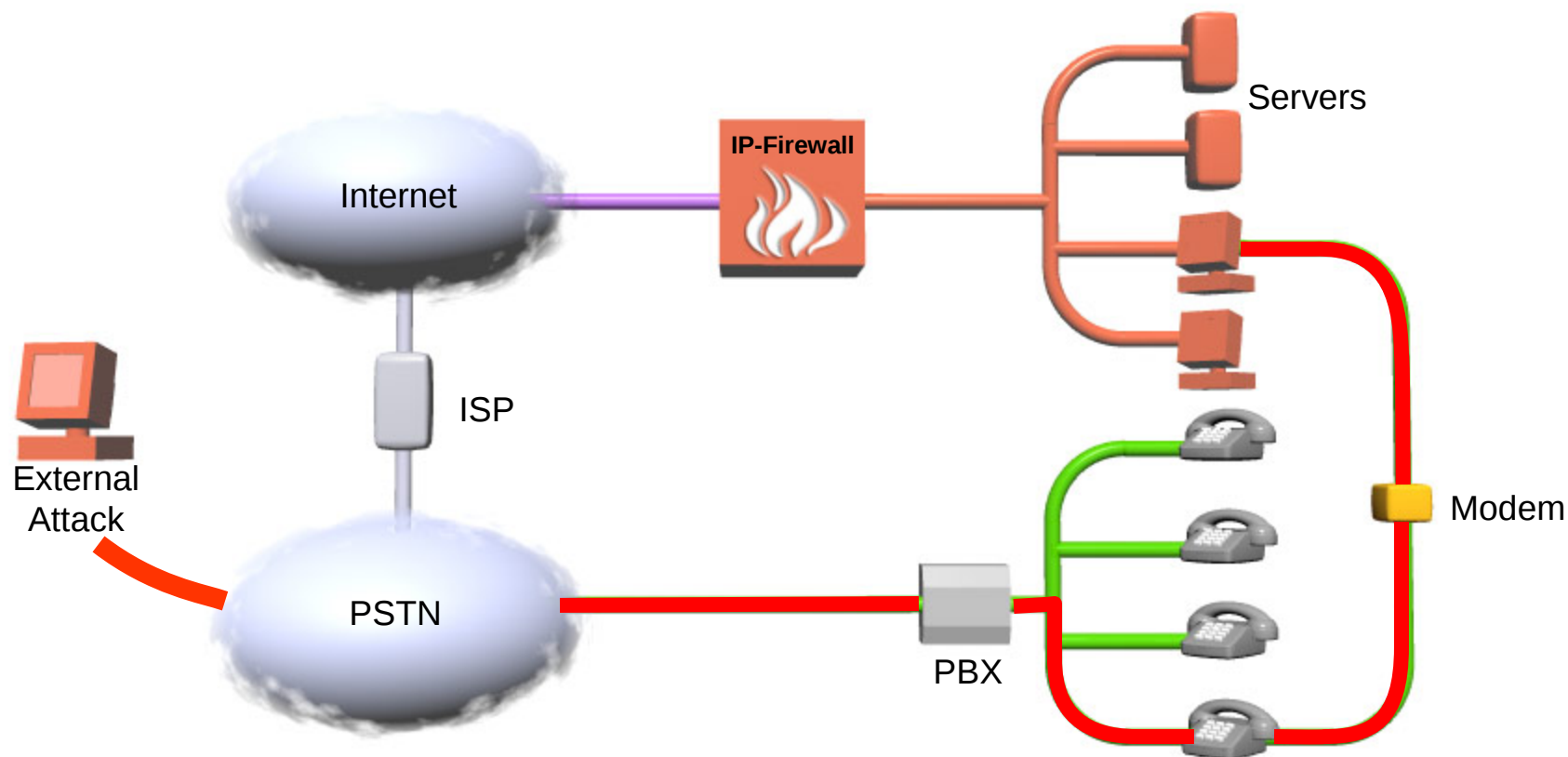


Employees use a modem to dial around the Firewall and IDS.

Hacker “piggybacks” off ISP connection to access the Data Network.

Biggest issue might be re-contamination with malicious software.

Cross Network Attacks – WarDialing

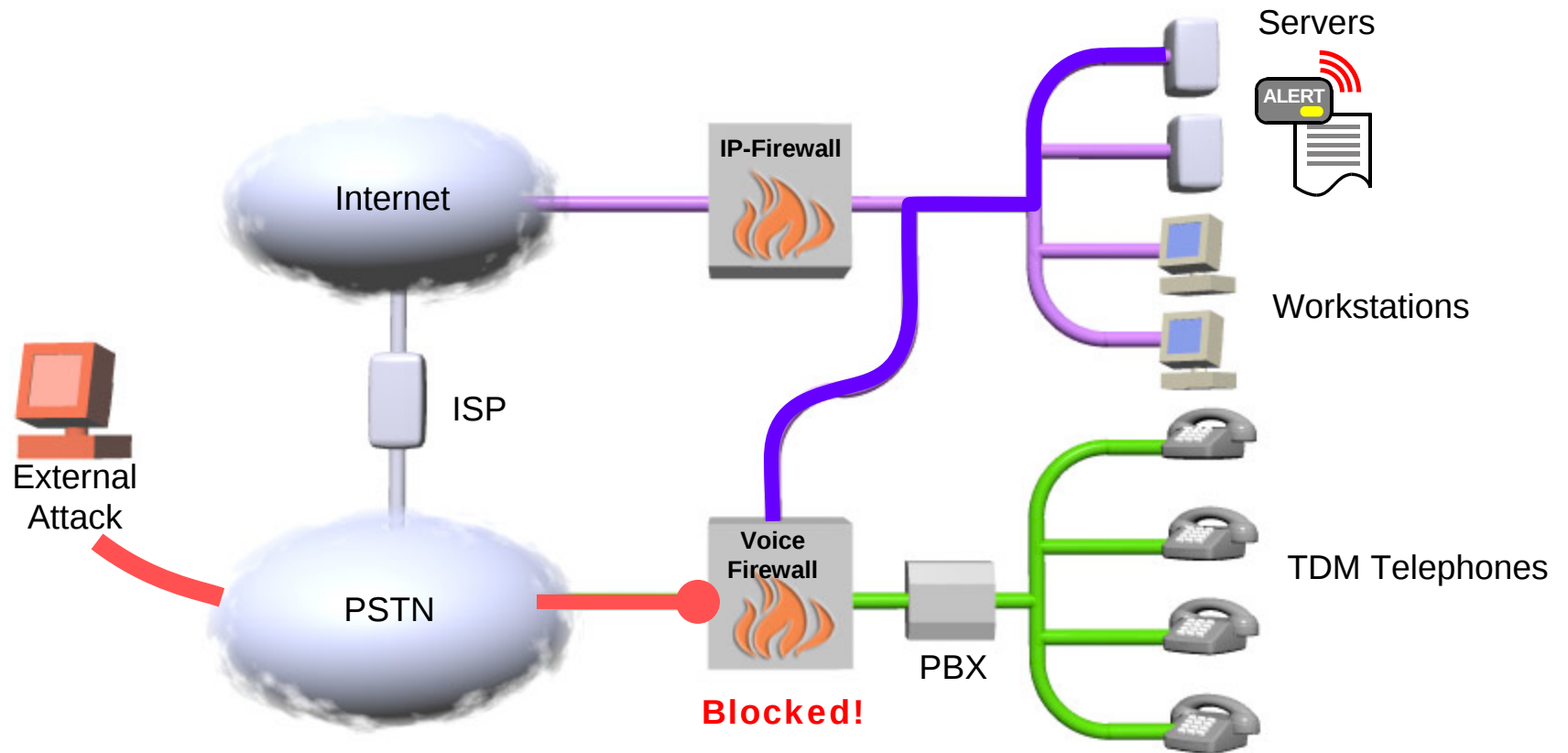


Whitehat Wardialing – 2 % -4 % of phone lines have unauthorized modems.

However, only 20 % of UNAUTHORIZED modems detected via Whitehat Wardialing.

Voice Firewall Technology Base

Voice Firewall Deployment in TDM Network



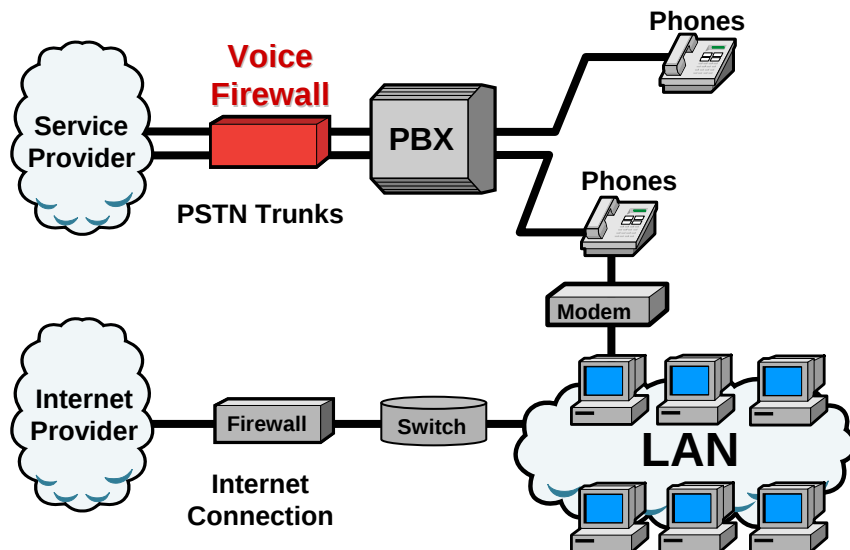
Voice Firewall Core Functionality

- **Log all Call Progress Information:**
 - Source, destination, time, duration, etc...
 - Enterprise-wide, real-time, back to central server
- **Characterize Call Type:**
 - Voice, fax, modem, VTC, STU-III (secure)
 - Continuous monitoring of call for type changes
- **Generic Security / Management Policy:**
 - Rule-based analysis of each call
 - Autonomous execution
 - Centrally managed push-down policy

*Also a logical platform to support
POLICY BASED CALL RECORDING with centralized, near real-time retrieval.*

Technology Overview

Voice Firewall



Application Suite

Performance Manager:

Enterprise-wide dashboard. Real-time performance monitoring & diagnostics.

Voice Firewall:

Blocks phone line attacks. Controls voice network access and service use.

Voice IPS:

Prevents malicious and abusive call patterns such as toll fraud.

Usage Manager:

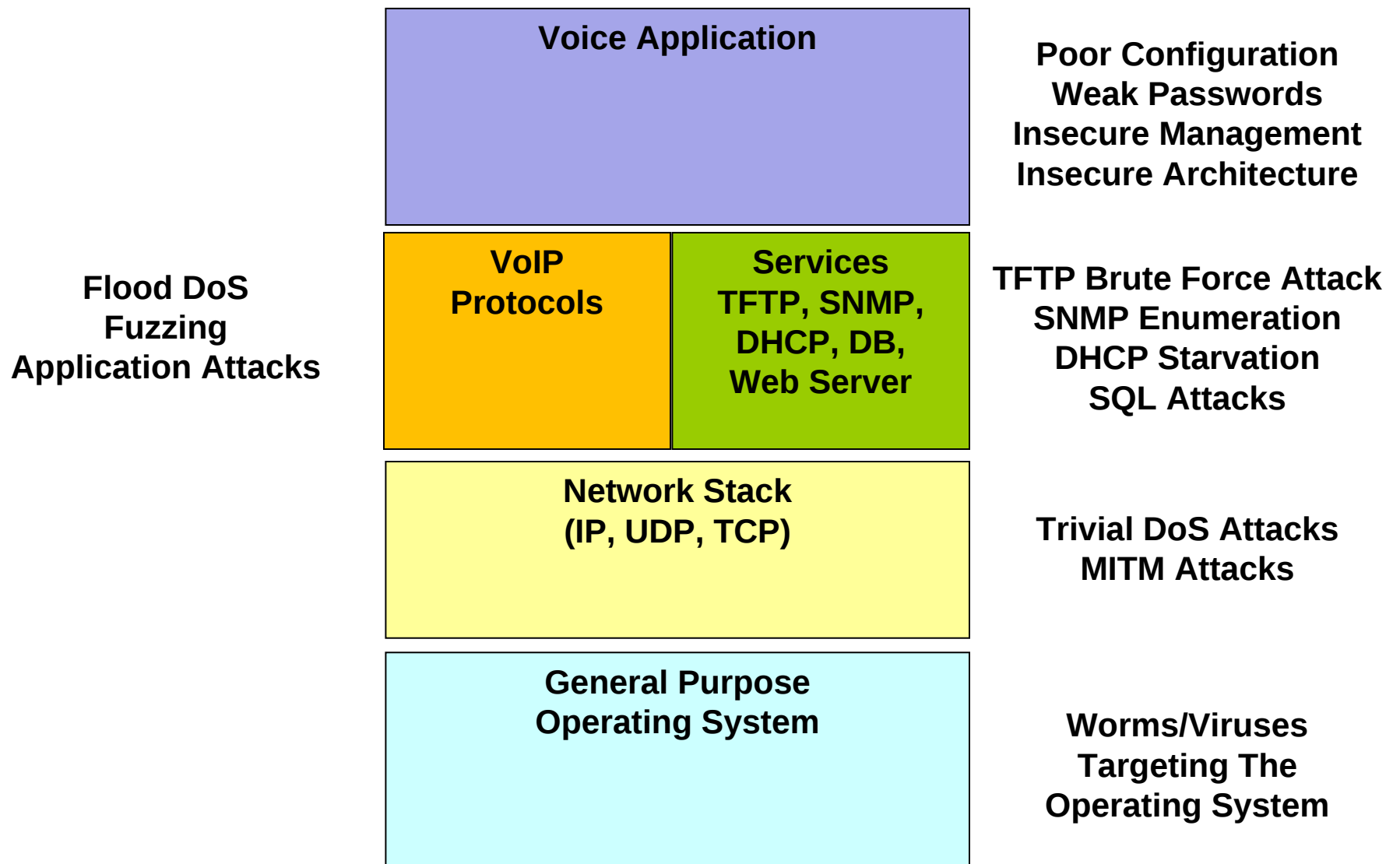
Enterprise-wide, PBX-independent CDR, call accounting, & resource utilization.

Call Recorder:

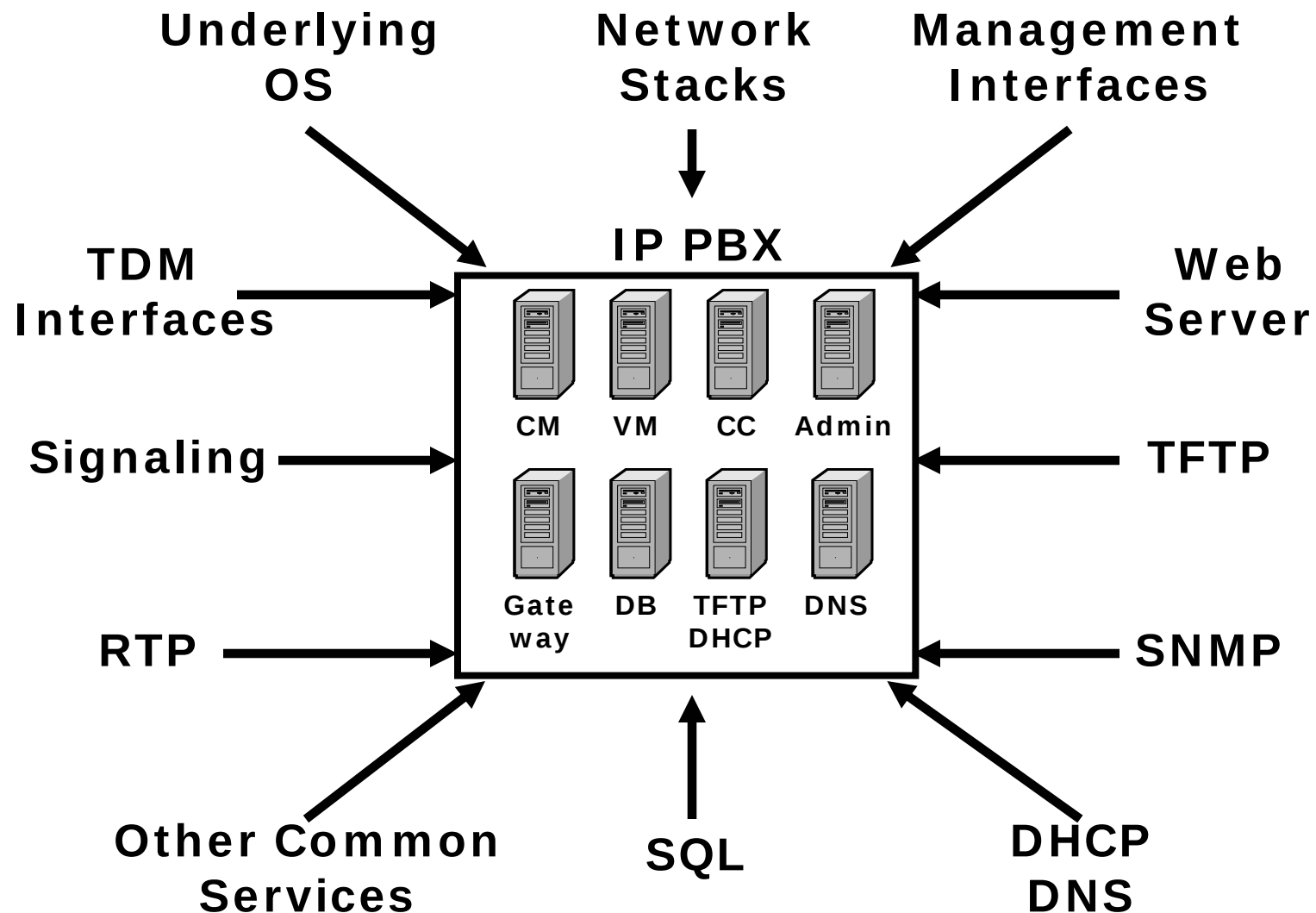
Policy-based recording of targeted calls. Trunk-side, cost effective solution.

Voice Firewalls and Campus Level VoIP Deployments

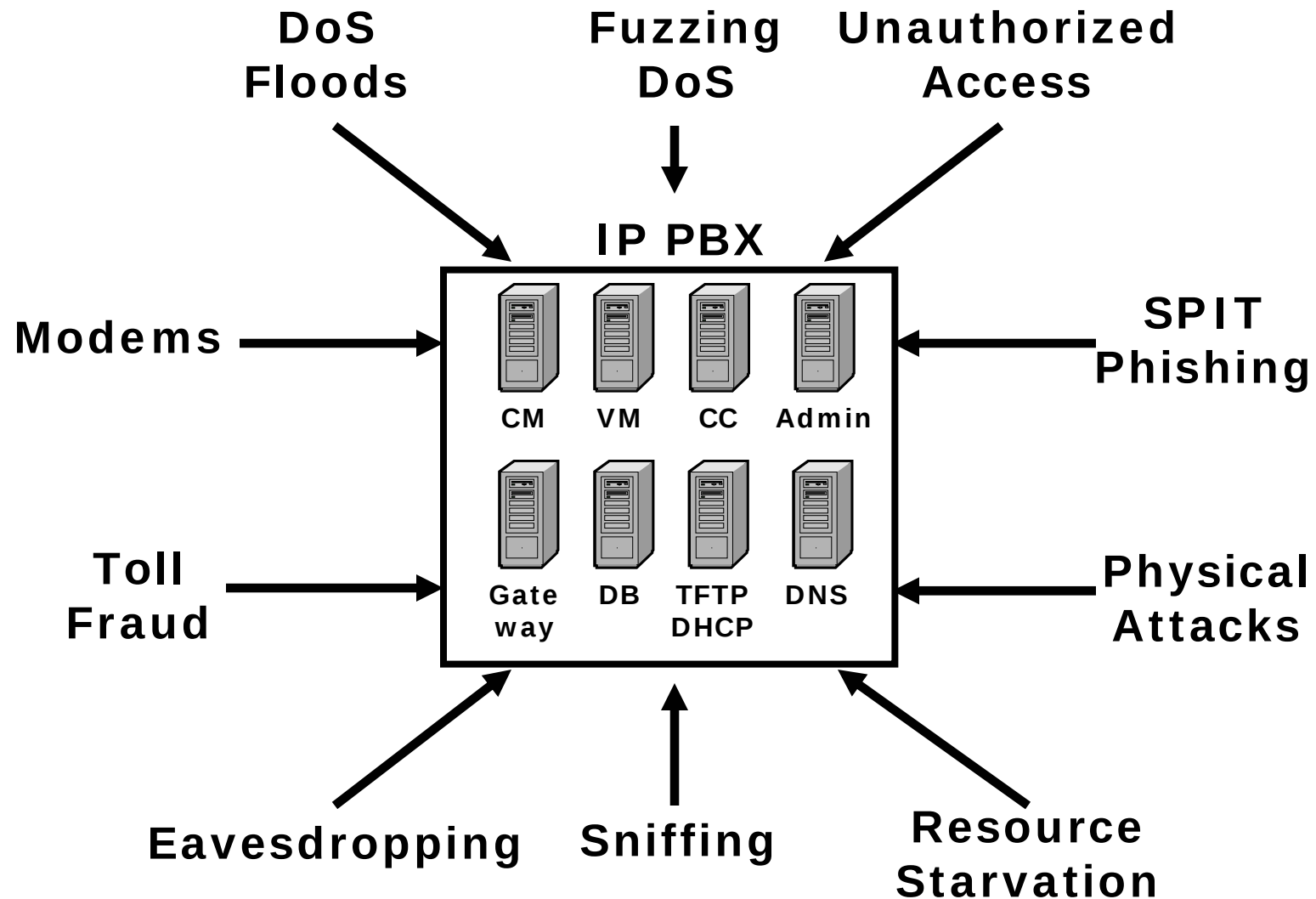
IP PBX Vulnerabilities



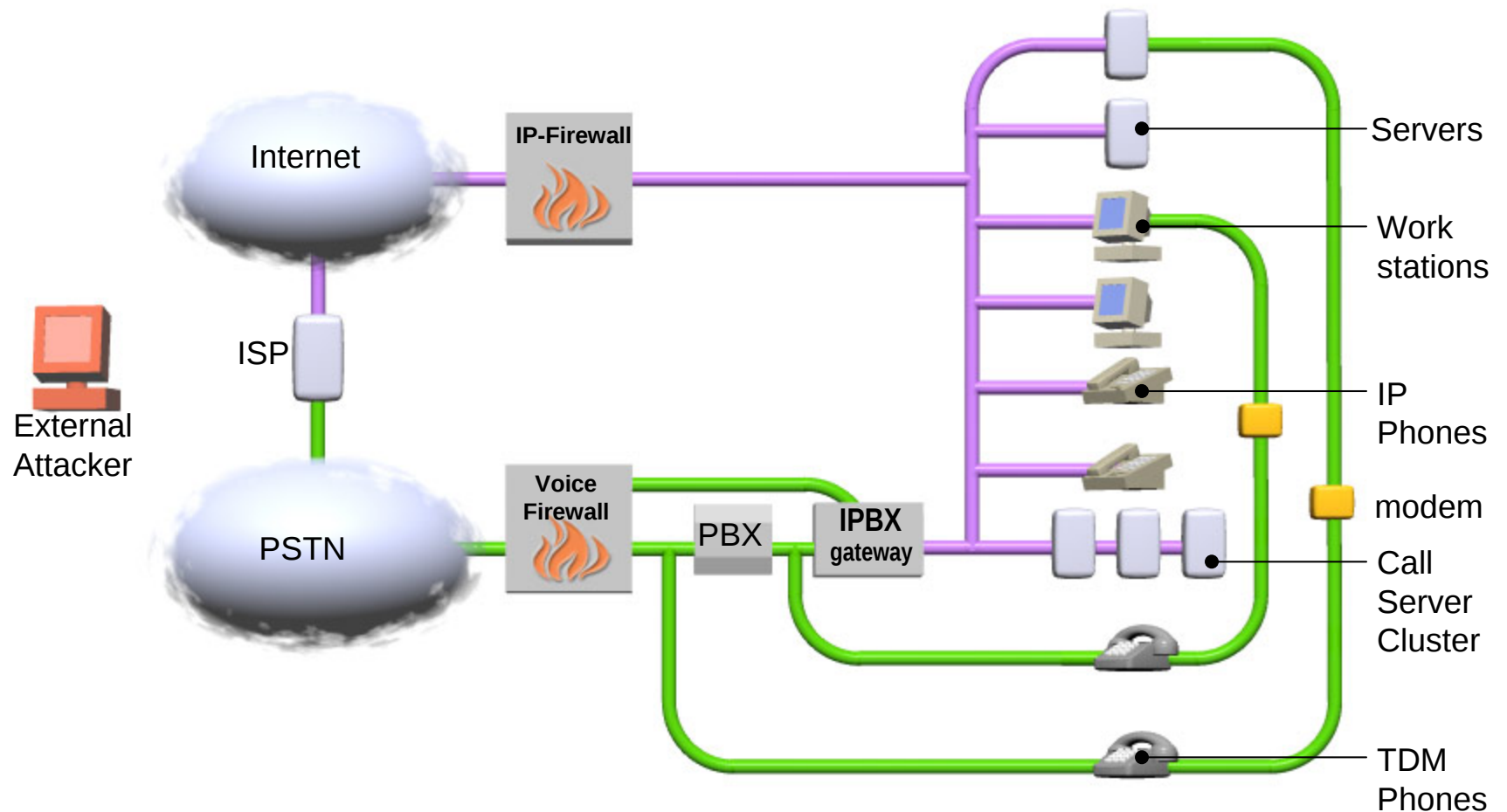
IP PBX Vulnerabilities



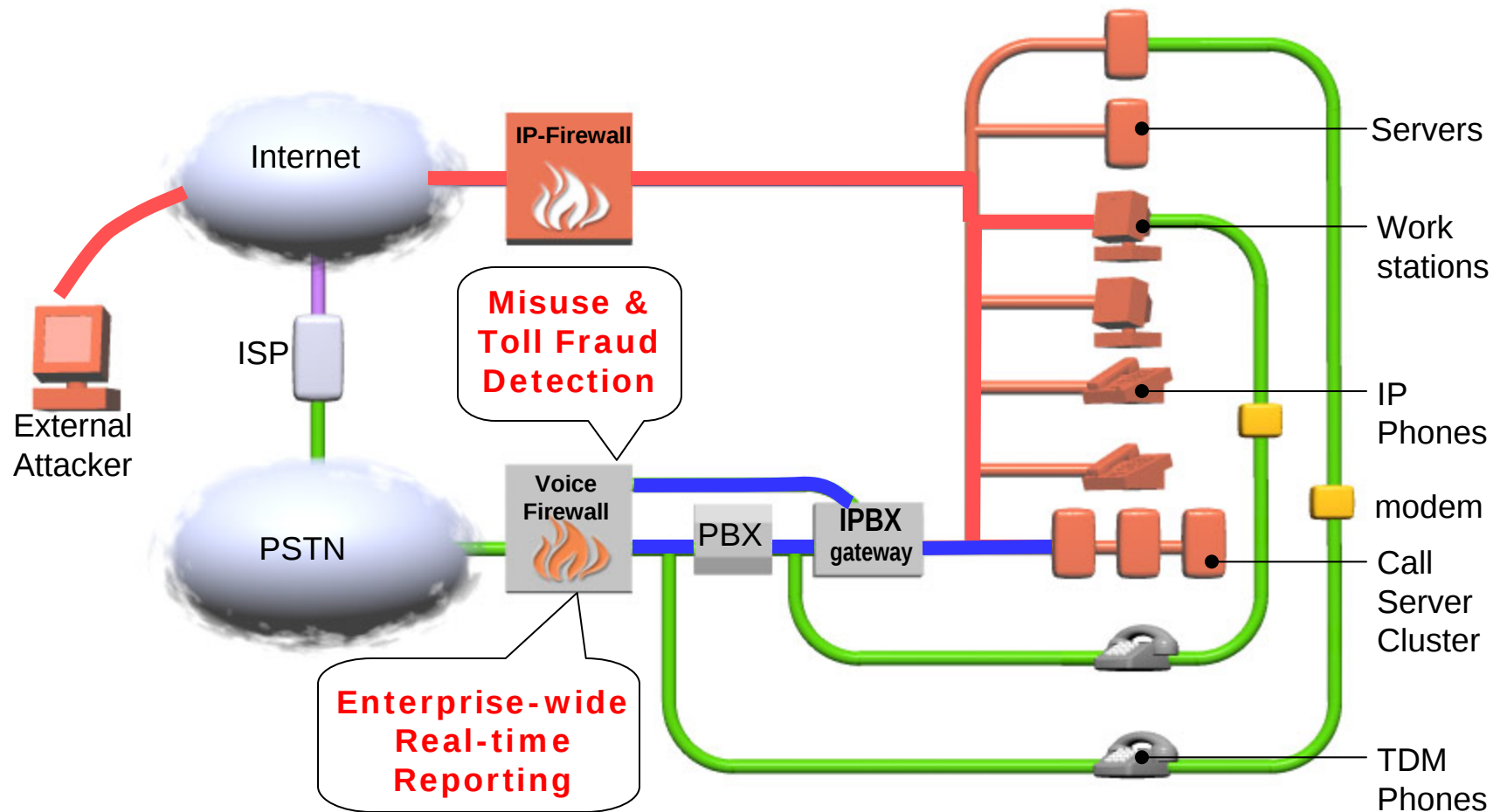
IP PBX Attacks



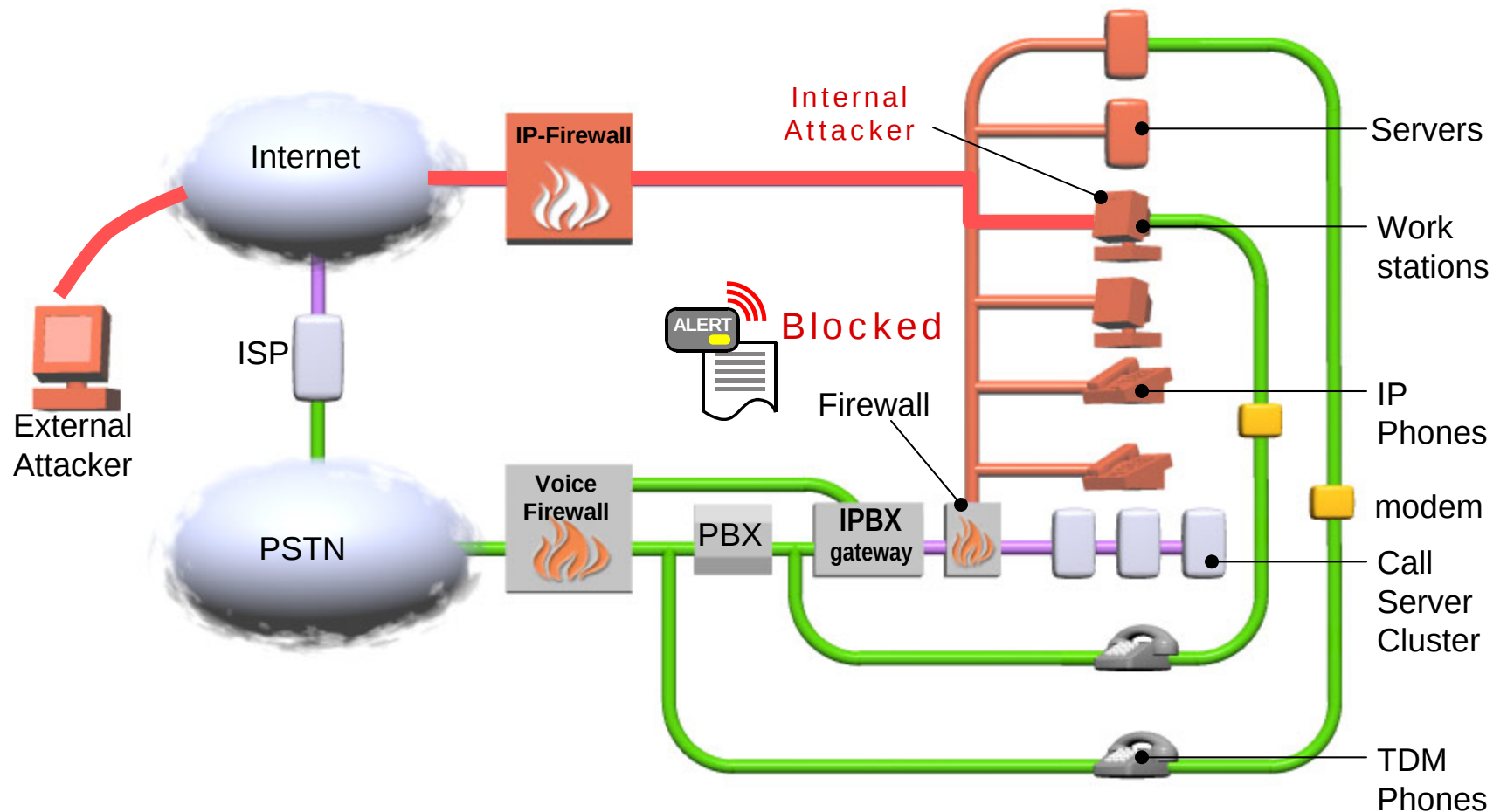
Campus VoIP Server Security



Campus VoIP Server Security



Campus VoIP Server Security



Security Impact of VoIP Deployments

Campus VoIP deployments have enriched the *vulnerability* base, increased the *target set* and multiplied *attack vectors*.

However, the level of attacks still appears relatively low because the overall VoIP target set is still comparatively small and not yet connected directly to the public network.

Voice Fraud in the News

Communications Fraud Control Association's

March 2006

"Terrorist organizations embrace communications fraud to generate funds by illegally gaining access to a network and then reselling the service."

<http://www.cfca.org/pdf/press/3-28-06PR.pdf>

Businesses Ignore Telecoms Fraud (Huge Losses)

July 2008

<http://www.networkworld.com/news/2008/072808-businesses-ignore-telecoms.html>

BT: Fraudsters Return to Dial Through Fraud/PBX Hacking

December 2008

<http://www.networkworld.com/news/2008/072808-businesses-ignore-telecoms.html>

Cybercrime Cost Firms \$1 Trillion Globally, McAfee Study Says Hacker Makes Costly Calls

December 2008

http://www.winnipegfreepress.com/local/hacker_makes_costly_calls.html

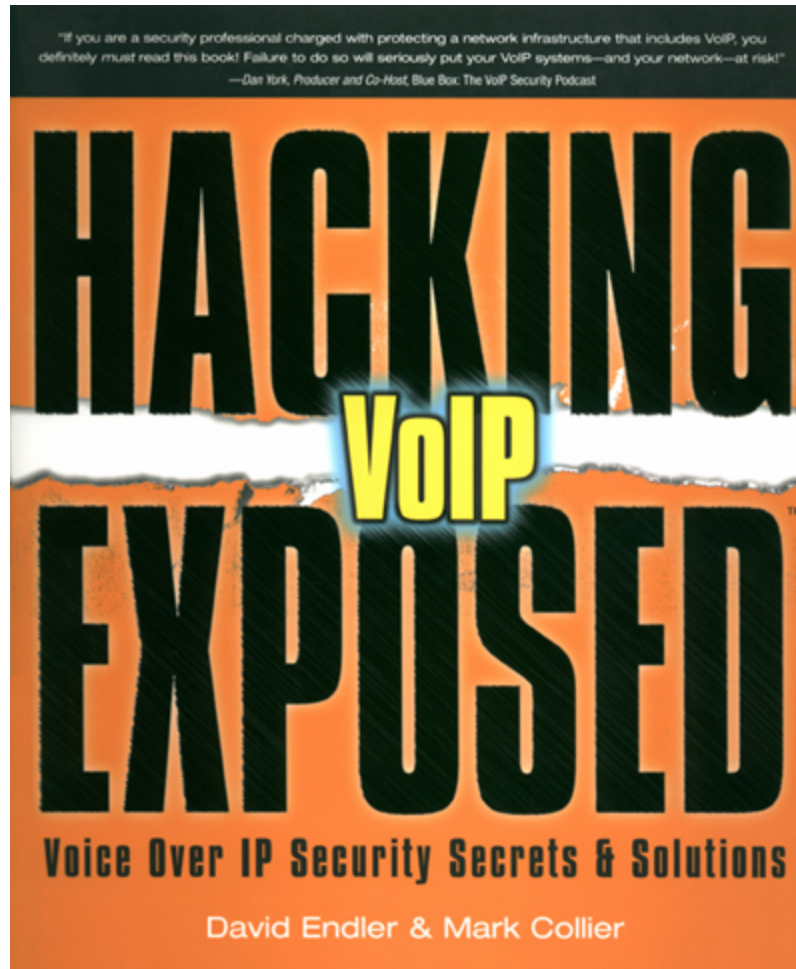
FEMA Phones Hacked; Calls Made to Mideast, Asia

August 2008

<http://www.msnbc.msn.com/id/26319201>

These are only a few out of hundreds of cases!

Hacking Exposed

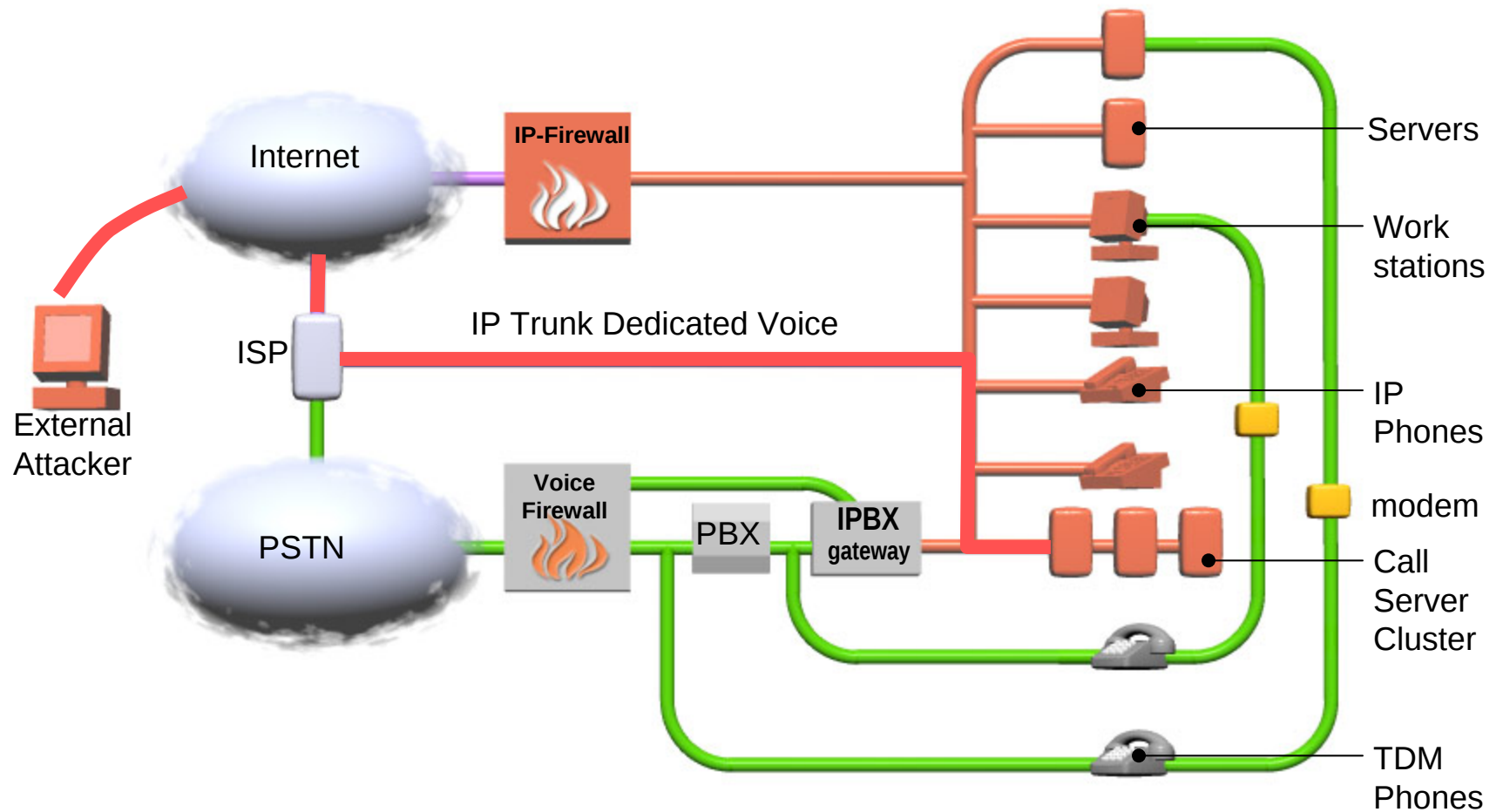


Still the most
comprehensive VoIP
Security book on the
market.

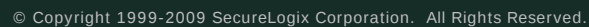
Voice Firewalls and SIP Trunking

IP Trunk Risk

External attack through IP Trunks against IP Voice and Data Network

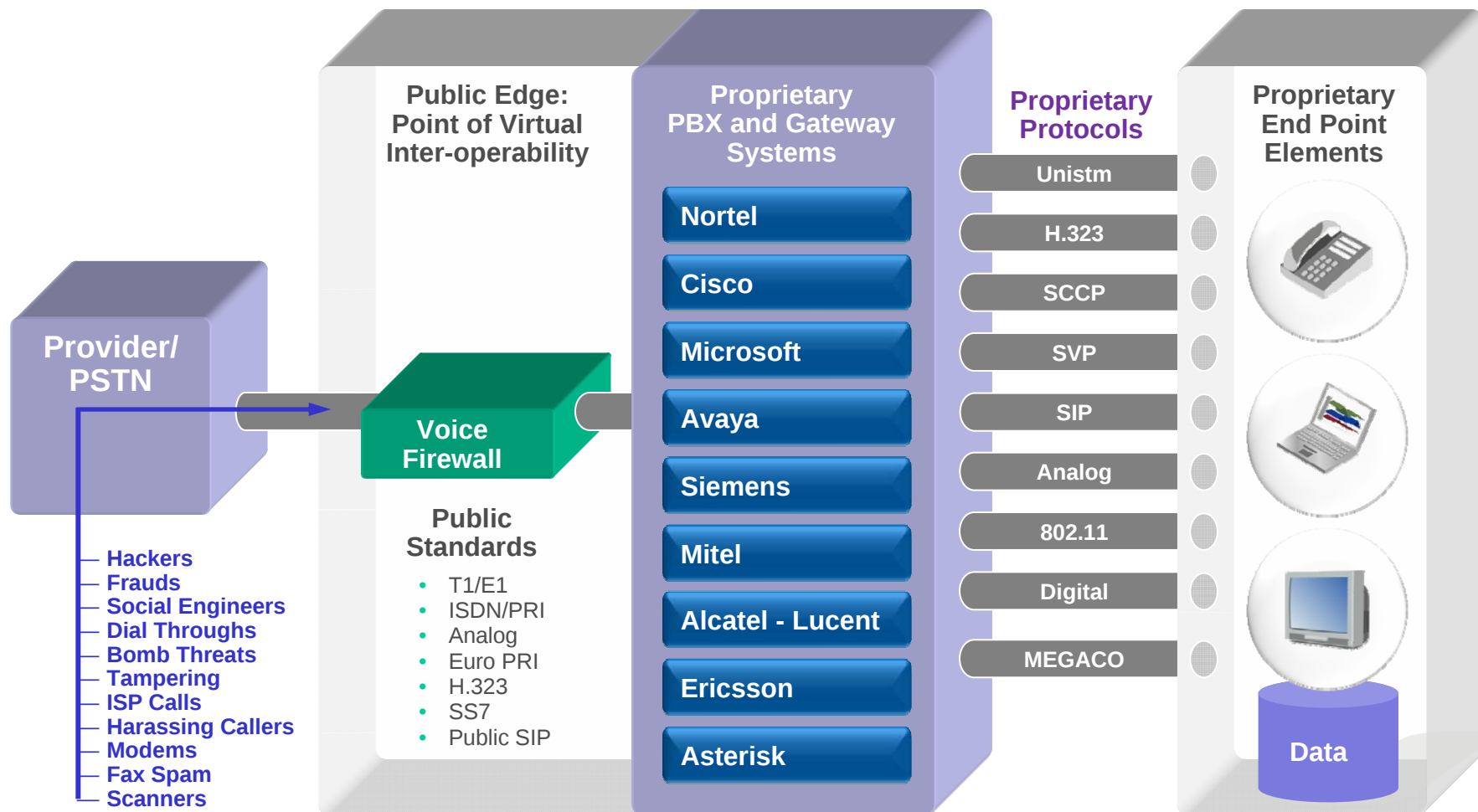


Real-Time Mixed Media Firewall



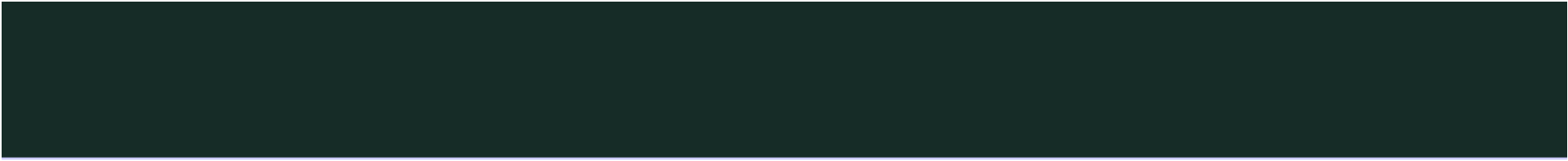
The Point of Protection is at the Edge

Phone network is still your largest network!!??



SIP is just another protocol!

But the VOICE SERVICE is NOT JUST ANOTHER APPLICATION!!



Voice Firewalls Impact on Incident Response

Voice Originated Attack Scenario

1. Voice connections to data network provide near 100% success rate for invisible access to data network resources
2. Voice network connections are relatively slow so they're usually used to gain unauthorized access but not usually used for target exploitation
3. Once bogus accounts are established the attacker will usually exit the phone connection and enter via the newly established accounts via the data network connection
4. Ongoing exploitation is conducted at normal network speeds until discovered
5. If accounts are closed the attacker simply returns to the voice network to gain access again and repeat the above
6. The Enterprise has NO visibility into this exploit without the deployment of VOICE FIREWALL technology

Incident Response for Voice

- Legacy voice network interconnectivity has always been a step-child attack vector for the security community but it has never fallen out of favor with the hacker community
- Enterprise security operations and incident response teams are running half blind without addressing VOICE INCIDENT RESPONSE
- VoIP deployments exacerbate the problem but Voice Firewall technology addresses these new issues as well
- Voice network vulnerabilities, such as modem based interconnectivity, are already recognized throughout traditional security best practices and is growing in importance in regulatory and compliance communities

Voice Incident Categories

- **Unauthorized modems** used for ISP sessions
- **Remote access (modem) attacks** against server farms and PBX's
- **Phone service misuse** by authorized personnel (Employee and Janitorial Toll Fraud)
- **Toll Fraud** attacks against PBX's and VoIP Systems
- **Harassing/Threatening calls** against personnel and executive staff
- **Malicious Software** insertion/re-infection via ISP sessions (unauthorized modems)
- **Vishing attacks** - social engineering exploiting call centers (call recording)
- **Denial of Service** attacks via VoIP system vulnerabilities
- **Bomb threats** - need quick call capture, retrieval and dissemination (call recording)
- **Improve voice uptime** via real-time forensics/diagnostics/alerts
- **Stop data leakage** via voice resources
- **Reduce telecom total cost** of ownership - peak utilization rates, outages, etc.
- **Baseline/plan/optimize** new UC/VoIP deployments
- **Policy-driven recording** of targeted calls for compliance, safety and forensics

Summary

- Voice Firewall technology addresses age old vulnerabilities
- Voice Firewalls provide a lock-down mechanism for containment, eradication and recovery for the other half of the enterprise communications network during malicious software outbreaks and network attacks
- Voice Incident Response falls neatly within the construct for traditional incident response practices: *preparation; prevention; detection and analysis; containment, eradication, and recovery.*
- Growing interest from the Enterprise market such that Voice Incident Response is being offered within new Managed Security Services for Voice (MSSVs)