Welcome to the Cisco Collaboration Community!

Enterprise Voice Security and Policy Using Cisco ISRs and ASRs

Technical Briefing
June 4, 2013

Speakers

John Vickroy
Product Manager
Cisco

Mark Collier
CTO and VP of Engineering
SecureLogix

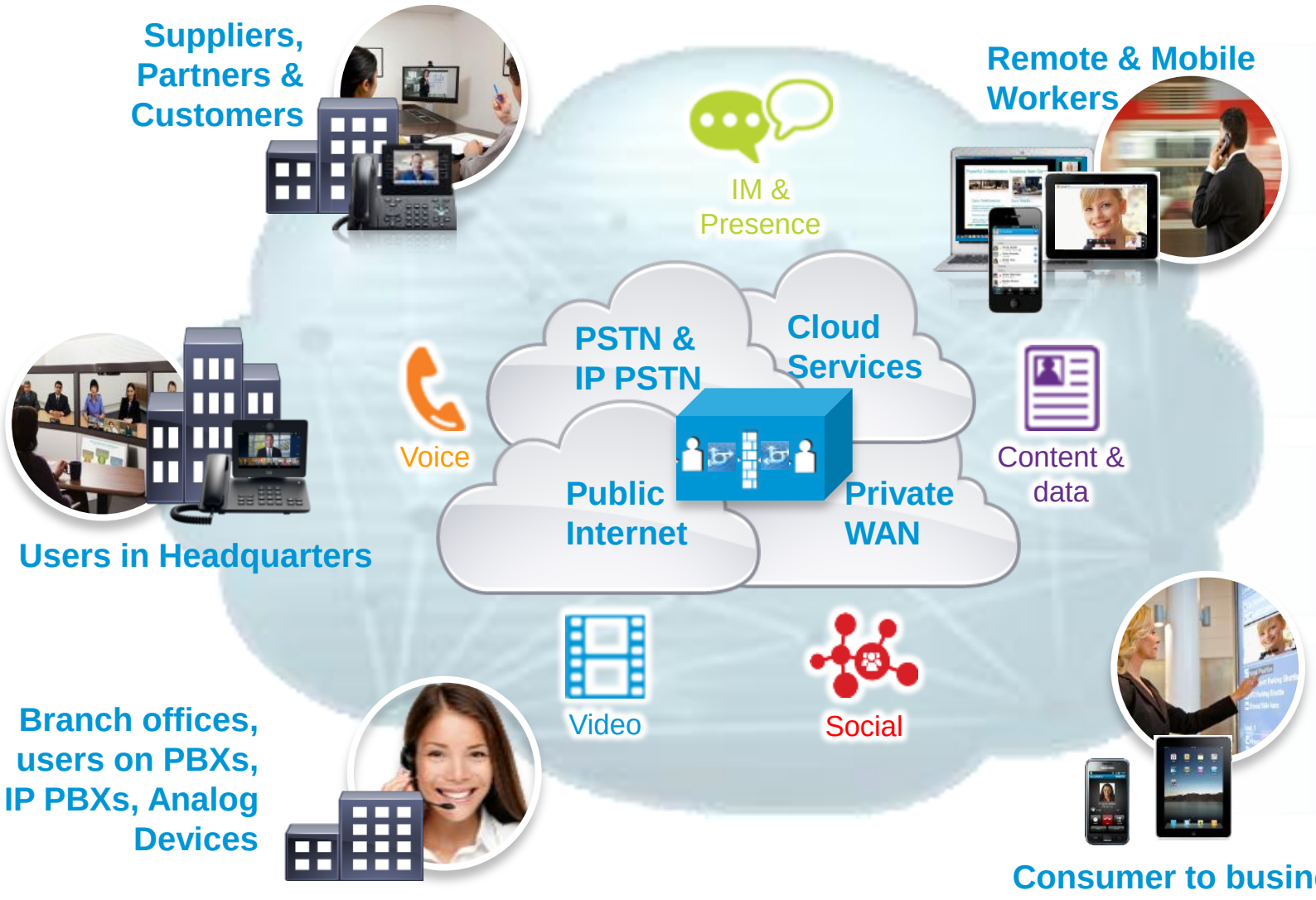
Rod Wallace
VP of Global Services
SecureLogix

Agenda

Topic and Timeframe (Pacific Time Zone)	Presenters
8 - 8:05 a.m. (5 min): Webcast logistics and welcome	**Patty Medberry**, Solutions Marketing Cisco
8:05 - 8:15 a.m. (10 min): CUBE product strategy Value of integrating voice policy and security into Session Border Controllers (SBC)	**John Vickroy**, Product Manager Cisco
8:15 - 8:45 a.m. (30 min): Unified communications policy and security Overview of threats to enterprise telephony network	**Mark Collier,** CTO and VP of Engineering SecureLogix
8:45 – 9:15 a.m. (30 min): Unified communications policy and security Details of TDoS and other voice policy use cases	**Rod Wallace,** VP of Global Services SecureLogix
9:15 – 9:25 a.m. (10 min): How Cisco and SecureLogix deliver a joint voice policy solution Webcast summary – key takeways	**John Vickroy**, Product Manager Cisco
9:25 – 9:30 a.m. (5 min): Next steps - evaluation and resources	**Patty Medberry**, Solutions Marketing Cisco

Cisco Collaboration Edge

Seamless multi-modal experiences to anyone, anywhere on any device



Open, Standards-based

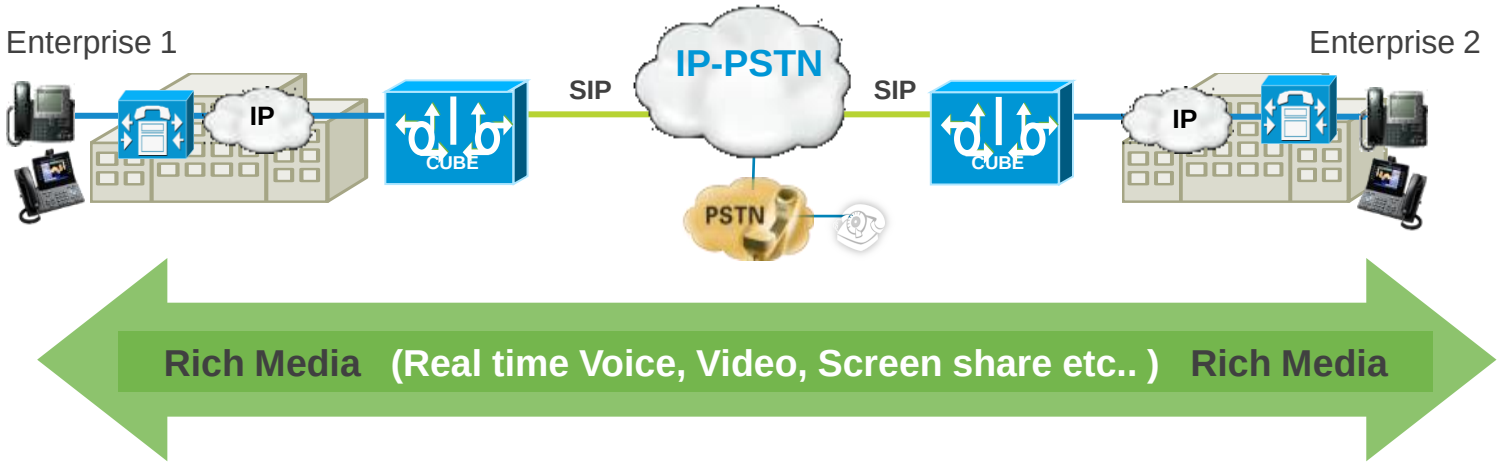
Proven Security

Architectural Flexibility

Seamless User Experiences

Cisco Unified Border Element (CUBE)

Cisco's Market Leading SBC is Essential UC Infrastructure Component



Deployed since 2004. The only router integrated SBC on the market.

7,000 customers, with 500 new customers per quarter, deployed in 160 countries

Market Share Leader for Enterprise Session Border Controllers (SBC) per Infonetics Research

In all segments: Finance, Manufacturing, Retail, Government, Defense, Emergency Services, Education & Healthcare

Collaboration Edge Use Cases Supported by CUBE

PSTN Access

Smoothly transition from TDM to SIP trunks

Using policy tools to monitor proper usage

Intra-Enterprise Connectivity

Trunk routing between multiple CUCM clusters

Inter-Cluster Routing

Business to Business

Secure Conferencing and Tele-presence between different organizations

Any network, public or private, voice and video

Remote Access

Consistent experience outside the network

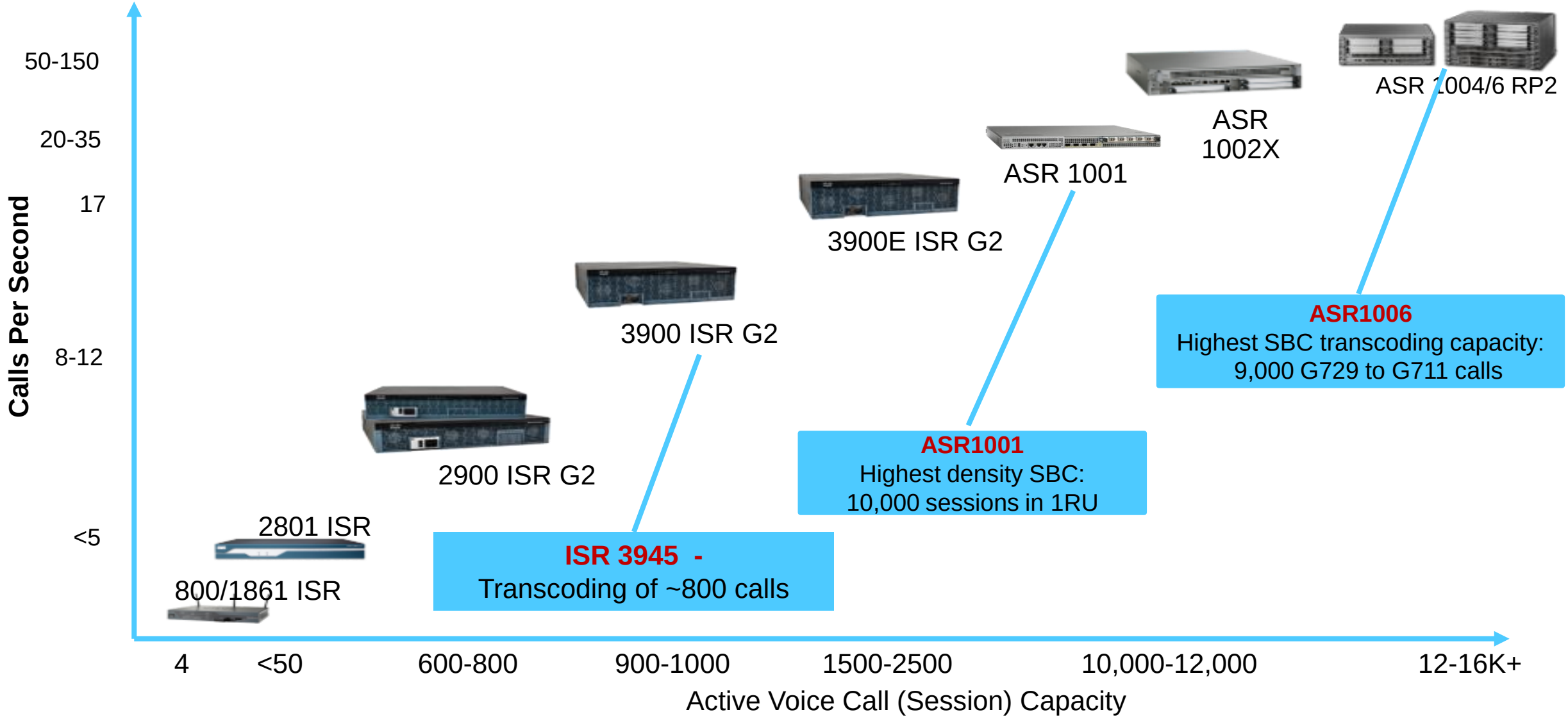
Securely on any device

Cloud Services

Hosted call control (HCS) and conferencing services

Improve reliability & connectivity

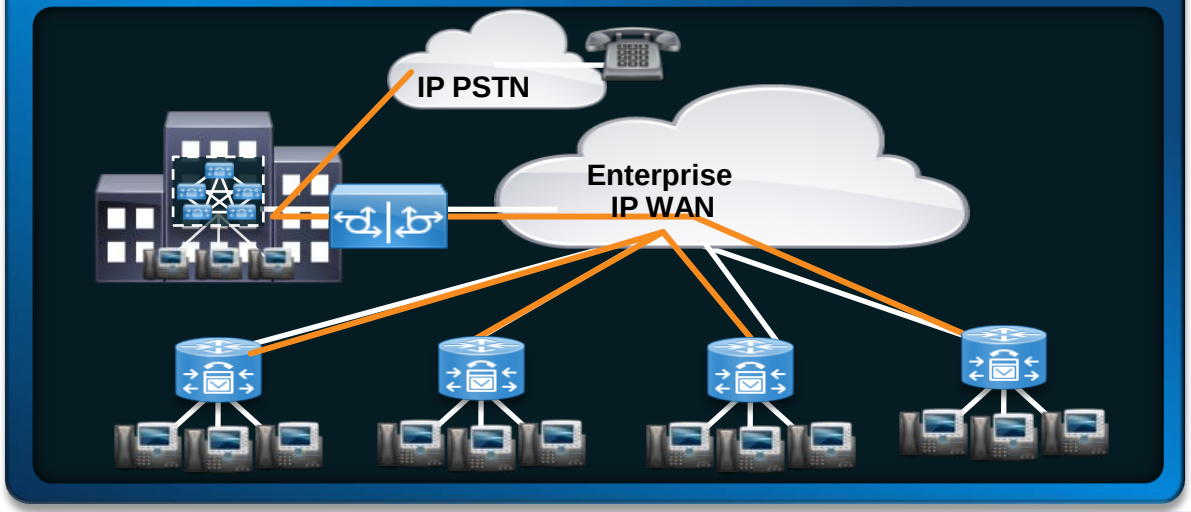
CUBE Scalability
Scalable Voice Trunk Capacity for Small to Large Businesses



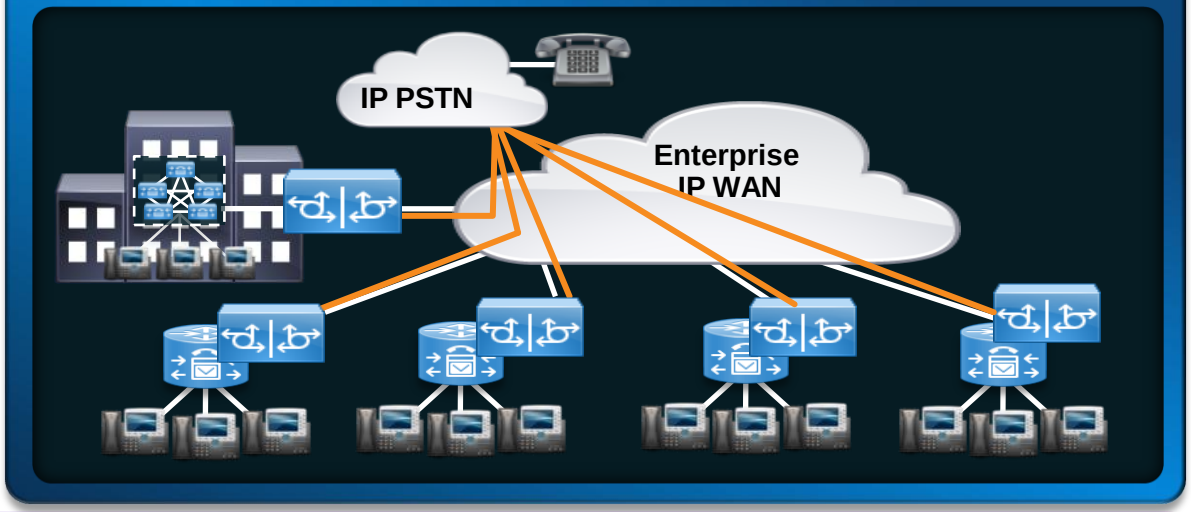
PSTN Access:

Flexible SIP Trunk Architectures supports varied Collaboration requirements

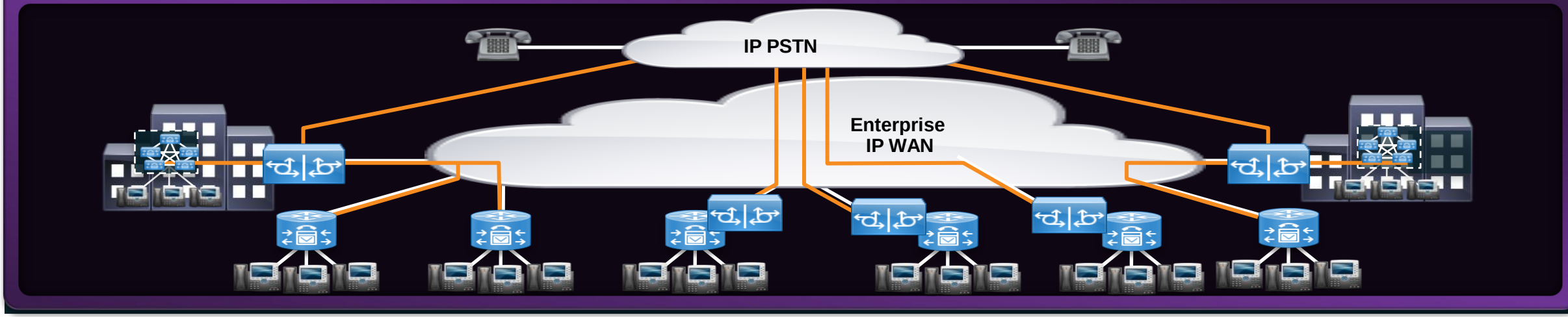
Centralized SIP Achitecture



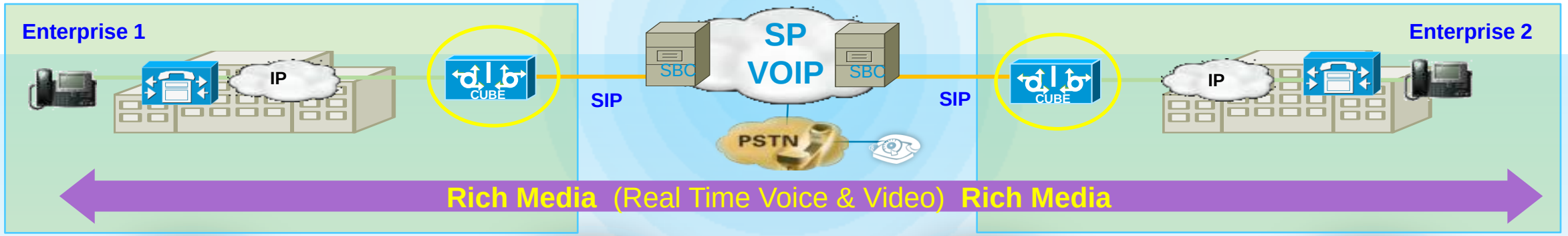
Distributed SIP Architecture



Hybrid SIP Architecture



CUBE
Enabling Session Border Control (SBC) on Cisco Routers



SESSION CONTROL

Call Admissions Control
VVQM w/ Medianet
Trunk Routing
Statistics and Billing
Redundancy/
Scalability

SECURITY

Encryption
Authentication
Registration
Rogue SIP Protection
VOICE POLICY
Firewall Placement
Toll Fraud

INTERWORKING

SIP - SIP
H.323 - SIP
SIP Normalization
DTMF Interworking
Transcoding
Codec Filtering

DEMARCATION

Fault Isolation
Topology Hiding
Network Borders
L5/L7 Protocol Demarcation

CUBE Enables Flexible Voice Policy Solutions
Ensures Productive Use of the Collaboration Voice and Video Network

Harassing / Threatening Callers

Lowers productivity & safety

Toll Fraud

Corporations lack real-time defense

Voice Service Abuse & Theft

Ensure employee use of voice network complies with business objectives

Contact Center Fraud / ID Theft

Legal risk and financial losses for corporations and customers

Capacity Monitoring

Enables better network planning and staffing requirements

Unauthorized Fax or Modem Usage

Most commonly found issue

Voice Policy Use Cases
ROI Opportunities in the Enterprise Voice Network

Enterprise Wide Capacity Management

- **Centralized reporting for the enterprise**
- Baseline and inventory voice network infrastructure
- Recover capacity lost to unauthorized traffic
- Right-size trunk infrastructure based on trunk utilization
- Identify and Eliminate unused PBX bypass lines
- Identify orphaned or unused extensions
- Consolidate/reduce unused fax resources
- Absence of call activity on trunking resources
- Excessive unanswered/busy calls on trunking resources
- Optimize staffing based on call activity reports

Enterprise Wide Control of Service Abuse

- **Centralized abuse prevention policy definition**
- Unauthorized Modem usage
- Voice Data Leakage Protection (DLP)
- Reduce toll fraud losses by blocking unauthorized calls
- 911 notification and response
- Managed calls to and from restricted numbers

Enterprise Wide Security Management

- **Centralized Security Policy Definition**
- TDOS (Telephony Denial of Service) Mitigation
- Eliminate Toll Fraud Losses from external dial through
- Prevent network penetration via blocking modems
- Alert and control business disrupting bomb threats
- Identify and Manage harassing calls.
- Alert/log maintenance port access, and block unauthorized connections
- Minimize Contact Center Service abuse or misuse
- Prevent identity theft on voice lines

Customer Service Monitoring

- Policy based recording to audit call agent performance
- Policy based recording of potential harassing calls

SLA Monitoring

- Log of service outages, disruptions, and errors
- Voice Usage uptime and performance reports

Voice Policy Use Cases
ROI Opportunities in the Enterprise Voice Network

Enterprise Wide Capacity Management

- **Centralized reporting for the enterprise**
- Baseline and inventory voice network infrastructure
- Recover capacity lost to unauthorized traffic
- Right-size trunk infrastructure based on trunk utilization
- Identify and Eliminate unused PBX bypass lines
- Identify orphaned or unused extensions
- Consolidate/reduce unused fax resources
- Absence of call activity on trunking resources
- Excessive unanswered/busy calls on trunking resources
- Optimize staffing based on call activity reports

Enterprise Wide Control of Service Abuse

- **Centralized abuse prevention policy definition**
- Unauthorized Modem / FAX usage
- Voice Data Leakage Protection (DLP)
- Reduce toll fraud losses by blocking unauthorized calls
- 911 notification and response
- Managed calls to and from restricted numbers

Enterprise Wide Security Management

- **Centralized Security Policy Definition**
- **TDOS (Telephony Denial of Service) Mitigation**
- Eliminate Toll Fraud Losses from external dial through
- Prevent network penetration via blocking modems
- **Alert and control business disrupting bomb threats**
- **Identify and Manage harassing calls**.
- Alert/log maintenance port access, and block unauthorized connections
- **Minimize Contact Center abuse or misuse**
- **Prevent identity theft on voice lines**

Customer Service Monitoring

- Policy based recording to audit call agent performance
- Policy based recording of potential harassing calls

SLA Monitoring

- Log of service outages, disruptions, and errors
- Voice Usage uptime and performance reports

TDoS Coverage Has Risen Dramatically in Past 2 Months

CSO

BUSINESS RISK LEADERSHIP

April 01, 2013 www.csoonline.com

NEWS

DHS, FBI warn over TDoS attacks on emergency centers

Telephony denial-of-service attacks on the rise against public and private organizations.

By Antone Gonsalves

KrebsonSecurity

In-depth security news and investigation

DHS Warns of 'TDos' Extortion Attacks on Public Emergency Networks

APRIL 1, 2013

As if emergency responders weren't already overloaded: Increasingly, extortionists are launching debilitating attacks designed to overwhelm the telephone networks of emergency communications centers and personnel, according to a confidential alert jointly issued by the **Department of Homeland Security** and the **FBI**.

The alert, a copy of which was obtained by KrebsOnSecurity, warns public safety answering points (PSAPs) and emergency communications centers and personnel about a recent spike in so-called "telephony denial-of-service" (TDoS) attacks:

"Information received from multiple jurisdictions indicates the possibility of attacks targeting the telephone systems of public sector entities. Dozens of such attacks have targeted the administrative PSAP lines (not the 911 emergency line). The perpetrators of the attack have launched high volume of calls against the target network, tying up the system from receiving legitimate calls. This type of attack is referred to as a TDoS or Telephony Denial of Service attack. These attacks are ongoing. Many similar attacks have occured targeting various businesses and public entities, including the financial sector and other public emergency operations interests, including air ambulance, ambulance and hospital communications."

According to the alert, these recent TDoS attacks are part of a bizarre extortion scheme that apparently starts with a phone call to an organization from an individual claiming to represent a collections company for payday loans. The caller usually has a strong accent of some sort and asks to speak with a current or former employee concerning an outstanding debt. Failing to get payment from an individual or organization, the perpetrator launches a TDoS attack. The organization will be inundated with a continuous stream of calls for an unspecified, but lengthy period of time.

DHS notes that the attacks can prevent both incoming and/or outgoing calls from being completed, and the alert speculates that government offices/emergency services are being "targeted" because of the necessity of functional phone lines. The alert says that the attacks usually follow a person with a heavy accent demanding payment of $5,000 from the company because of default by an employee who either no longer works at the PSAP or never did. The full alert is reposted here (PDF).

A much shorter version of this alert appeared in January 2013 on the Web site of the **Internet Crime Complaint Center** (IC3), which warned of another twist in these TDoS attacks: "The other tactic the subjects are now using in order to convince the victim that a warrant for their arrest exists is by spoofing a police department's telephone number when calling the victim. The subject claims there is a warrant issued for the victim's arrest for failure to pay off the loan. In order to have the police actually respond to the victim's residence, the subject places repeated, harassing calls to the local police department while spoofing the victim's telephone number."

Neither alert specifies how these call floods are being carried out, but KrebsOnSecurity has featured several stories about commercial services in the underground that can be hired to launch TDoS attacks.

Image: SecureLogix

According to a recent report from **SecureLogix**, a company that sells security services to call centers, free IP-PBX software such as Asterisk, as well as computer-based call generation tools and easy-to-access SIP services, are greatly lowering the barrier-to-entry for voice network attackers.

The company says TDoS attacks can be difficult to detect, because the attacker typically changes the caller ID on every call. From their report: "This makes it very difficult even for service providers to detect the attacks. Unless these attacks can be quickly traced back to an originating carrier that typically does not generate many calls to the contact center, they are very difficult to differentiate from legitimate calls. The attacks also typically move through multiple service providers, making them time consuming to trace back to the source."

SecureLogix said TDoS attacks can employ simple audio content, including white noise or silence (which could be dismissed as a technical problem), foreign language audio (representing a confused user), or repeated DTMF patterns.

"These are simple techniques, with future attacks likely using other types of mutating audio. In the future, these attacks will be much more severe. By simply generating more calls or using more entry points to the [target] network, many more calls can be generated, resulting in a very expensive attack or one which degrades the performance of a contact center, rendering access unavailable to legitimate callers and potentially impairing brand image."

SecureLogix "We see your voice"

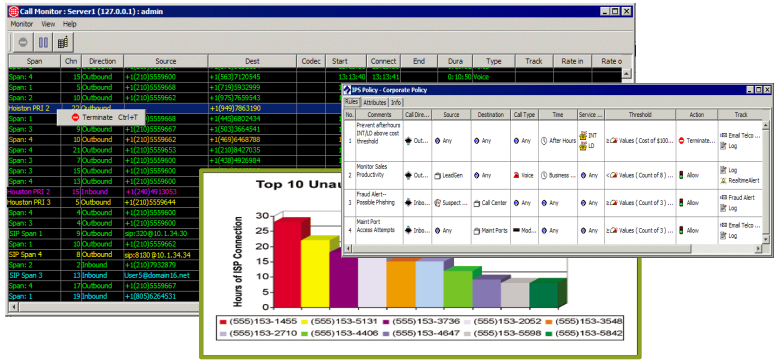
courtesy of krebsonsecurity.com

2013 coverage in over 50+ print/online publications including:

- Krebs on Security
- CSO Magazine
- Network World
- InfoWorld
- Security Week
- Infosecurity Magazine
- InfoWorld
- CFO World
- eWeek
- Government Computer News
- GovInfoSecurity
- TechEye
- InfoTech
- SC Magazine, etc..

Integrated Voice Gateway / Voice Policy Solution

Cisco & SecureLogix



UC Application

Unified Voice Policy Control

Network

TDM Gateway

CUBE

Platform

Cisco ISR / ASR

SecureLogix
Application Layer Voice Policy:

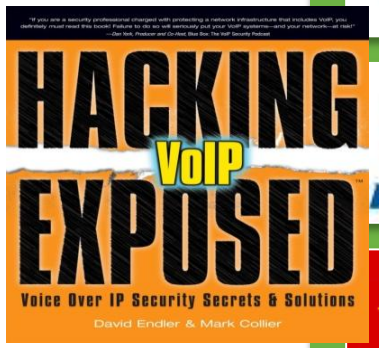
- Centralized policy creation/distribution
- Protection from external harassing calls
- Service Abuse Control by Internal Users
- Enterprise-wide UC reporting & analytics
- Compliance & Data Leakage prevention
- Call recording archive

Cisco
Voice Service Infrastructure:

- Internetworking
- Transcoding & Transrating
- Protocol fixes and interoperability
- Packet level encryption security
- NAT and topology protection
- IP Firewall
- QoS

About SecureLogix

- Voice/UC Security & Intelligence Leader
  - 17 patents granted
  - Authored ***State of Voice Security*** report
  - Authored ***Hacking Exposed: VoIP and UC***
  - Publishes www.voipsecurityblog.com
- Strong Cisco partner
  - CDN - Preferred Solution Developer
  - Solution Incentive Plus
- Trusted voice security expert
  - For U.S. government and military
  - For largest U.S. companies
- Global Distribution Alliance via Comstor



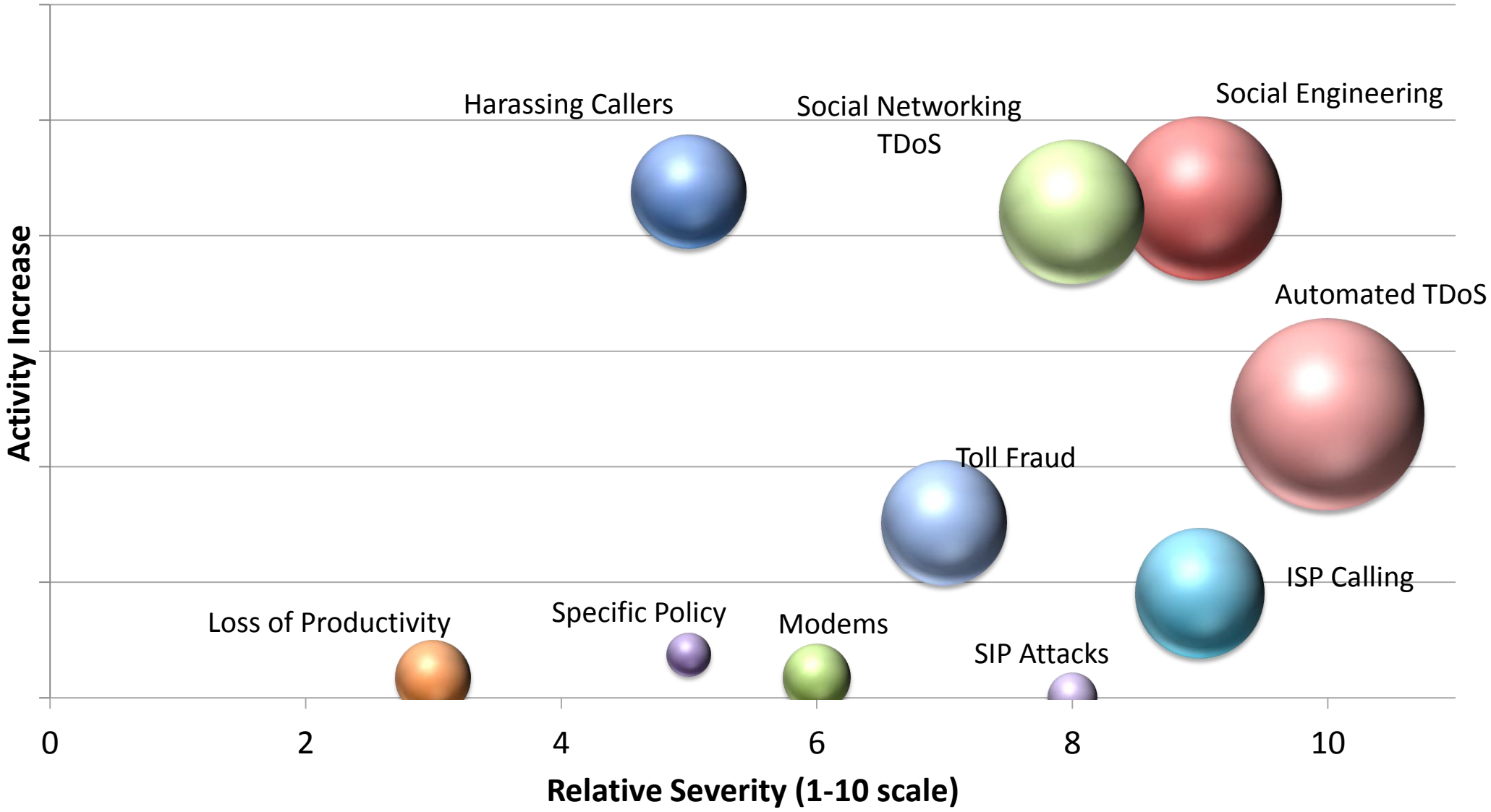
SecureLogix Unified Communications Policy and Security

Mark Collier
Chief Technology Officer and VP Engineering, SecureLogix
Rod Wallace
Global VP Services, SecureLogix

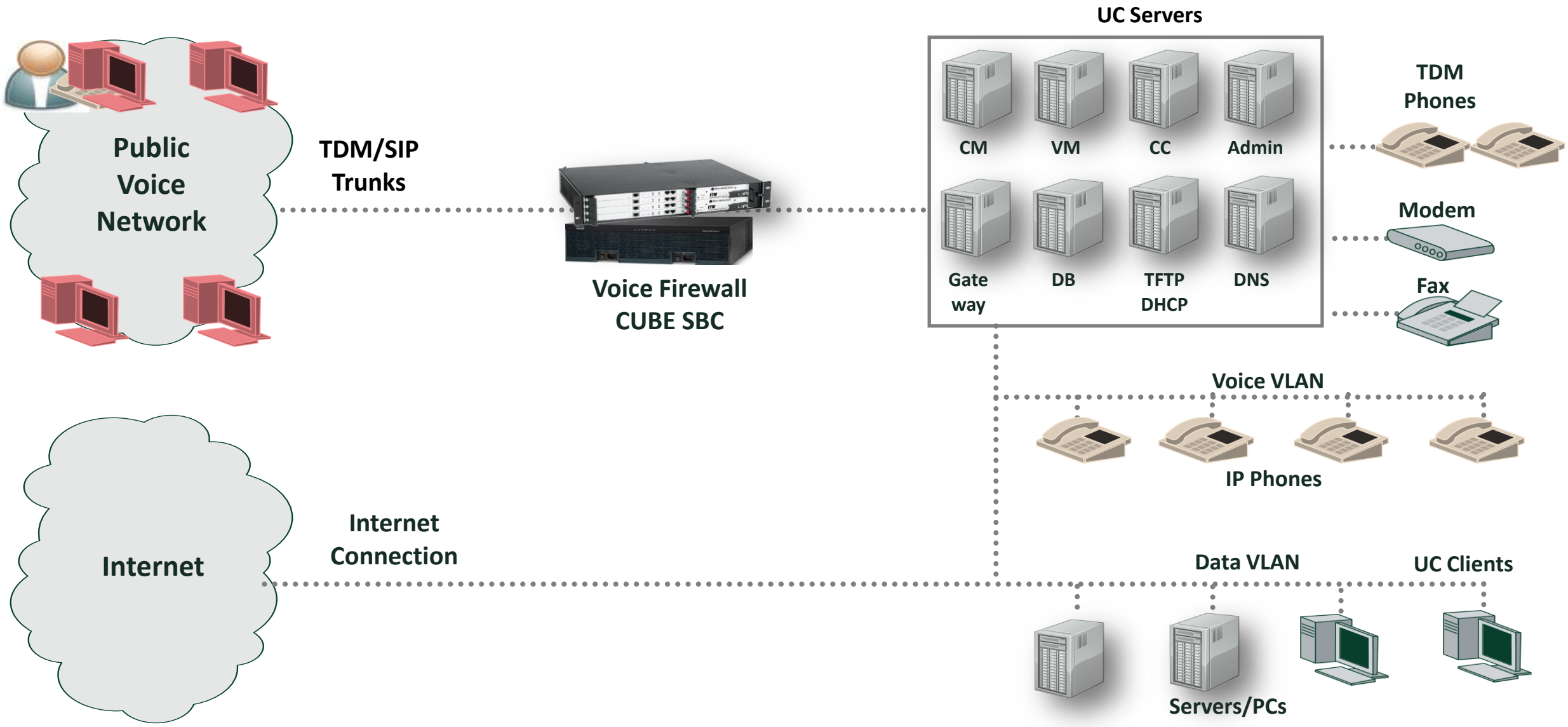
State of Security Report – Voice and Unified Communications

http://www.securelogix.com/sos/

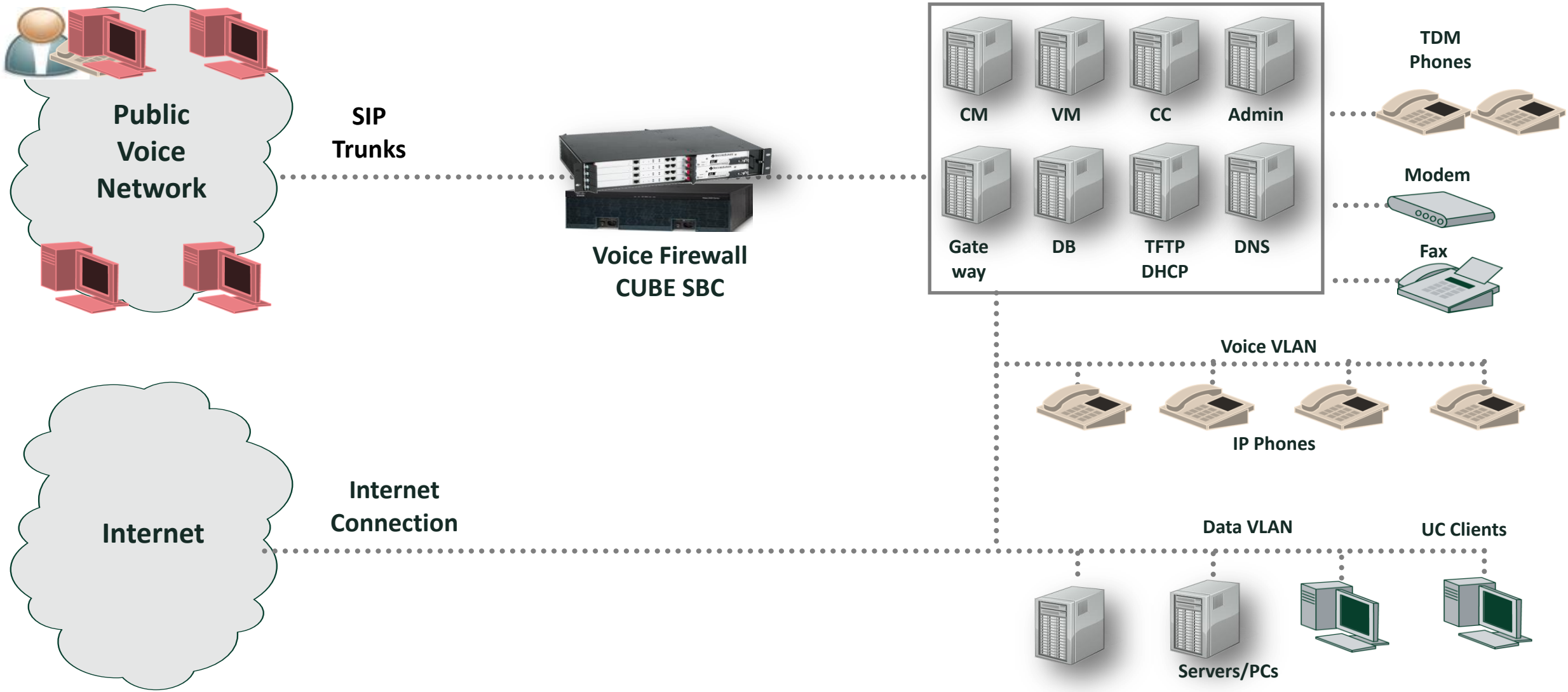
UC Threats Overview



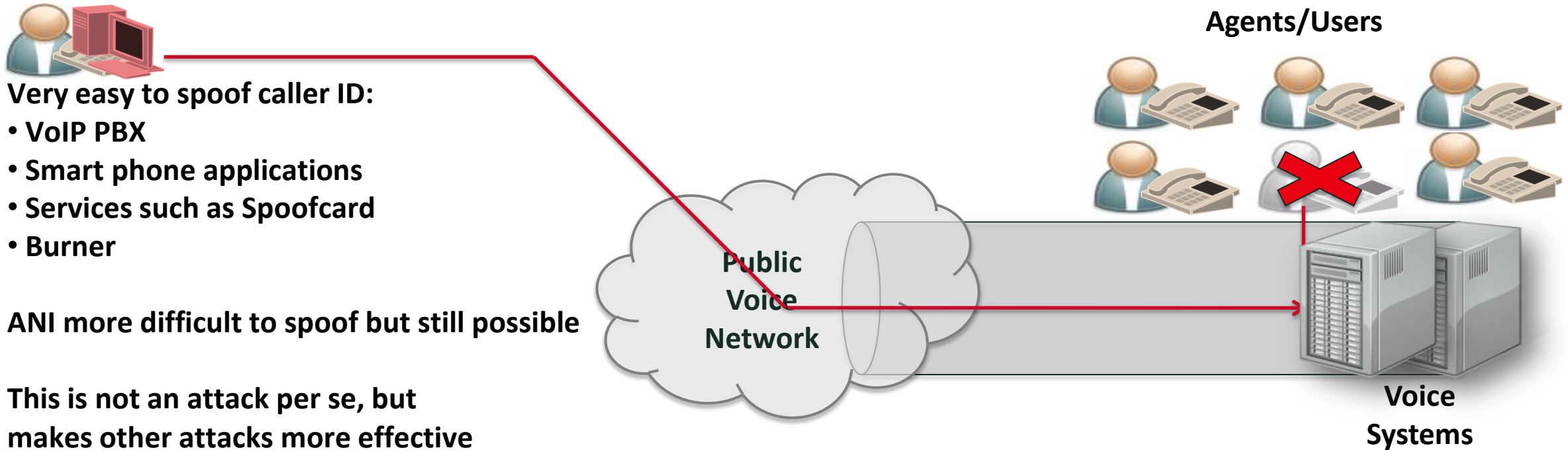
The Public Voice Network Has Become Very Hostile



SIP Trunk Security



Calling Number Spoofing



Very easy to spoof caller ID:

- **VoIP PBX**
- **Smart phone applications**
- **Services such as Spoofcard**
- **Burner**

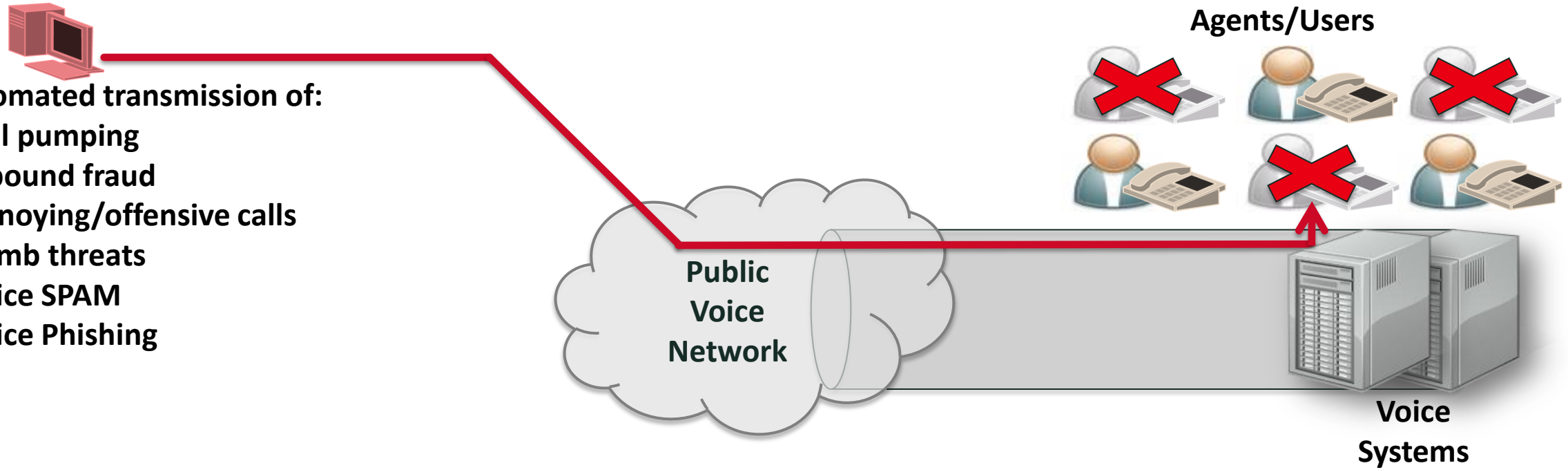
ANI more difficult to spoof but still possible

This is not an attack per se, but makes other attacks more effective

Harassing Calls

Automated transmission of:

- Call pumping
- Inbound fraud
- Annoying/offensive calls
- Bomb threats
- Voice SPAM
- Voice Phishing



Telephony Denial of Service (TDoS) Overview

- What is TDoS:
  - Flood of unwanted calls received by an enterprise, often in a contact center
  - Disrupt operations by consuming system bandwidth, crowds out legitimate calls
  - First identified by FBI in May 2010. Increase of attacks against enterprises, contact centers, PSAP (911) centers
- How TDoS Happens:
  - Occurs on SIP, UC, or TDM networks due to malicious calls – not necessarily malicious packets
  - Inexpensive or free SIP access, free and powerful PBX software such as Asterisk and call generators have made TDoS generation much easier
  - A serious issue due to the increased hostility of the public voice network
  - Attacks can occur through misuse of social networking sites such as facebook and twitter
  - Related attacks such as harassing calls, call pumping, and toll fraud can also create TDoS conditions

Original 2010 TDoS Public Warning

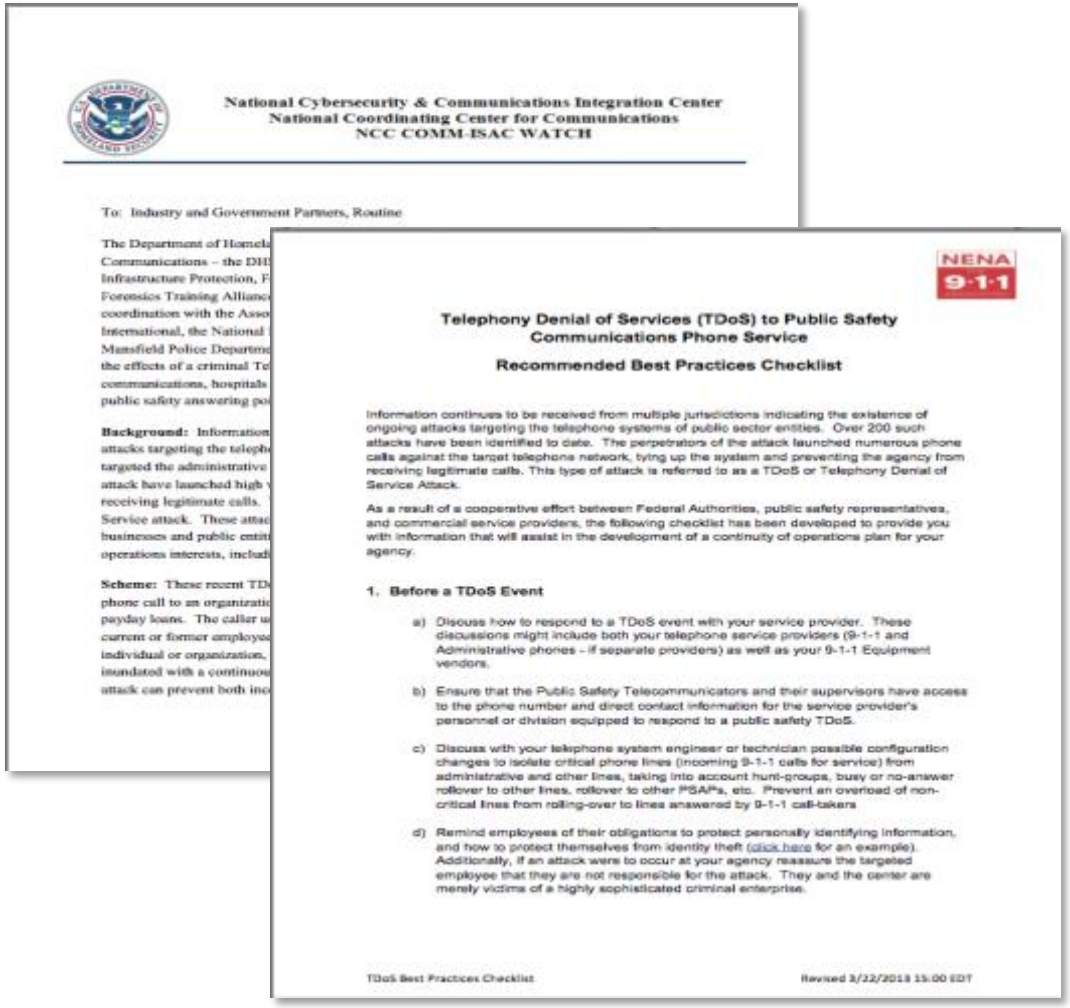
Phony Phone Calls Distract Consumers from Genuine Theft

FBI and Partners Warn Public

May 11, 2010

The FBI is warning consumers today about a new scheme that uses telephony denial-of-service attacks as a diversion to what is really happening: the looting of bank and online trading accounts.

2013 Surge of TDoS Attacks – Contact Centers & PSAPs



National Cybersecurity & Communications Integration Center
National Coordinating Center for Communications
NCC COMM-ISAC WATCH

To: Industry and Government Partners, Routine

NENA 9-1-1

Telephony Denial of Services (TDoS) to Public Safety Communications Phone Service

Recommended Best Practices Checklist

Information continues to be received from multiple jurisdictions indicating the existence of ongoing attacks targeting the telephone systems of public sector entities. Over 200 such attacks have been identified to date. The perpetrators of the attack launched numerous phone calls against the target telephone network, tying up the system and preventing the agency from receiving legitimate calls. This type of attack is referred to as a TDoS or Telephony Denial of Service Attack.

As a result of a cooperative effort between Federal Authorities, public safety representatives, and commercial service providers, the following checklist has been developed to provide you with information that will assist in the development of a continuity of operations plan for your agency.

1. **Before a TDoS Event**

a) Discuss how to respond to a TDoS event with your service provider. These discussions might include both your telephone service providers (9-1-1 and Administrative phones - if separate providers) as well as your 9-1-1 Equipment vendors.

b) Ensure that the Public Safety Telecommunicators and their supervisors have access to the phone number and direct contact information for the service provider's personnel or division equipped to respond to a public safety TDoS.

c) Discuss with your telephone system engineer or technician possible configuration changes to isolate critical phone lines (incoming 9-1-1 calls for service) from administrative and other lines, taking into account hunt-groups, busy or no-answer rollover to other lines, rollover to other PSAPs, etc. Prevent an overload of non-critical lines from rolling-over to lines answered by 9-1-1 call-takers

d) Remind employees of their obligations to protect personally identifying information, and how to protect themselves from identity theft (click here for an example). Additionally, if an attack were to occur at your agency reassure the targeted employee that they are not responsible for the attack. They and the center are merely victims of a highly sophisticated criminal enterprise.

TDoS Best Practices Checklist — Revised 3/22/2013 15:00 EDT

2013 Public TDoS Attack Warnings Issued by:

- **FBI –** Federal Bureau of Investigations
- **DHS –** Department of Homeland Security
- **NENA 911 –** National Emergency Number Assoc.
- **APCO International –** Assoc. of Public-Safety Communications Officials
- Several U.S. state agencies

> Dozens of TDoS attacks have targeted administrative PSAP lines. The perpetrators have launched high volumes of calls against the target network, tying up the system from receiving legitimate calls.

TDoS Media Coverage Over Past 2 Months

CSO

BUSINESS RISK LEADERSHIP

April 01, 2013 www.csoonline.com

NEWS

DHS, FBI warn over TDoS attacks on emergency centers

Telephony denial-of-service attacks on the rise against public and private organizations.

By Antone Gonsalves

KrebsonSecurity

In-depth security news and investigation

DHS Warns of 'TDos' Extortion Attacks on Public Emergency Networks

APRIL 1, 2013

As if emergency responders weren't already overloaded: Increasingly, extortionists are launching debilitating attacks designed to overwhelm the telephone networks of emergency communications centers and personnel, according to a confidential alert jointly issued by the **Department of Homeland Security** and the **FBI**.

The alert, a copy of which was obtained by KrebsOnSecurity, warns public safety answering points (PSAPs) and emergency communications centers and personnel about a recent spike in so-called "telephony denial-of-service" (**TDoS**) attacks:

"Information received from multiple jurisdictions indicates the possibility of attacks targeting the telephone systems of public sector entities. Dozens of such attacks have targeted the administrative PSAP lines (not the 911 emergency line). The perpetrators of the attack have launched high volume of calls against the target network, tying up the system from receiving legitimate calls. This type of attack is referred to as a TDoS or Telephony Denial of Service attack. These attacks are ongoing. Many similar attacks have occured targeting various businesses and public entities, including the financial sector and other public emergency operations interests, including air ambulance, ambulance and hospital communications."

According to the alert, these recent TDoS attacks are part of a bizarre extortion scheme that apparently starts with a phone call to an organization from an individual claiming to represent a collections company for payday loans. The caller usually has a strong accent of some sort and asks to speak with a current or former employee concerning an outstanding debt. Failing to get payment from an individual or organization, the perpetrator launches a TDoS attack. The organization will be inundated with a continuous stream of calls for an unspecified, but lengthy period of time.

DHS notes that the attacks can prevent both incoming and/or outgoing calls from being completed, and the alert speculates that government offices/emergency services are being "targeted" because of the necessity of functional phone lines. The alert says that the attacks usually follow a person with a heavy accent demanding payment of $5,000 from the company because of default by an employee who either no longer works at the PSAP or never did. The full alert is reposted here (PDF).

A much shorter version of this alert appeared in January 2013 on the Web site of the **Internet Crime Complaint Center** (IC3), which warned of another twist in these TDoS attacks: "The other tactic the subjects are now using in order to convince the victim that a warrant for their arrest exists is by spoofing a police department's telephone number when calling the victim. The subject claims there is a warrant issued for the victim's arrest for failure to pay off the loan. In order to have the police actually respond to the victim's residence, the subject places repeated, harassing calls to the local police department while spoofing the victim's telephone number."

Neither alert specifies how these call floods are being carried out, but KrebsOnSecurity has featured several stories about commercial services in the underground that can be hired to launch TDoS attacks.

Image: SecureLogix

According to a recent report from **SecureLogix**, a company that sells security services to call centers, free IP-PBX software such as Asterisk, as well as computer-based call generation tools and easy-to-access SIP services, are greatly lowering the barrier-to-entry for voice network attackers.

The company says TDoS attacks can be difficult to detect, because the attacker typically changes the caller ID on every call. From their report: "This makes it very difficult even for service providers to detect the attacks. Unless these attacks can be quickly traced back to an originating carrier that typically does not generate many calls to the contact center, they are very difficult to differentiate from legitimate calls. The attacks also typically move through multiple service providers, making them time consuming to trace back to the source."

SecureLogix said TDoS attacks can employ simple audio content, including white noise or silence (which could be dismissed as a technical problem), foreign language audio (representing a confused user), or repeated DTMF patterns.

"These are simple techniques, with future attacks likely using other types of mutating audio. In the future, these attacks will be much more severe. By simply generating more calls or using more entry points to the [target] network, many more calls can be generated, resulting in a very expensive attack or one which degrades the performance of a contact center, rendering access unavailable to legitimate callers and potentially impairing brand image."

SecureLogix "We see your voice"

courtesy of krebsonsecurity.com

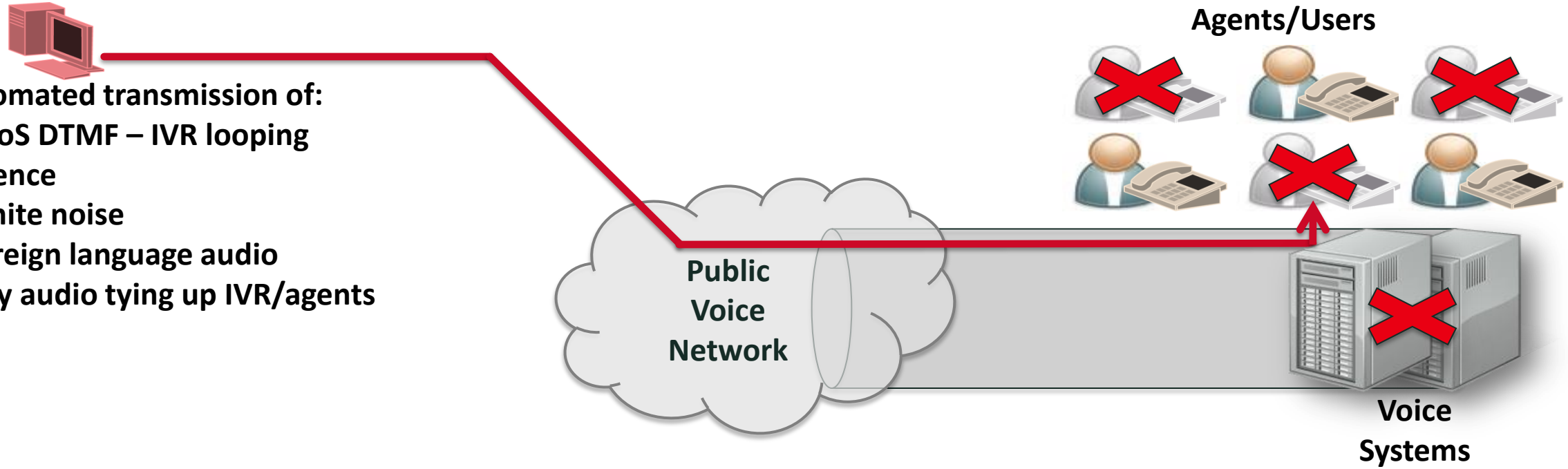
2013 coverage in over 50+ print/online publications including:

- Krebs on Security
- CSO Magazine
- Network World
- InfoWorld
- Security Week
- Infosecurity Magazine
- InfoWorld
- CFO World
- eWeek
- Government Computer News
- GovInfoSecurity
- TechEye
- InfoTech
- SC Magazine, etc..

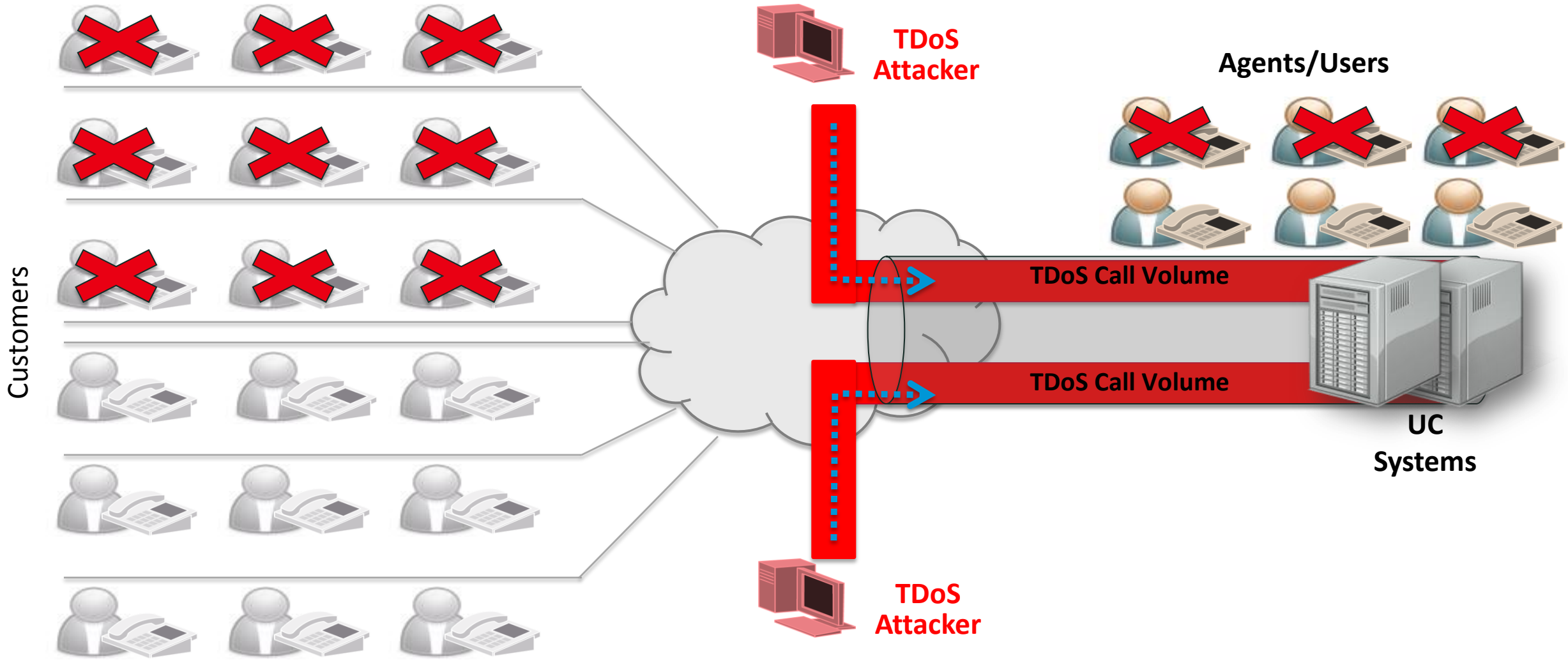
Automated TDoS

Automated transmission of:

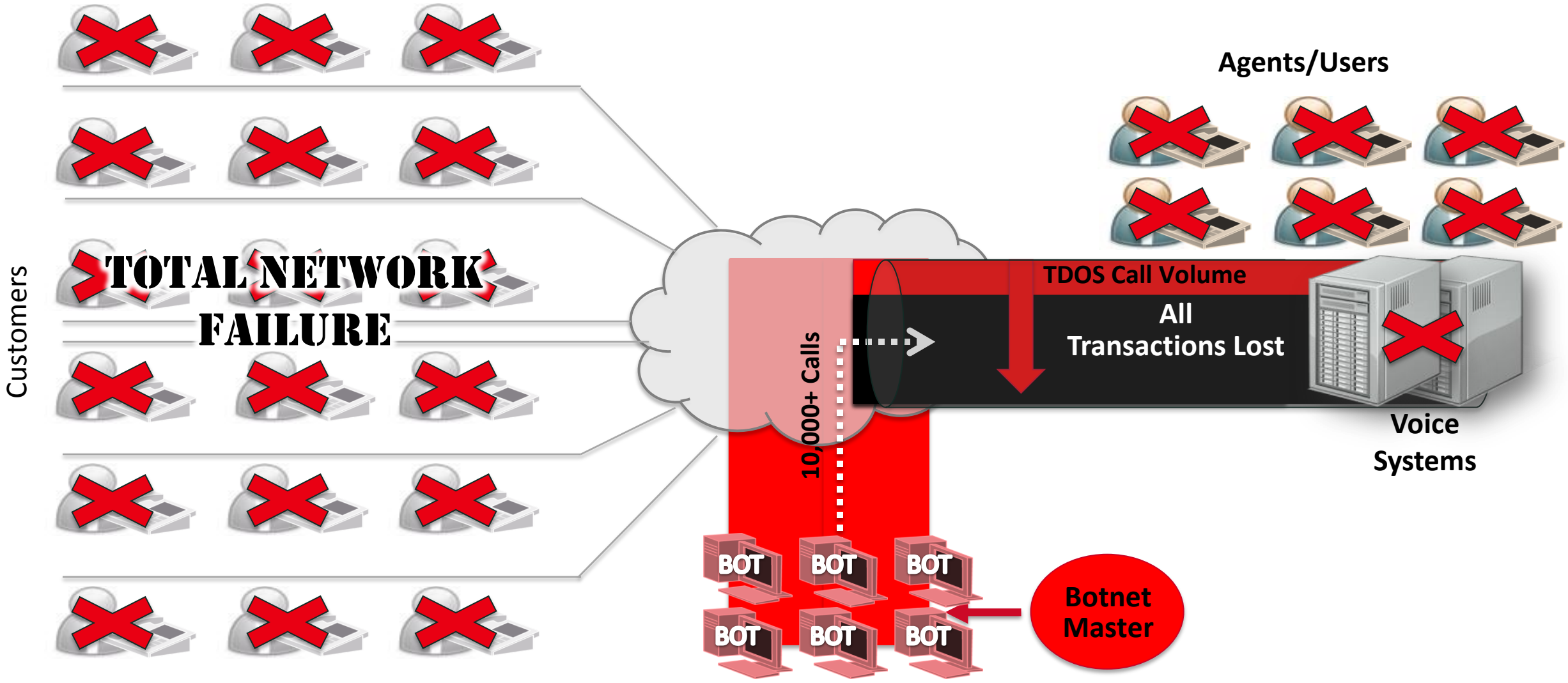
- **TDoS DTMF – IVR looping**
- **Silence**
- **White noise**
- **Foreign language audio**
- **Any audio tying up IVR/agents**



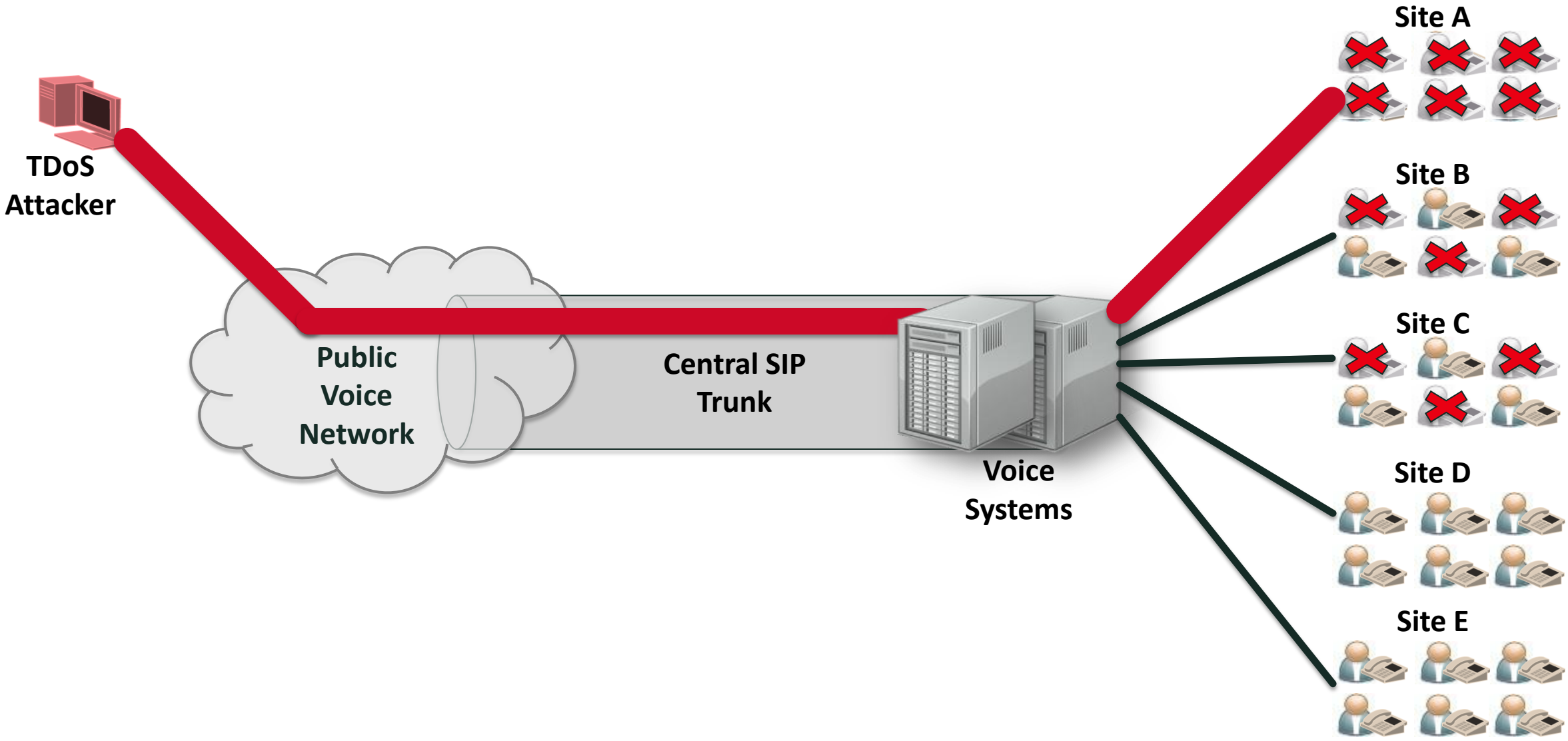
Automated TDoS



Automated Distributed TDoS

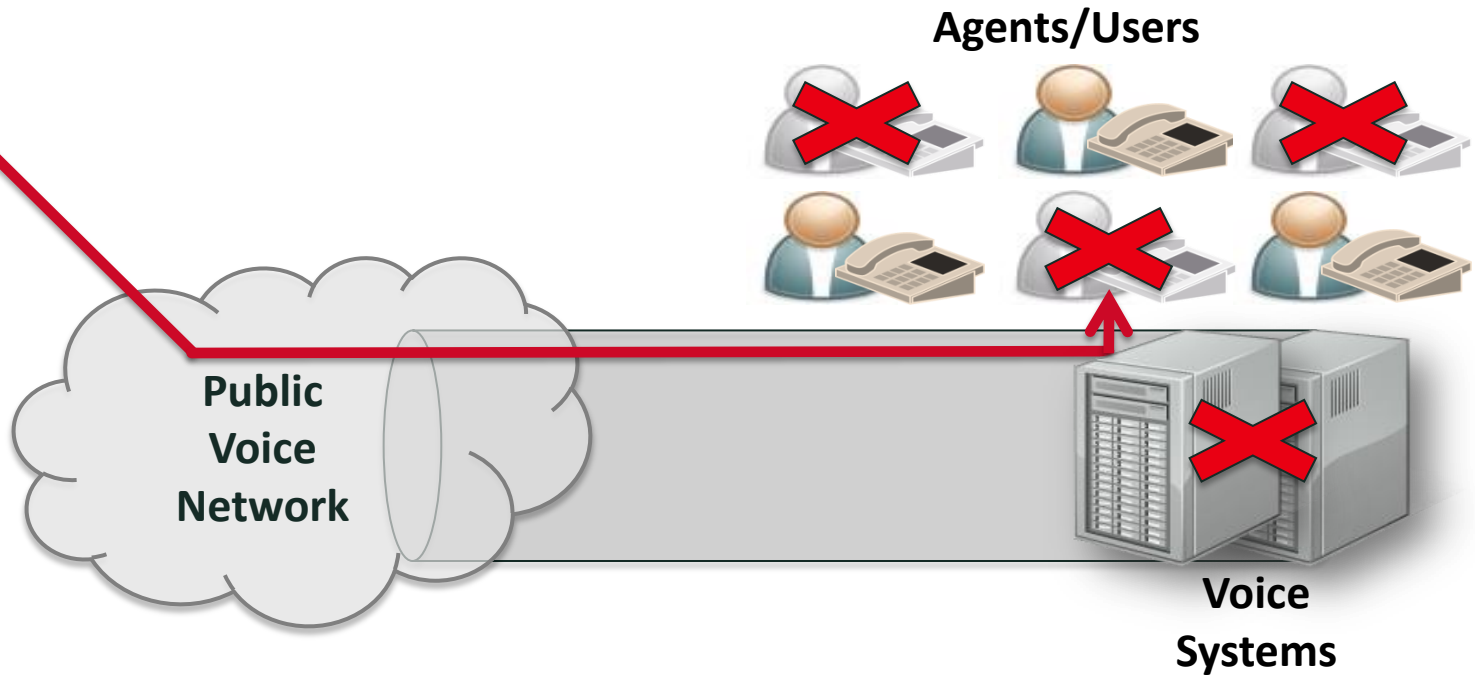


Central SIP Trunk TDoS

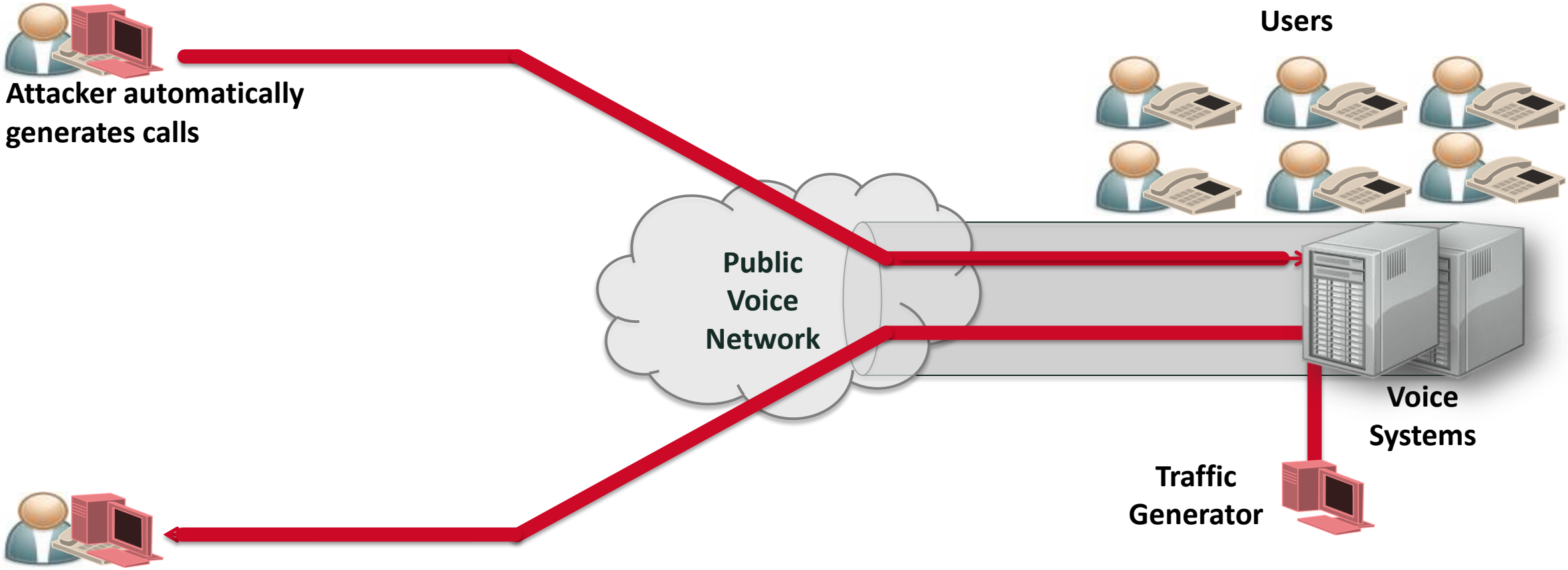


Social Networking TDoS

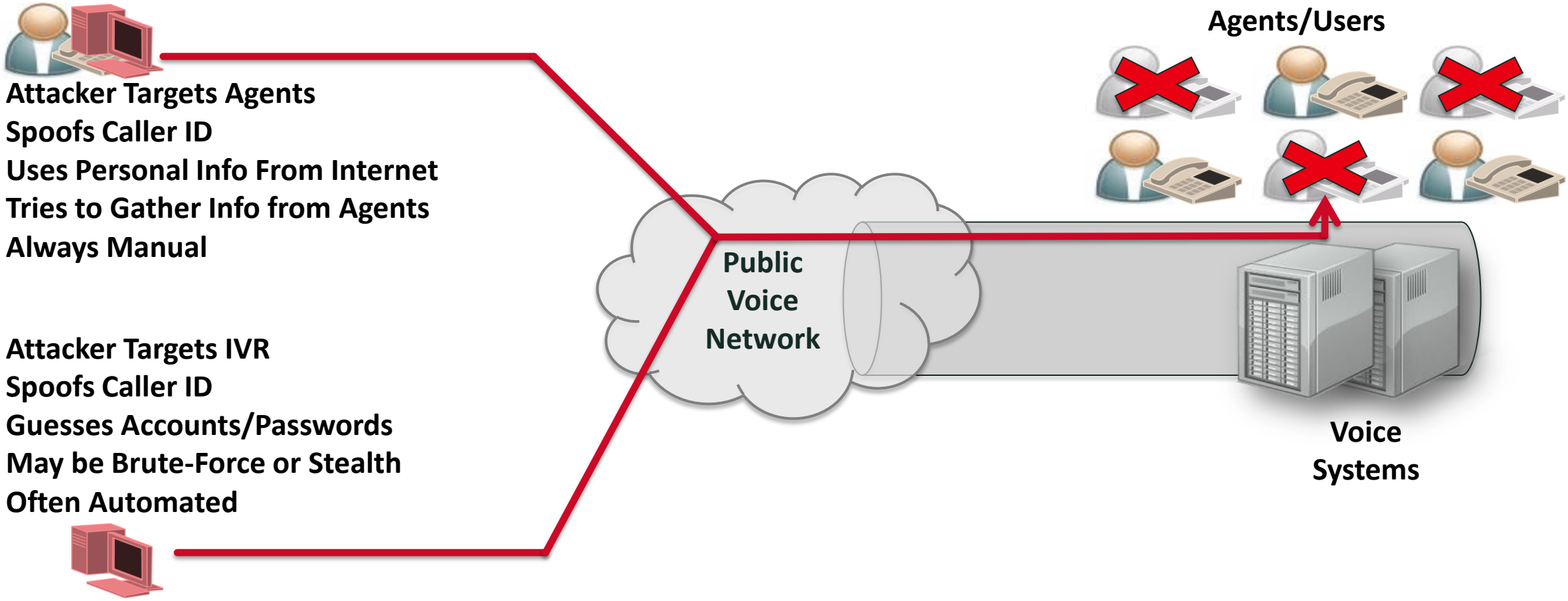
Social networking and many participants used to organize an attack



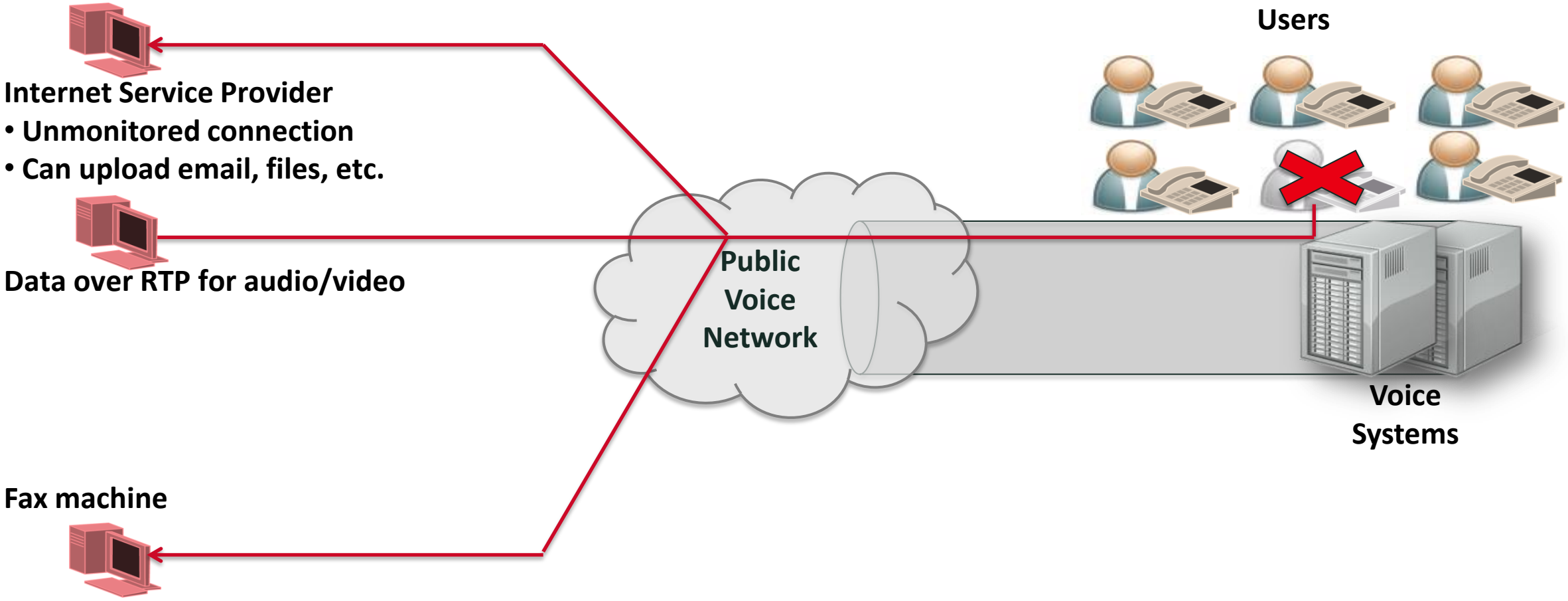
Dial-Through Fraud



Social Engineering

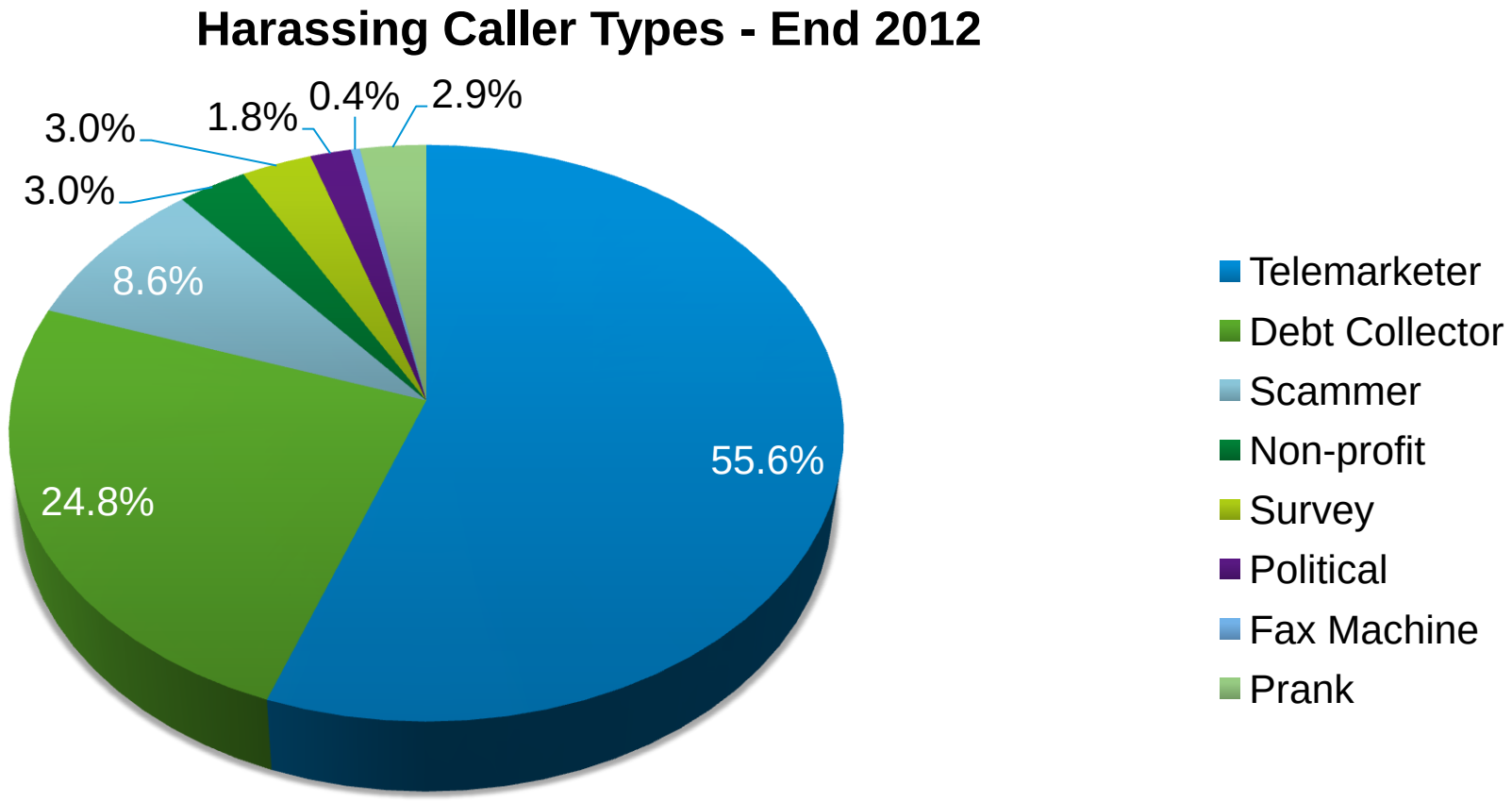


Data Leakage



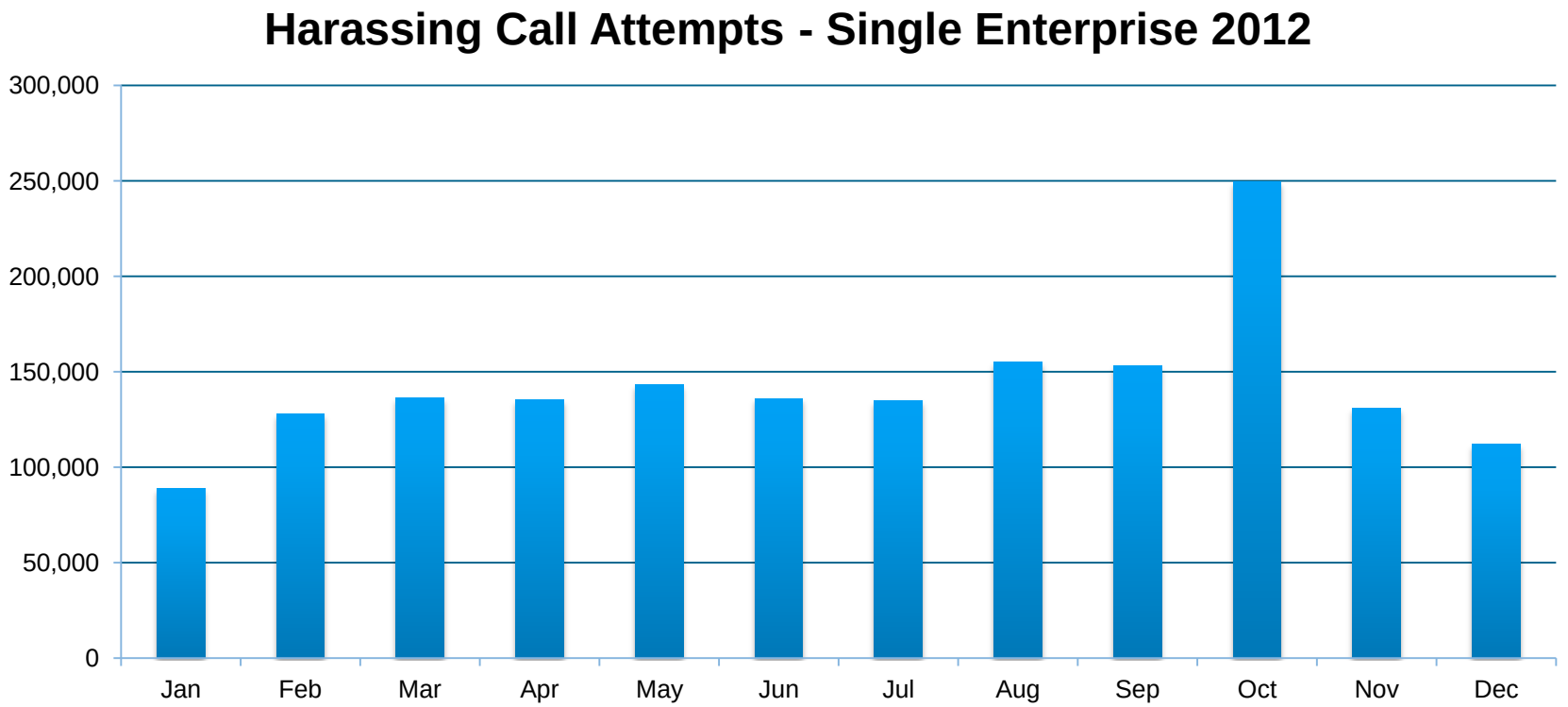
Unified Communications and Voice Attack Examples and Real-World Data

Harassing Caller Database – Massive Growth



100x growth in SecureLogix database over last 2 years
Over 6 million records used to create our blocking list

Example Harassing Caller Attempts

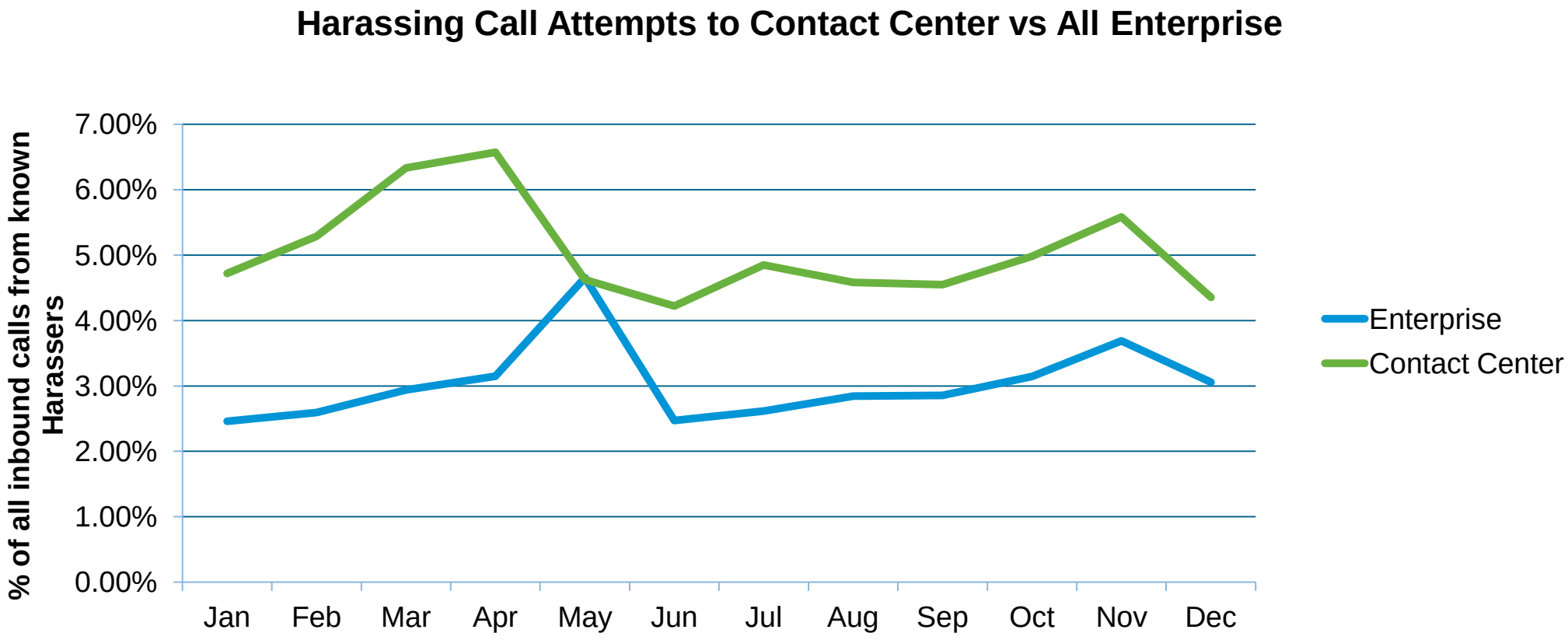


Average 4.17% of inbound calls have a match to our harassing caller DB

4.18x increase 2012 vs 2011

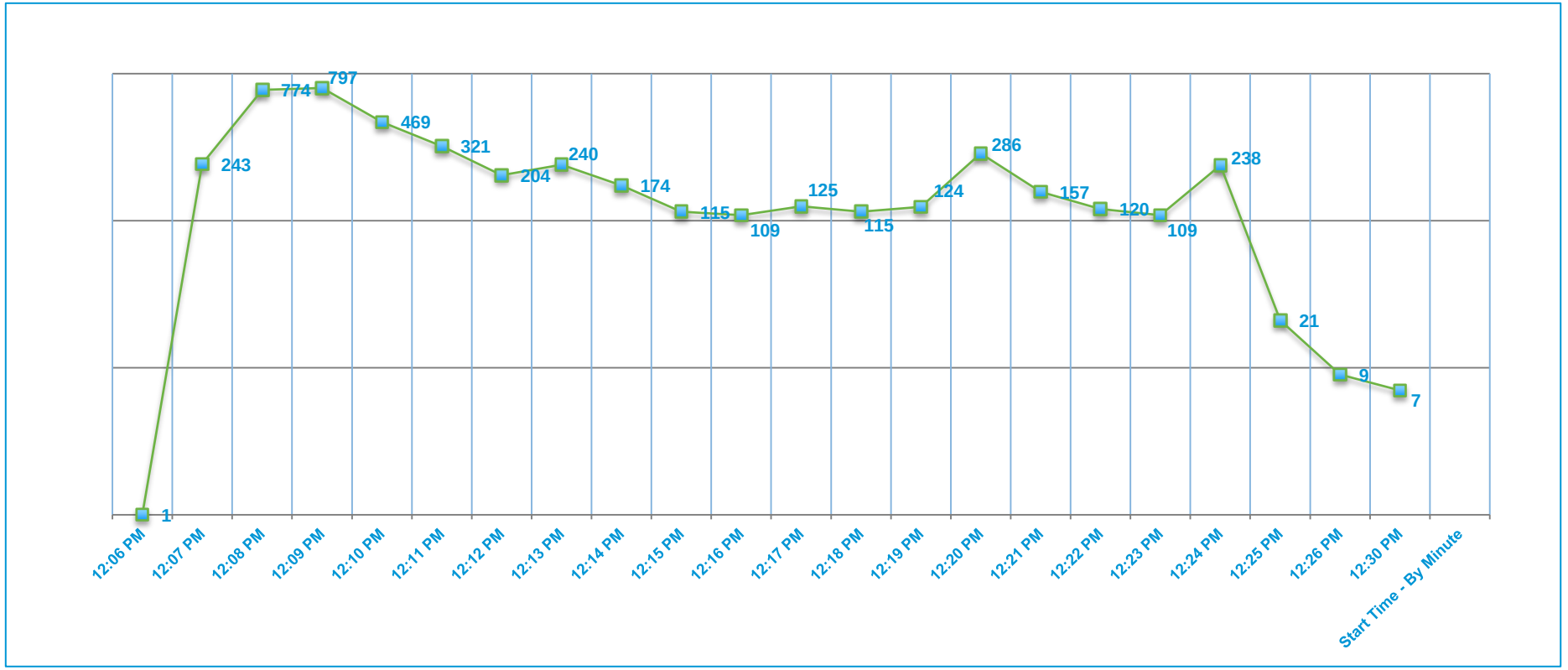
Like anti-virus, it is important to keep a current harassing caller list.

Contact Centers are a Target



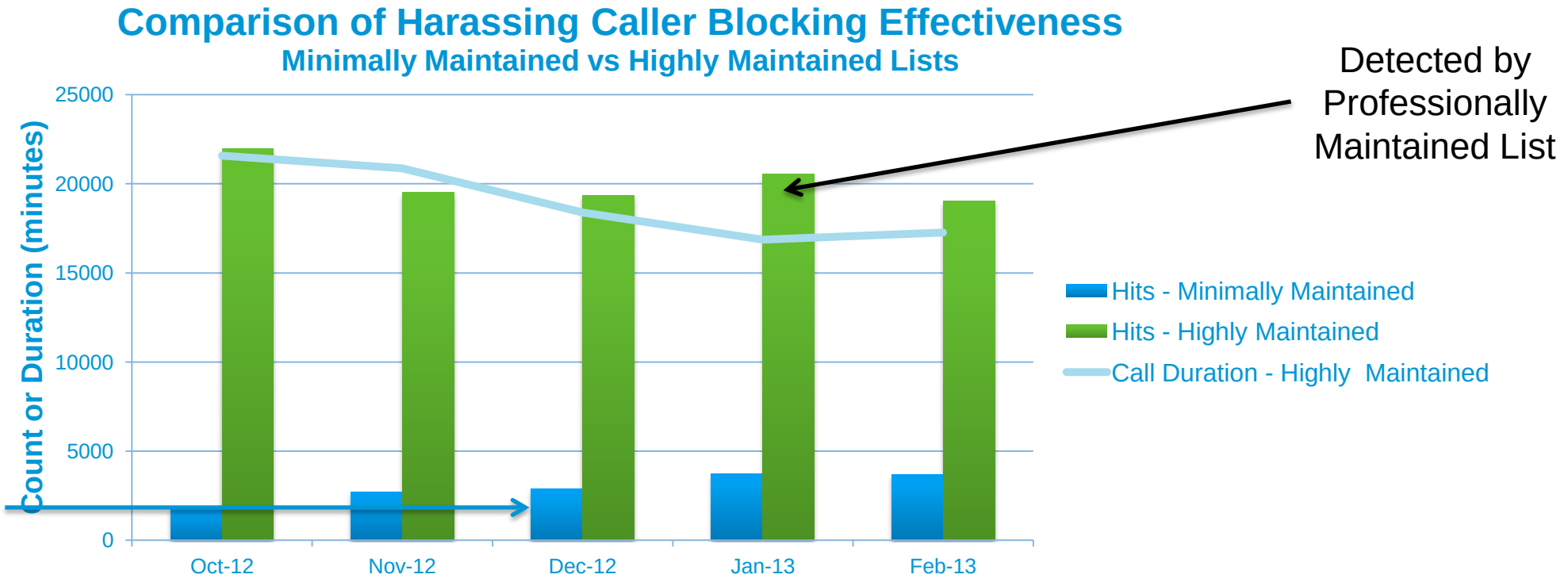
This contact center had an IVR!
5.52% on average harassing callers vs
4.17% for overall enterprise

High Volume Calling Campaigns More Common



Approx. 4800 calls in 25 minutes

Effect of Harassing Caller List Maintenance



Best-effort list detected 14,920 harassing calls.

Professional list detected >100,000 MORE harassing calls

The 100,000 extra calls consumed 95,000 minutes of employee time.

High Risk Calls and Social Engineering

- US sanctions stemming from engaging in financial transactions with OFAC countries/entities.
- Other high risk origin & destination countries: Common fraud launching points
- SecureLogix ETM alerts on OFAC calls, records calls, alert on social engineering attempts

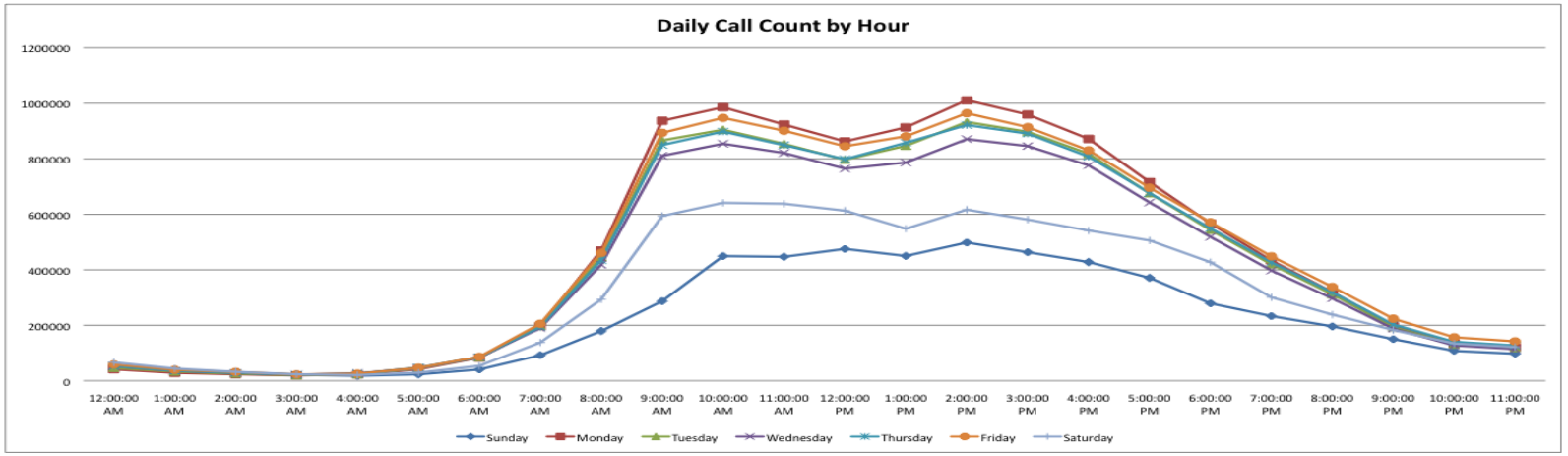
- Case Study - US Financial Institution:

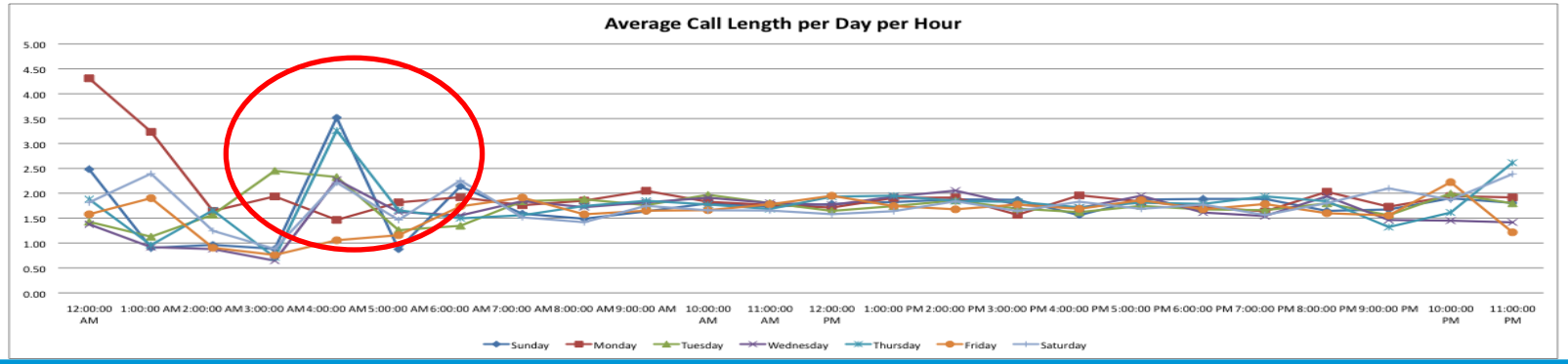
  In 2 weeks, 88 calls to OFAC countries for 5 hours
- Case Study - US Financial Institution:

  NSF check fraud perpetrated from Ghana in combination with US players.
- Case Study – US Financial Institution

  Detected multiple calls to Contact Center using Social Engineering to perform organizational mapping: requesting locations and phone numbers etc.

Call Metrics, Statistics & Exception Notification

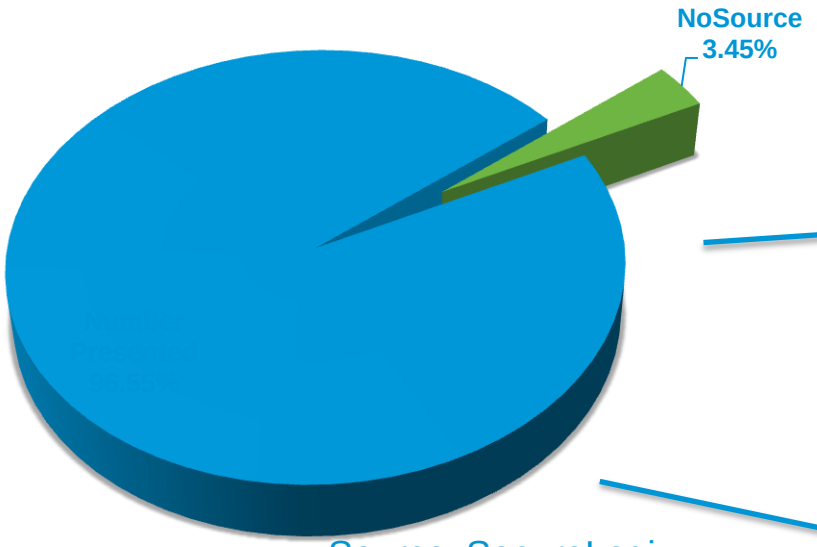




35% of all credit cards scams involve a social engineering call to a bank Contact Center.

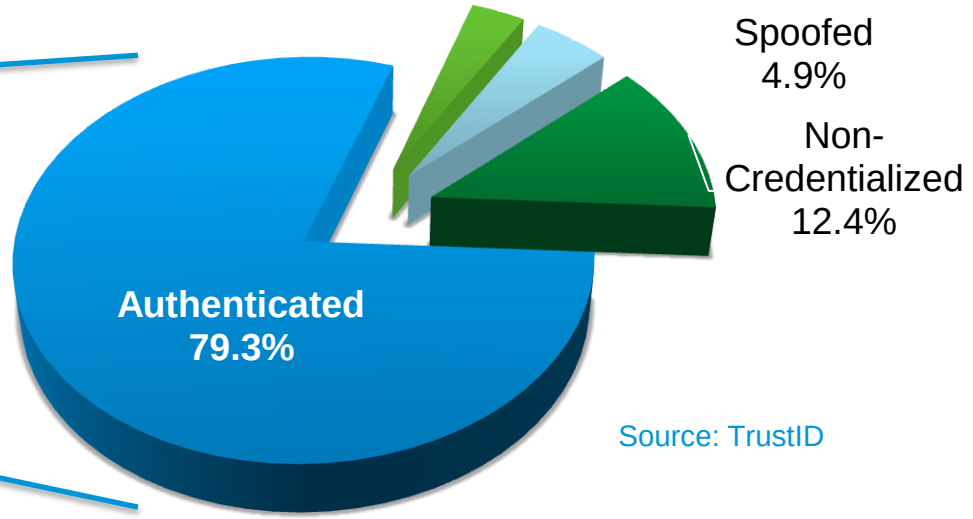
Social Engineering – Quantifying the Risk

Proportion of Calls with No Caller ID



Source: SecureLogix

Caller Authentication

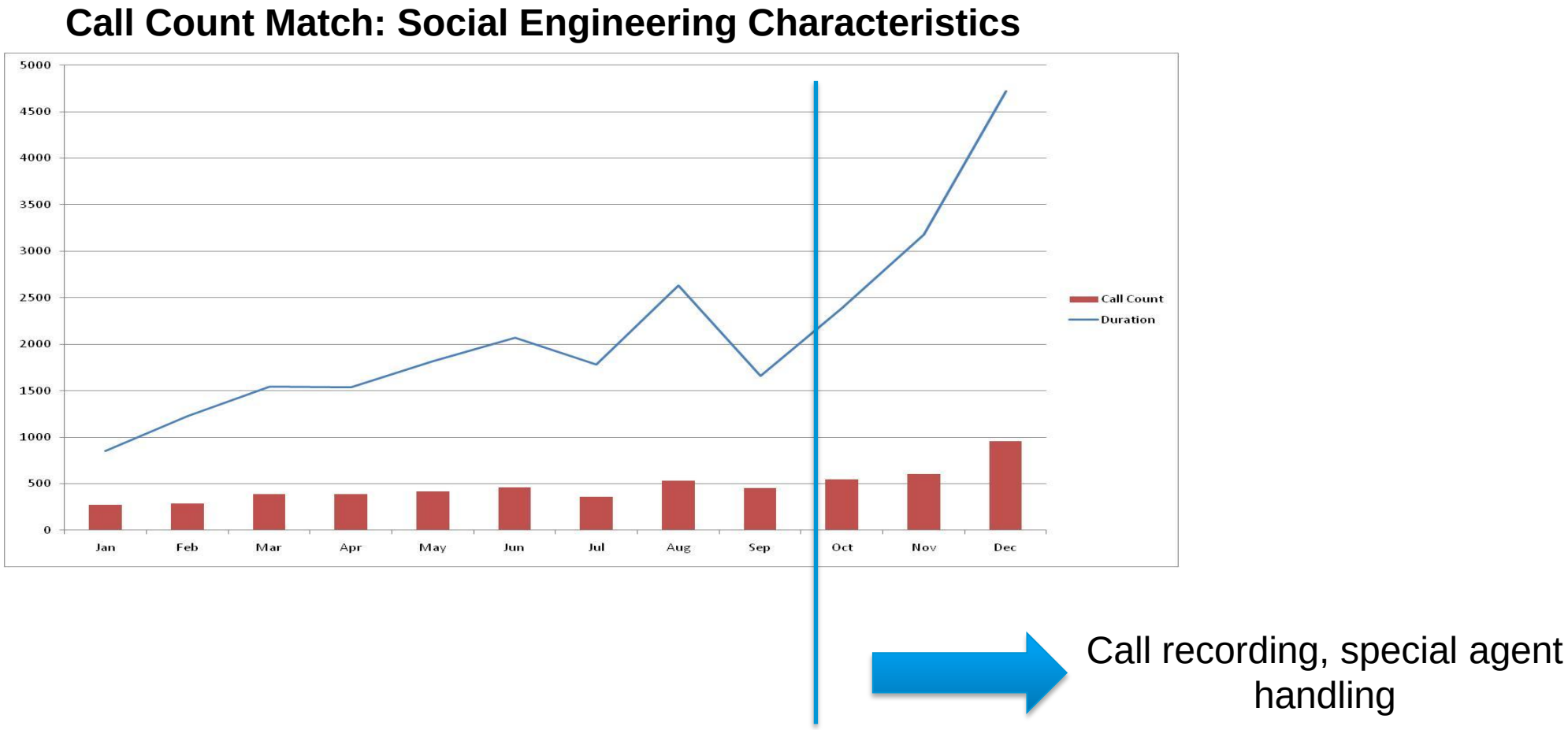


Source: TrustID

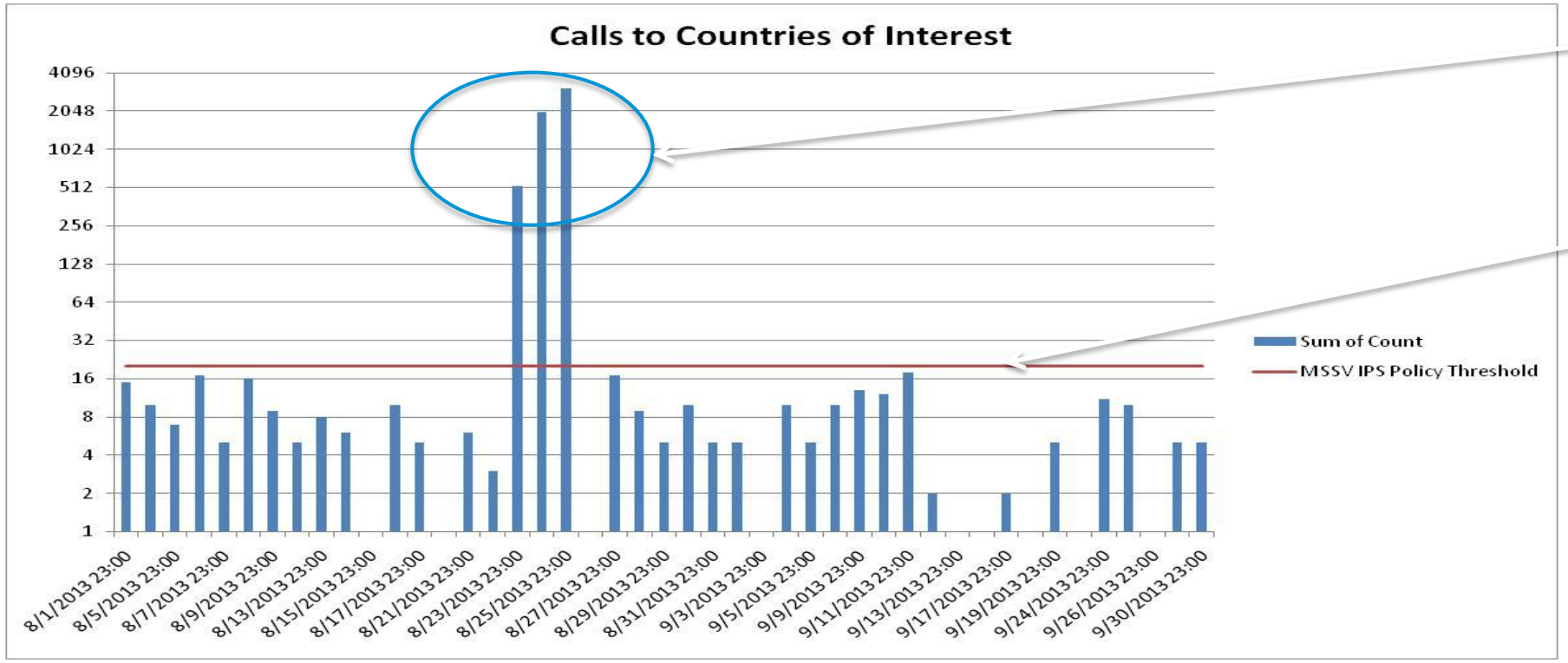
1.5% – 7% inbound calls have no source number

5% of remaining calls verifiably spoofed

Detecting Social Engineering in Contact Centers



Blocking Blacklist/Graylist International Calls



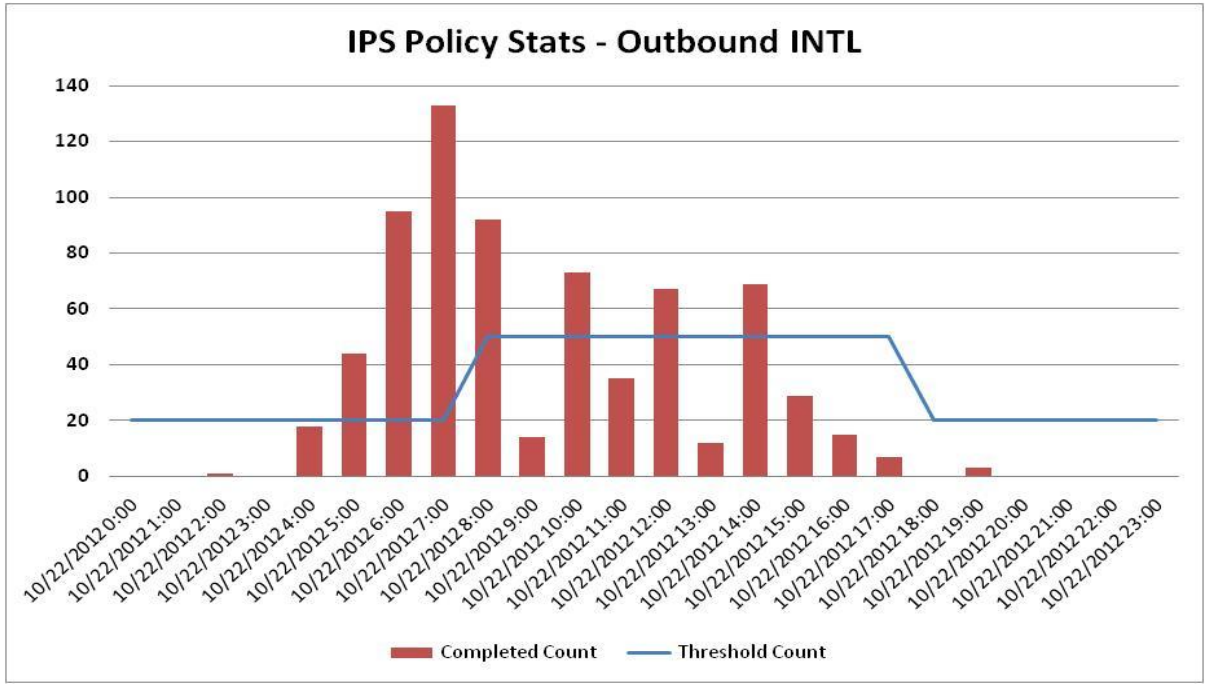
Calls to Gray-list countries

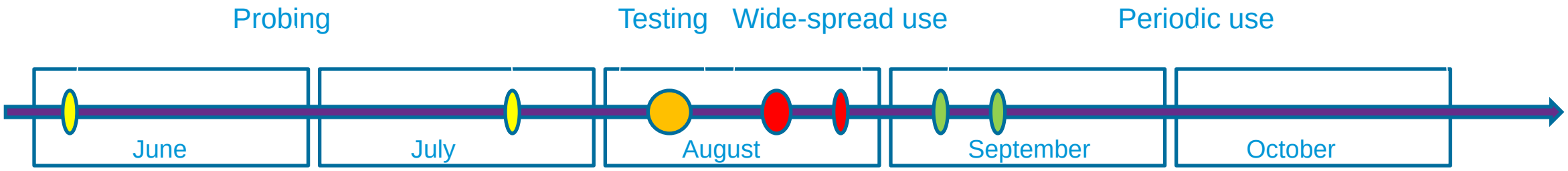
Typical Threshold

Maintain an actively managed blacklist if you can
Or
Set-up real-time alerts for Gray-list countries

Dial-Through Fraud & Misuse

- Contact Centers are places where low volume exploits are easily hidden
- Misconfiguration or intentional back-doors



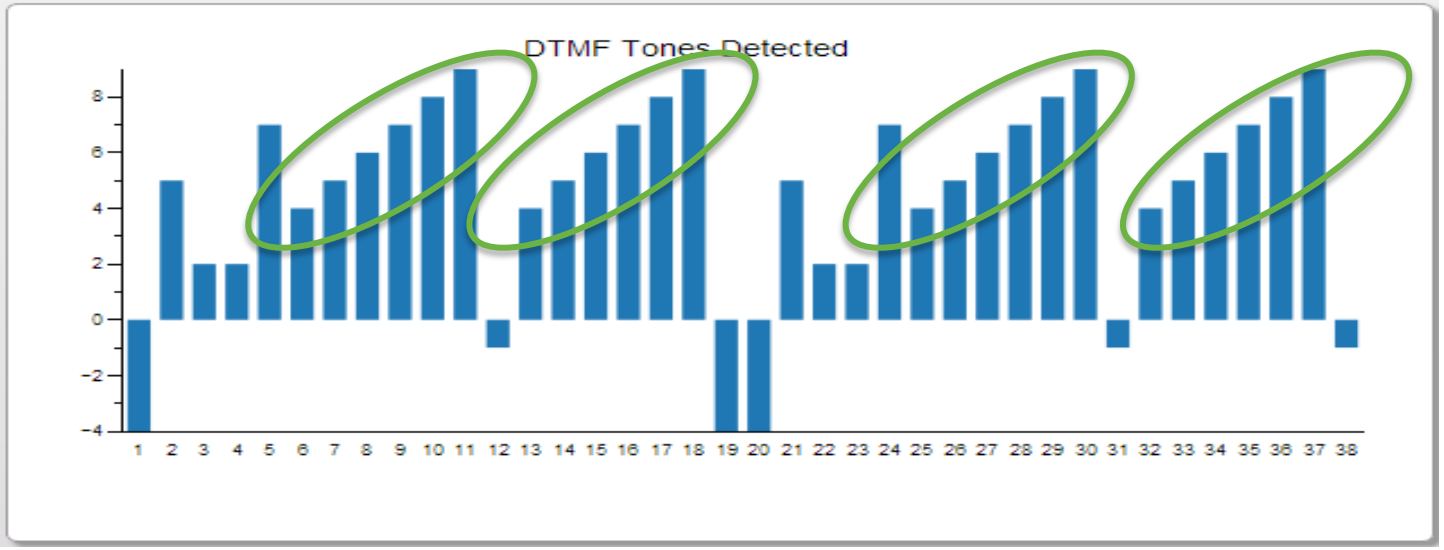


DTMF Digit Collection – looking for Fraud

- DTMF sequence looks unusual and contains an international telephone number or a repeated pattern – indicative of dial-through fraud or attempted misuse.
- DTMF sequence is unusual and call is long duration – indicative of an IVR error or someone intentionally looping in IVR.

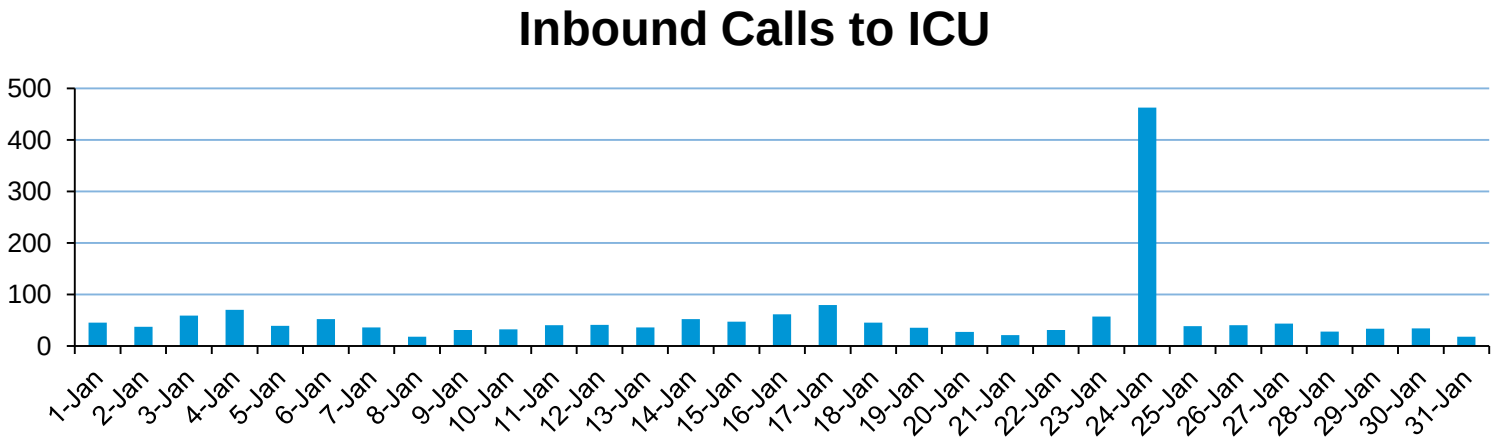
Capture all DTMF digits and trigger on patterns

DTMF Analysis



"456789" repeated over and over.
Can be indicative of a password cracking attempt.
May be IVR dwelling.
Maybe a sign of Dial-Through Fraud on IVR.

Example 1: Payday Loan Scam – Hospital



The New York Times

Business Day

WORLD | U.S. | N.Y. / REGION | BUSINESS | TECHNOLOGY | SCIENCE | HEALTH | SPORTS | OPINION

Search | Global | DealBook | Markets | Economy | Energy

Debt Collector Is Faulted for Tough Tactics in Hospitals

By JESSICA SILVER-GREENBERG
Published: April 24, 2012

Hospital patients waiting in an emergency room or convalescing after surgery are being confronted by an unexpected visitor: a debt collector at bedside.

Enlarge This Image

Craig Lassig for The New York Times

Marcia Newton took her son Maxx to a hospital where debt collectors were among employees.

This and other aggressive tactics by one of the nation's largest collectors of medical debts, Accretive Health, were revealed on Tuesday by the Minnesota attorney general, raising concerns that such practices have become common at hospitals across the country.

The tactics, like embedding debt collectors as employees in emergency rooms and demanding that patients pay before receiving treatment, were outlined in hundreds of company documents released by the attorney general. And they cast

FACEBOOK
TWITTER
GOOGLE+
EMAIL
SHARE
PRINT
SINGLE PAGE
REPRINTS

- Inbound calls from a harassing caller to Hospital ICU
- High volume calls would overwhelm ICU phone system.
- Harassing callers target hospitals according to our experience.
- Patients in hospitals are a focus of debt collectors and other harassing callers.

Example 2: Targeted Attack – Major US Bank

THE WALL STREET JOURNAL.

U.S. EDITION · Wednesday, October 17, 2012 As of 9:28 PM EDT

Home | World | U.S. | New York | Business | Tech | Markets | Market Data | Opinion | Life & Culture | Real

Digits | Personal Technology | What They Know | All Things Digital | CIO Journal

TOP STORIES IN WSJ

1 of 12

Arthur Brooks: Republicans and Their Faulty Moral Arithmetic

2 of 12

The Reverse-Joads of California

3 of 12

Say Goodbye to 4% Rule for Retirement

ASIA TECHNOLOGY | October 17, 2012, 9:28 p.m. ET

Iran Renews Internet Attacks on U.S. Banks

Officials Blame Tehran for Sophisticated Disruptions of Capital One and BB&T Websites; More Strikes Planned Thursday

Major Global Service Provider of Voice and Data services says 85% of companies being attacked on data side are also being attacked through UC

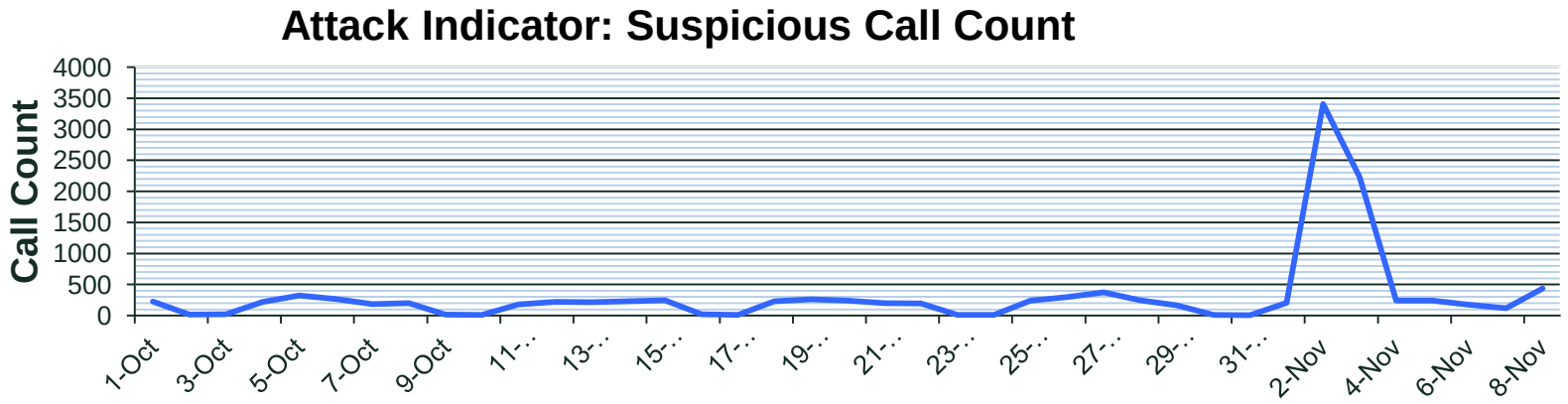
Example 2: Targeted Attack – Major US Bank

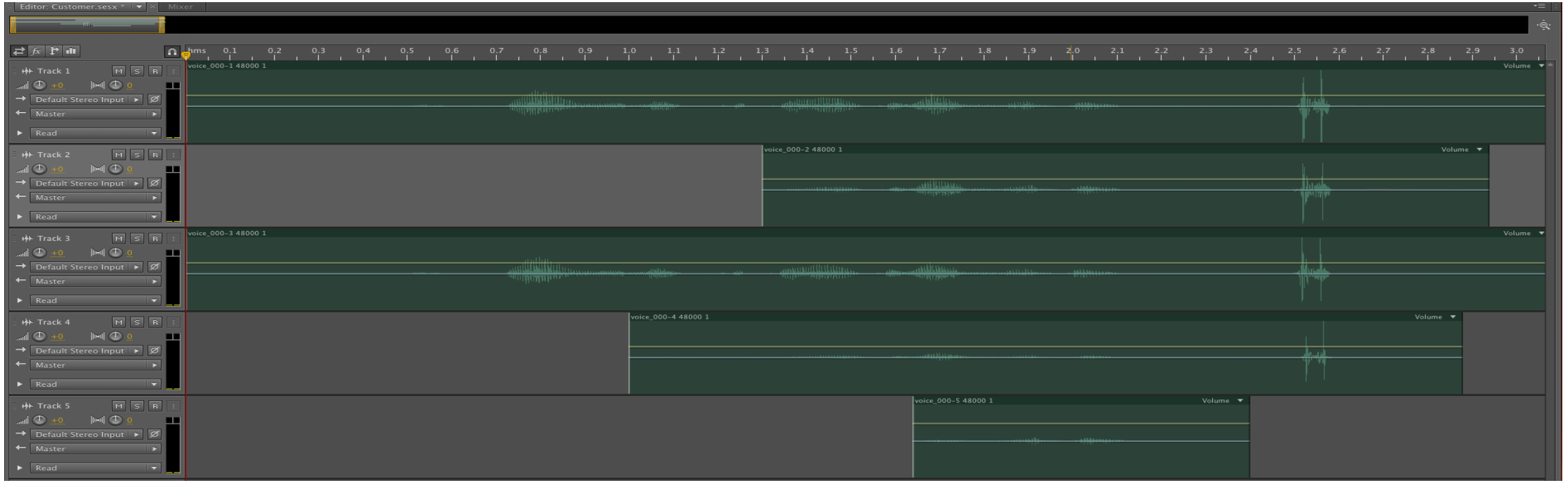
External Number
[1](989)3080617
[1](212)9308061
[1](212) 3656535*
[1](917) 6450047*
CIDR
[93]()08061771
[1](212)3083462
[98]() 9308061771
[1](212)9308346
[44]() 9308346263
[1](212)4493083
[1](989)3083462

Self-identified Persian calling into high $$ contact center

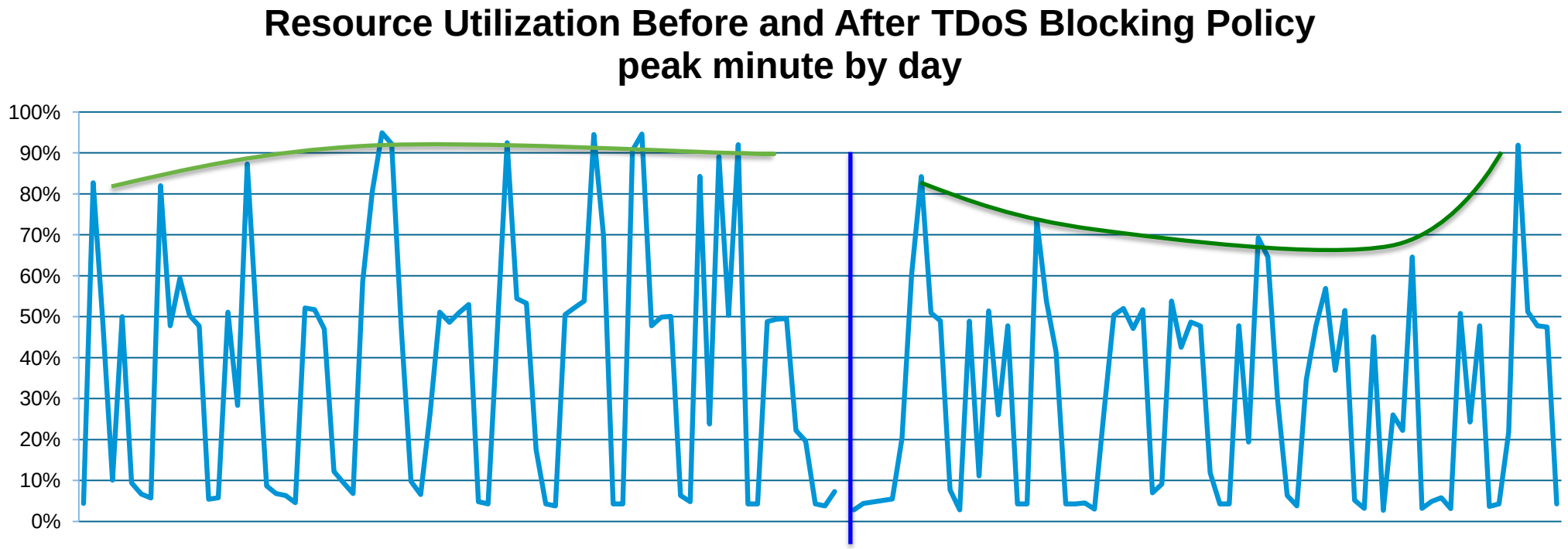
Used DTMF, CIDR, spoofed source to target & evade

Example 3: Automated Attack - Retailer



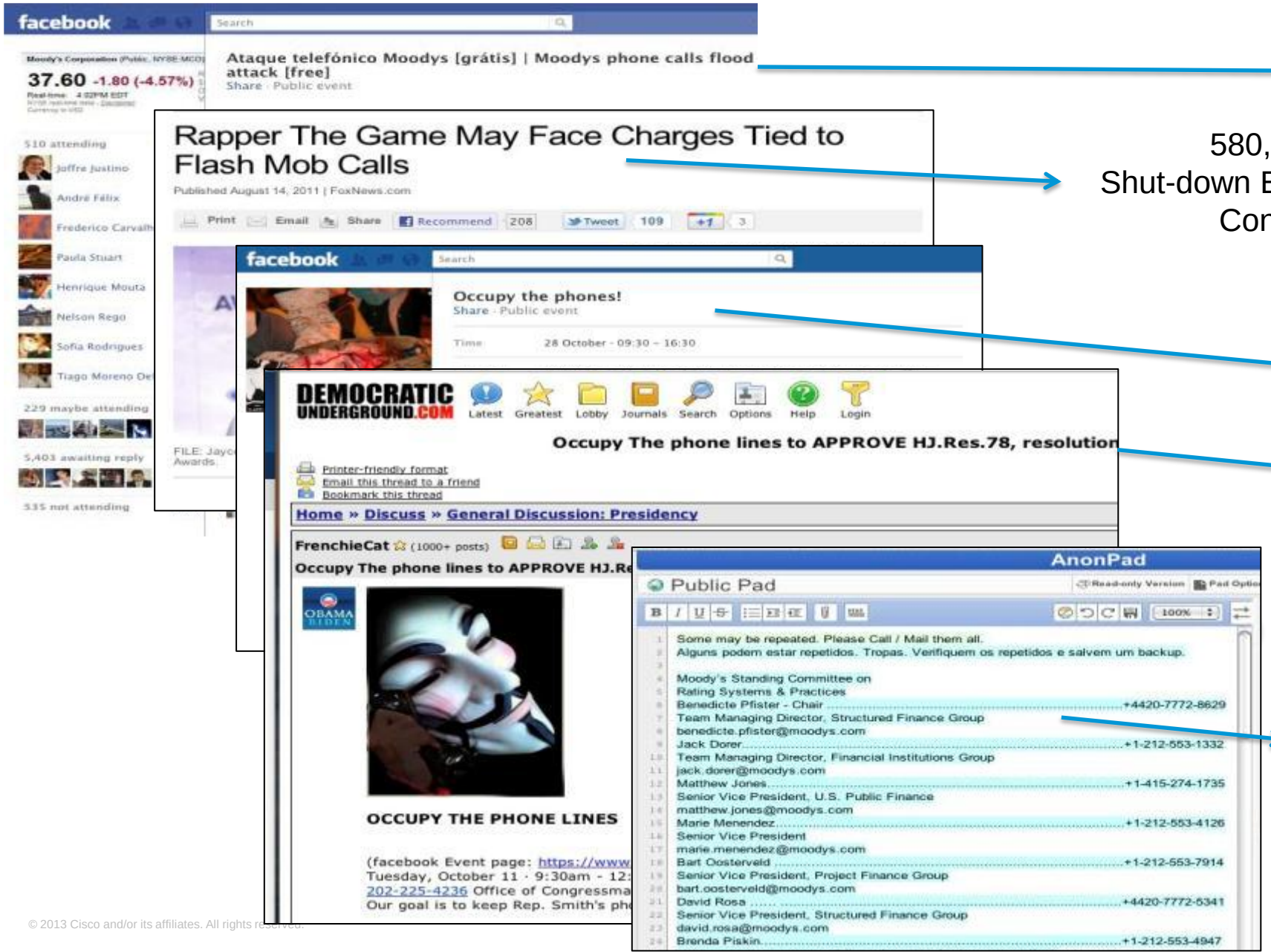


Example 4: Automated Attack - Advertising



TDoS drove circuits to peak capacity
Post blocking, circuit capacity increased 60%
Real peak calling by customers accommodated rather than busy condition

Example 5: Social Networking TDoS – Financial



July 11- Nov 11
Approx 6,000 invitees

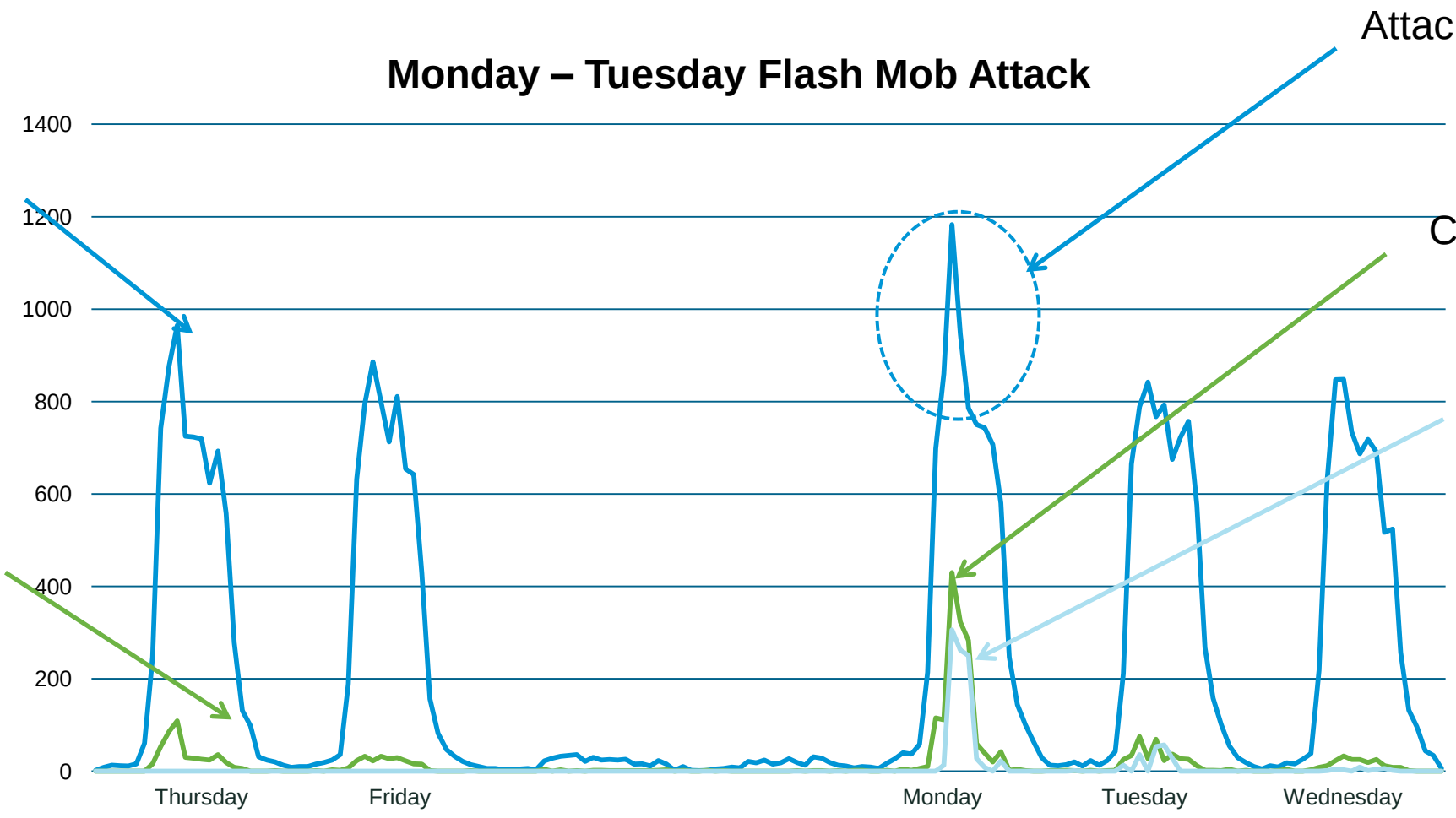
580,000 invitees
Shut-down Emergency Services Contact Center

Occupy Wall St

Becoming a mainstream tool

Researched list of numbers to call

Example 5: Social Networking TDoS – Financial



Attack Starts Monday at 11 AM

Typical daily call volume

Contact Center was main target

Attack calls blocked

Typical day at Contact Center

Unified Communications and Voice Policy and Security Detection and Mitigation

SecureLogix Solution
Unified, Enterprise-Wide Policy Management

Enterprise-wide Centralized Security/Management – SIP and TDM
Centralized policy – CPE and Service Provider Independent
Complimentary to SBCs (CUBE)

VOICE FIREWALL
TDoS,
SPIT, Call Pumping
Fraud
Social Engineering

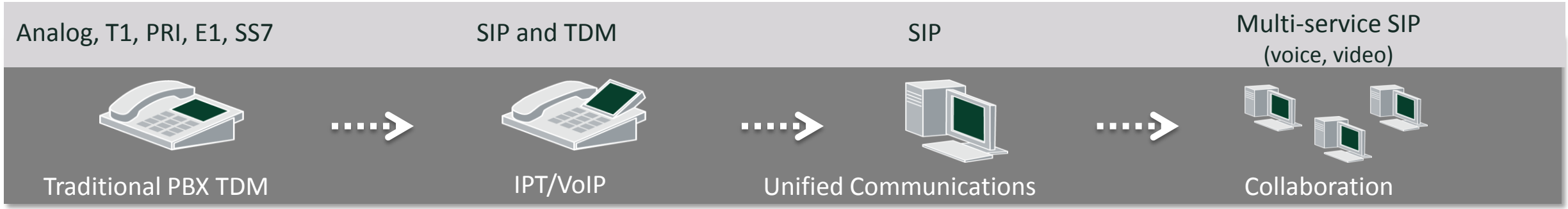
VOICE IPS
TDoS,
SPIT, Call Pumping
Fraud, Toll Fraud,
Social Engineering

USAGE MANAGER
Reporting & Analytics
Optimization, TDoS
Risk & investigations
Productivity

PERFORMANCE
Network Mgmt
Uptime & Reliability
Performance Alerting
Troubleshooting

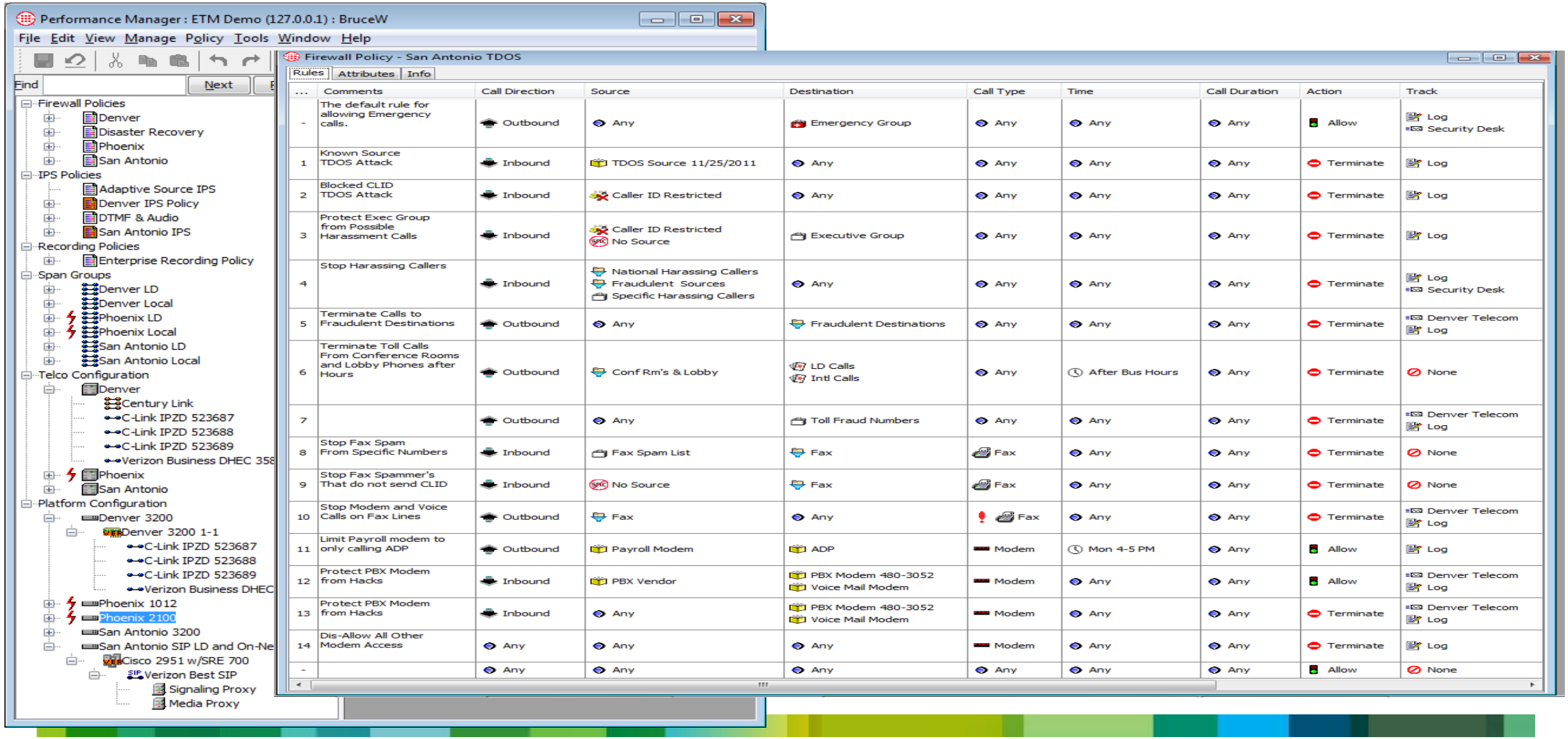
CALL RECORDER
Threatening Calls
Data Leakage, TDoS
Investigations
Ops and Productivity

Any network evolution

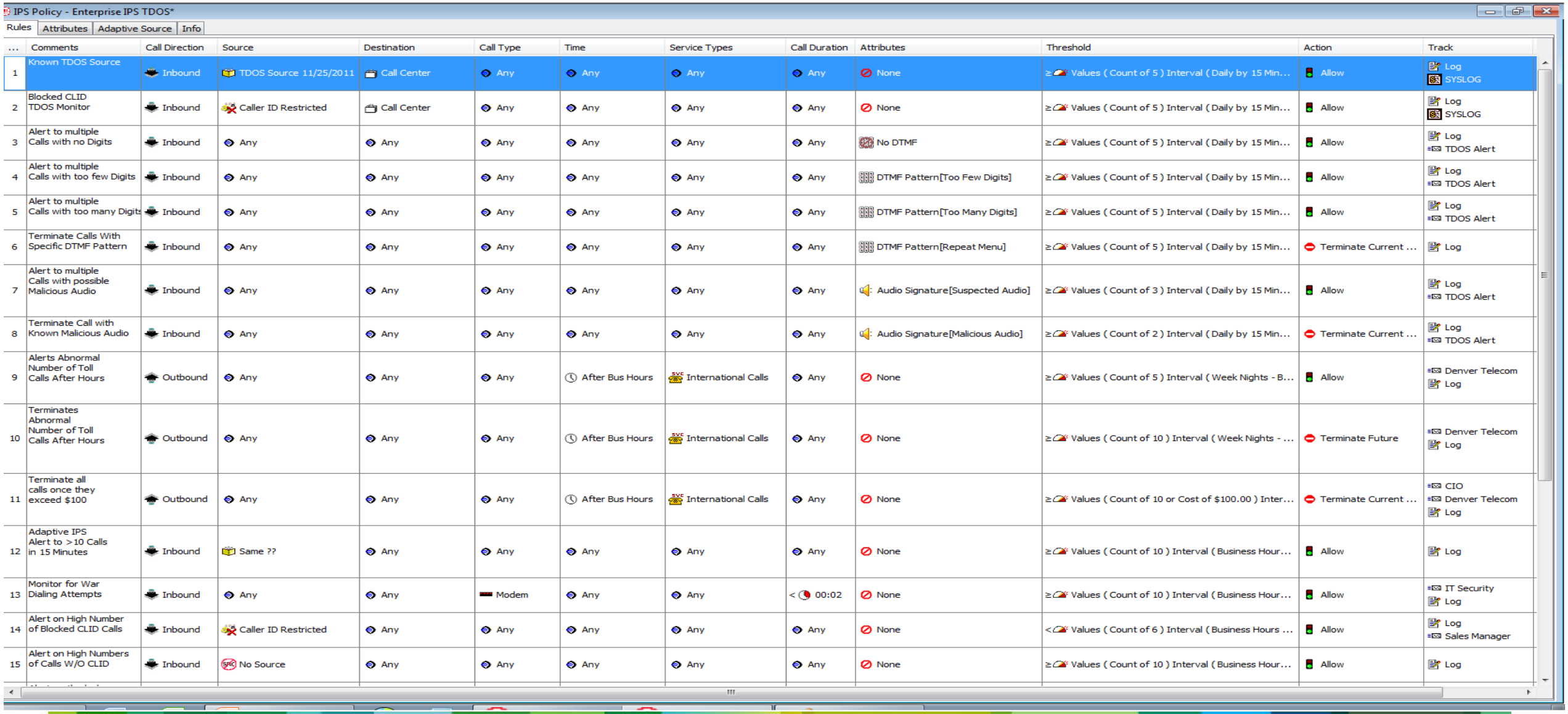


Real time Identification and Control of Attacks on the Voice/UC Network
Complimentary to SBCs

TDoS Mitigation - Firewall



TDoS Mitigation - IPS

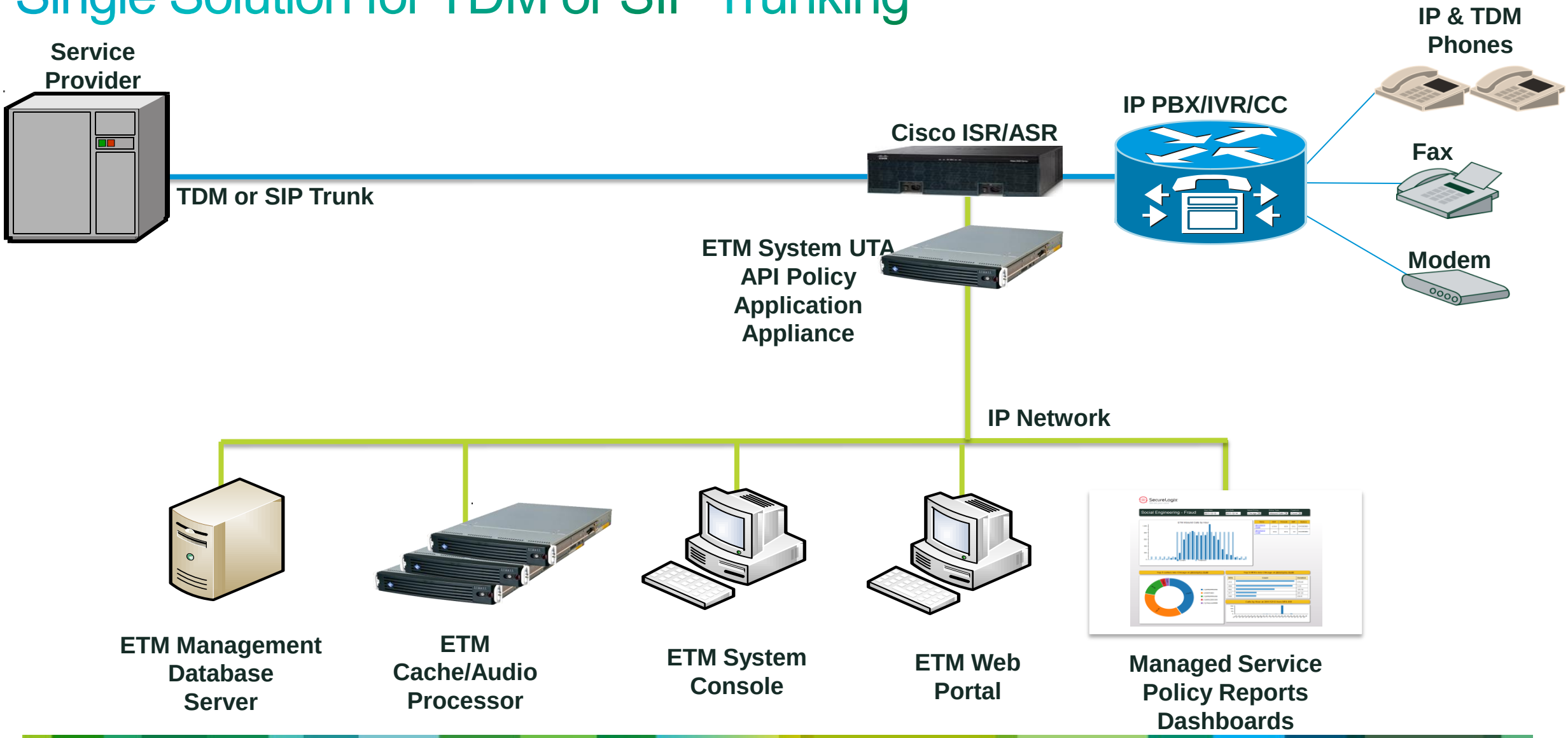


IPS Policy - Enterprise IPS TDOS*

Rules | Attributes | Adaptive Source | Info

...	Comments	Call Direction	Source	Destination	Call Type	Time	Service Types	Call Duration	Attributes	Threshold	Action	Track
1	Known TDOS Source	Inbound	TDOS Source 11/25/2011	Call Center	Any	Any	Any	Any	None	≥ Values (Count of 5) Interval (Daily by 15 Min...	Allow	Log SYSLOG
2	Blocked CLID TDOS Monitor	Inbound	Caller ID Restricted	Call Center	Any	Any	Any	Any	None	≥ Values (Count of 5) Interval (Daily by 15 Min...	Allow	Log SYSLOG
3	Alert to multiple Calls with no Digits	Inbound	Any	Any	Any	Any	Any	Any	No DTMF	≥ Values (Count of 5) Interval (Daily by 15 Min...	Allow	Log TDOS Alert
4	Alert to multiple Calls with too few Digits	Inbound	Any	Any	Any	Any	Any	Any	DTMF Pattern[Too Few Digits]	≥ Values (Count of 5) Interval (Daily by 15 Min...	Allow	Log TDOS Alert
5	Alert to multiple Calls with too many Digits	Inbound	Any	Any	Any	Any	Any	Any	DTMF Pattern[Too Many Digits]	≥ Values (Count of 5) Interval (Daily by 15 Min...	Allow	Log TDOS Alert
6	Terminate Calls With Specific DTMF Pattern	Inbound	Any	Any	Any	Any	Any	Any	DTMF Pattern[Repeat Menu]	≥ Values (Count of 5) Interval (Daily by 15 Min...	Terminate Current ...	Log
7	Alert to multiple Calls with possible Malicious Audio	Inbound	Any	Any	Any	Any	Any	Any	Audio Signature[Suspected Audio]	≥ Values (Count of 3) Interval (Daily by 15 Min...	Allow	Log TDOS Alert
8	Terminate Call with Known Malicious Audio	Inbound	Any	Any	Any	Any	Any	Any	Audio Signature[Malicious Audio]	≥ Values (Count of 2) Interval (Daily by 15 Min...	Terminate Current ...	Log TDOS Alert
9	Alerts Abnormal Number of Toll Calls After Hours	Outbound	Any	Any	Any	After Bus Hours	International Calls	Any	None	≥ Values (Count of 5) Interval (Week Nights - B...	Allow	Denver Telecom Log
10	Terminates Abnormal Number of Toll Calls After Hours	Outbound	Any	Any	Any	After Bus Hours	International Calls	Any	None	≥ Values (Count of 10) Interval (Week Nights - ...	Terminate Future	Denver Telecom Log
11	Terminate all calls once they exceed $100	Outbound	Any	Any	Any	After Bus Hours	International Calls	Any	None	≥ Values (Count of 10 or Cost of $100.00) Inter...	Terminate Current ...	CIO Denver Telecom Log
12	Adaptive IPS Alert to >10 Calls in 15 Minutes	Inbound	Same ??	Any	Any	Any	Any	Any	None	≥ Values (Count of 10) Interval (Business Hour...	Allow	Log
13	Monitor for War Dialing Attempts	Inbound	Any	Any	Modem	Any	Any	< 00:02	None	≥ Values (Count of 10) Interval (Business Hour...	Allow	IT Security Log
14	Alert on High Number of Blocked CLID Calls	Inbound	Caller ID Restricted	Any	Any	Any	Any	Any	None	< Values (Count of 6) Interval (Business Hours ...	Allow	Log Sales Manager
15	Alert on High Numbers of Calls W/O CLID	Inbound	No Source	Any	Any	Any	Any	Any	None	≥ Values (Count of 10) Interval (Business Hour...	Allow	Log

System Architecture
Single Solution for TDM or SIP Trunking



Summary

Voice Policy Use Cases - 5 Identifiable Categories

ROI Opportunities in the Enterprise Voice Network

Enterprise Wide Capacity Management

- **Centralized reporting for the enterprise**
- Baseline and inventory voice network infrastructure
- Recover capacity lost to unauthorized traffic
- Right-size trunk infrastructure based on trunk utilization
- Identify and Eliminate unused PBX bypass lines
- Identify orphaned or unused extensions
- Consolidate/reduce unused fax resources
- Absence of call activity on trunking resources
- Excessive unanswered/busy calls on trunking resources
- Optimize staffing based on call activity reports

Enterprise Wide Control of Service Abuse

- **Centralized abuse prevention policy definition**
- Unauthorized Modem usage
- Voice Data Leakage Protection (DLP)
- Reduce toll fraud losses by blocking unauthorized calls
- 911 notification and response
- Managed calls to and from restricted numbers

Enterprise Wide Security Management

- **Centralized Security Policy Definition**
- TDOS (Telephony Denial of Service) Mitigation
- Eliminate Toll Fraud Losses from external dial through
- Prevent network penetration via blocking modems
- Alert and control business disrupting bomb threats
- Identify and Manage harassing calls.
- Alert/log maintenance port access, and block unauthorized connections
- Minimize Contact Center Service abuse or misuse
- Prevent identity theft on voice lines

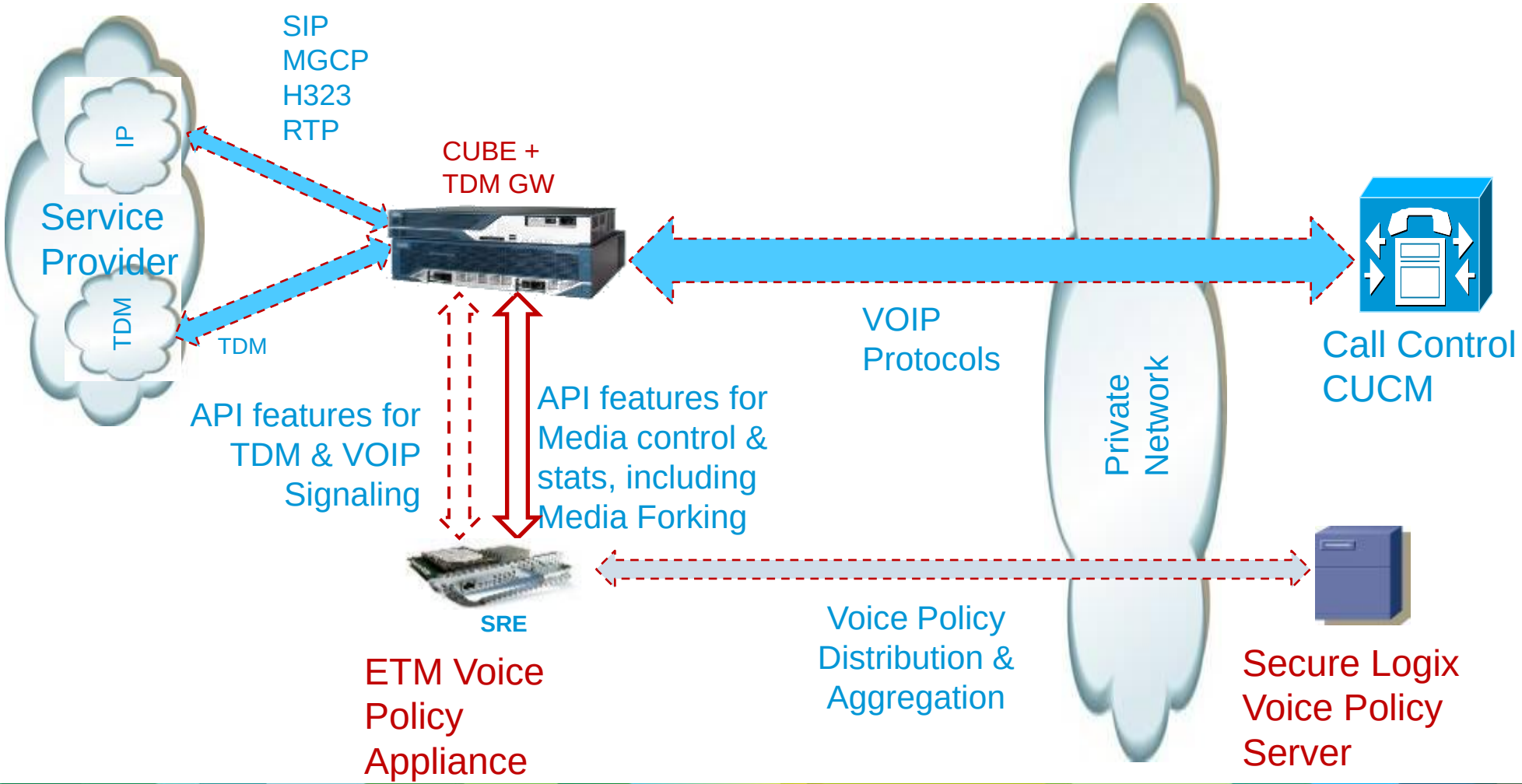
Customer Service Monitoring

- Policy based recording to audit call agent performance
- Policy based recording of potential harassing calls

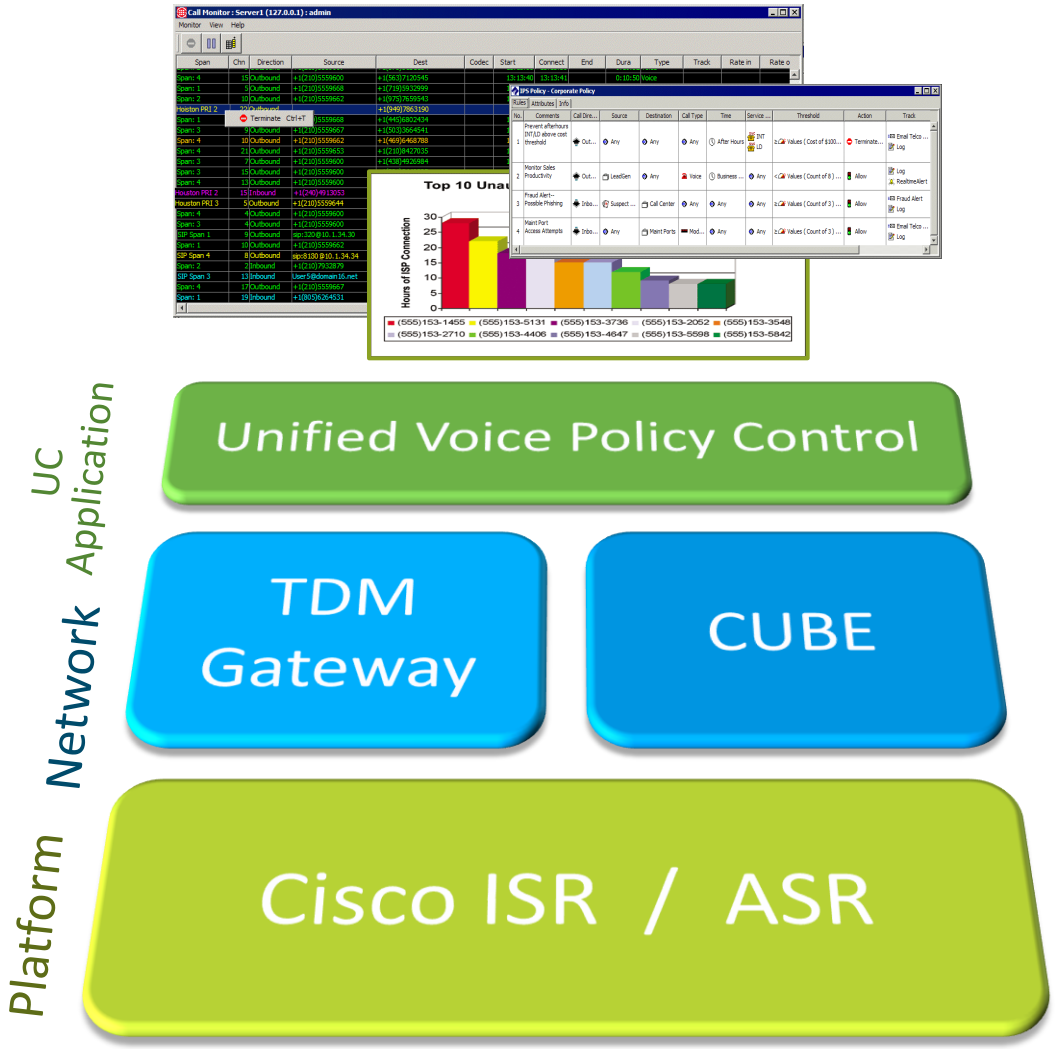
SLA Monitoring

- Log of service outages, disruptions, and errors
- Voice Usage uptime and performance reports

Protects Entire Network Edge - TDM & SIP Trunking
Network Topology for Cisco & SecureLogix Solution



Cisco / SecureLogix Voice Policy Solution: Key Takeaways



- Voice Policy supports a very broad range of use cases
  - Voice Policy ensures that the strategic voice network is used for appropriate functions
  - At least 5 categories of relevant use cases
- Telephony Denial of Service (TDoS) is a rapidly growing threat
  - Published telephone numbers are the primary vector for TDoS attacks.
  - Call centers are particularly vulnerable.
- Cisco and SecureLogix deliver the only complete Voice Gateway / Policy Solution
  - Addresses all 5 major categories of use cases.
  - Allows architectural flexibility
  - Address TDM and SIP Trunking

Next Steps: Evaluate and Access Resources

Evaluate Webcast

How did we do? Complete the evaluation as you exit

Enterprise Voice Security and Policy Using Cisco ISRs and ASRs

Evaluation Questions	Answers
1. This webcast provided me a better understanding of enterprise voice security and policy using Cisco ISRs and ASRs.	
2. This webcast was valuable and a good use of my time. *	
3. The speakers clearly presented the information. *	
4. I am a: *	
5. Will you attend another webcast of similar style and format in the future? *	
6. Are you more likely to buy Cisco products as a result of viewing this program? *	Yes No
7. What did you like best about this webcast?	
8. How can we improve this seminar?	
9. What topics would you like to see addressed in future community webcasts?	

Resources and Next Steps

Access resources

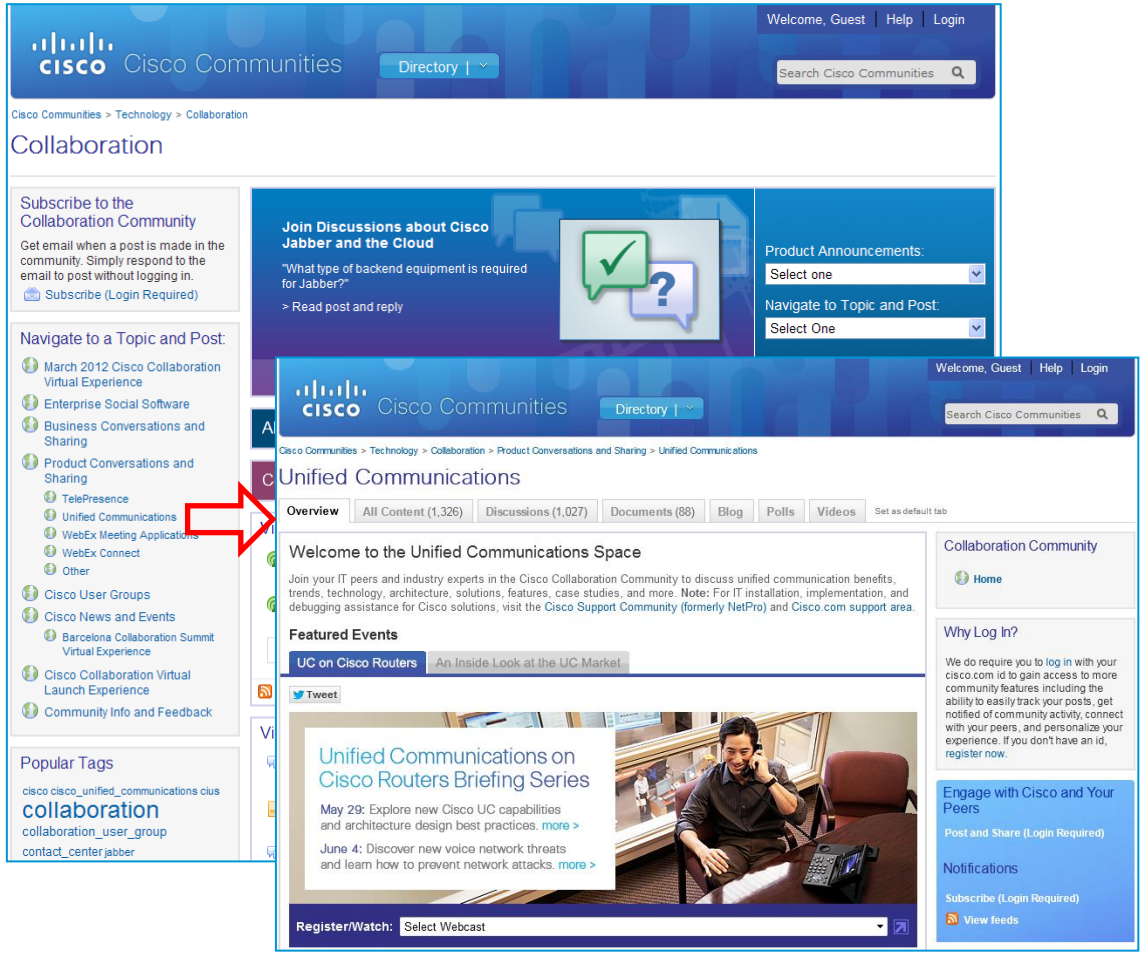
http://communities.cisco.com/message/124194

- This presentation and replay of this briefing
- Q&A from today (posted by June 7)
- Links to Cisco and SecureLogix reports, web pages, etc

Watch Replay of May 29 Technical Webcast:

New Cisco UC Capabilities and Design Tips for Cisco ISRs and ASRs

- Overview of new Cisco UC capabilities now available on Cisco ISRs and ASRs, including enhancements for SIP trunking, gateways, branch and cloud telephony survivability, and branch call control
- Best practices for designing your UC and collaboration architecture to benefit from these new capabilities



Engage with peers and experts in community

www.cisco.com/go/joinconversation (select "Unified Communications" to access May 29 and June 4 webcasts)

Thank you.