



# Management and Security Issues for IP-PBXs Lessons from the Trenches Session 1 of 2

PlanNet Consulting, LLC

Ken Agress, Senior Consultant

Craig Burness, Senior Consultant



## Agenda

- **Introductions and Firm Background**
- **Transitioning From the Vendor Team**
- **Common First Year Problems**
- **Essential Management Tools**
- **Securing Your System**



## Introductions and Firm Background

Seventh  
VoiceCon!

### **PlanNet Consulting**

- Independent communications technology consulting
  - Voice, Data, Video, Cabling, A/V, Security
- Project consulting and services for a wide range of enterprises
- Frequent presenter at industry conferences
- Numerous articles published in BCR

### **Ken Agress**

- 17 years communications experience
- Extensive network, performance experience

### **Craig Burness**

- 20 years in the communications industry
- Numerous voice and contact center engagements



## Transitioning From the Vendor Team

- **Transitioning support will be a critical time for your organization**
  - The “real” shift of roles and responsibilities
  - The integrator is phasing out; eliminating a “security blanket” for your staff
  - Your staff will have to run with “support by committee” and communicate well
- **Don’t overlook the difficulties of the transition**
  - Prepare a solid plan
  - Pilot the processes if you can
  - Proactively engage staff to reduce frustration and improve communication



## Making an Effective Transition

- **Define who's on the transition team**
  - Vendor PM
  - Vendor Technical Resources
    - Technicians, Specialists, Trainers
  - Key Staff Resources
    - Voice Support, Data Support, Help Desk
- **Ensure all contact information is up to date**
- **Make sure mobile contact information is available**



## Making an Effective Transition (continued...)

- **Clearly define roles and responsibilities**
  - *“The proposer shall provide no less than three on-site technicians from the date of cut-over until...”*
  - *“The proposer shall provide problem identification and resolution assistance for all aspects of support...”*
- **Don’t let the vendor PM “leave” until you’ve accepted the system!**
- **Define when transitions are scheduled to occur; don’t catch your staff off guard**



## Setting up a Successful Transition

- **Require on-site vendor assistance during the cutover and for some period of time thereafter**
  - Be specific regarding roles and skill sets
    - Help Desk, Voice Specialist, Data Specialist, Trainer
  - Be realistic about the staffing levels required
    - You will be paying for this...
  - Include these requirements in the RFP
- **Reserve the right to interview critical personnel**
- **Think about the “fit” with your own support staff**



## Kicking Off the Transition

- **Prior to cutover, begin transition meetings with your staff and the vendor's team to determine:**
  - Who will fill what role
  - Where resources will be located
  - How much "On the Job Training" will be provided
  - How issues will be escalated
- **Place staff and vendor resources where they're likely to do the most good**
  - Make the support staff available to the users
  - No sitting around in "War Rooms"
  - Place support personnel near "critical communities" to facilitate rapid response



## Your First Days After Cutover

- **Get support staff out and about!**
  - Immediate assistance to those with problems is “good press” even if things are going wrong
  - Allows users to easily attract support personnel stationed in critical areas (such as a call center)
  - Helps to prevent the help desk from becoming a support bottle neck
- **Make sure your dispatch team is up to speed and is able to communicate with support staff**
- **Check in regularly with staff to make sure communication and processes are effective**



## Get the Most From Your Vendor

- **Have your staff “shadow” vendor support**
  - Learning troubleshooting techniques is as important as understanding configurations and technologies
  - “Real world” experience with the vendor’s team helps build your staff’s confidence
  - Allows you to “phase in” your staff while the vendor is still available for immediate assistance
- **Emphasize the importance of learning by doing**
  - A “shadow” shouldn’t be watching all the time; they also need to be doing...
  - Set expectations with your vendor that they will be required to answer questions as they go
  - Try to avoid splitting up teams unless critical issues require it



## Your First Problems

Know Your Staff

- **For your first problems...**
  - Do you want the vendor to take the lead?
  - Do you want your staff to lead and just have the vendor “consult” on direction and decisions?
  - Who will be on the phone with the manufacturer for the first support calls?
  - How will you and your support team prioritize issues and responses?
- **Gear the plan to your staff’s skill level and the vendor support team**



## Your First Problems

Oversight

- **Pay attention to the early issues**
  - Look for end-user training issues and direct resources appropriately
  - Look for staff training issues and identify areas for additional study or courses
  - Make sure the vendor is playing their role effectively
- **Involve IT/Voice Management in early problems if it will help ensure positive outcomes**
- **Use help desk logs, trouble tickets, and feedback from staff and end-users for system acceptance**



“Don’t Let ‘em  
Just Walk Away”

- **Make sure the vendor provides a well documented “Run Book”**
  - Know what hardware and software is installed
  - Know how it is configured
  - Make sure changes have been logged properly
- **Define required documentation in RFP or contract**
  - Diagrams (logical and physical)
  - Configurations or configuration templates
  - Commentary on the configurations detailing settings
  - Issues/Problem logs
  - Acceptance testing checklists, activities, and results
- **Ensure management tools are running properly prior to acceptance**



## Move Your Staff to the Front

- **Have your staff lead problem identification and resolution as you move towards acceptance**
  - Vendor staff should still assist; don't let them "off the hook" for contracted support
  - Call manufacturer support to learn their systems and understand what they'll need to know
- **Verify that change and configuration management policies are being followed!**
- **Vendor should not be the only one involved with system test and acceptance**
  - Help perform tests or (at a minimum) observe



## What to Prepare For...

- **Converging support groups adds challenges**
  - “Support by committee” is likely to be a new factor
  - Organizations can be quick to let go of voice staff
  - “Language barriers” create issues (a pilot can help)
- **PBX projects can be “emotionally charged”**
  - Staff may resist new roles and responsibilities
  - The groups they support may be neutral or negative regarding the new system
  - The quality (and timing) of training will greatly impact the support load
- **Staff will need time to make good use of new tools and adjust to processes**



## Common First Year Problems

Self Inflicted

- **Making significant design changes “on the fly” or without careful consideration**
  - Call Processing placement and configuration
  - Dial plan
  - Call routing and coverage
  - Features enabled or disabled
- **“Ad hoc” purchases (such as headsets)**
  - Hard to control in many environments
  - Publish standards/information to help guide purchases
  - Work with purchasing to add technical review



## Common First Year Problems

### Administration Issues

- **Outdated or infrequently updated auto-attendant recordings**
  - Is someone responsible?
- **Firewall configuration issues**
  - Rules are too strict: Acceptable communications fail
  - Rules are too loose: System at risk for fraud or attack
  - Change control is lacking
  - Frequency of log reviews
- **Sorting out what the help desk does**
  - Are they the M-A-C Group?
  - Do they resolve problems or open tickets?
  - How do they dispatch and for what groups?



## Common First Year Problems

Design  
Details

- **Placement of security devices creates issues**
  - Insufficient throughput
  - Loss of QoS in headers
  - Unable to process QoS end-to-end
- **Network configuration**
  - Spanning Tree issues
  - Routing protocol issues
  - “Rogue” hubs, access points, servers, and services
- **Security posture and approach**
  - Is authentication working properly?
  - Are antivirus and firewall policies enforced?
  - Are the right services available?



## Common First Year Problems

- **QoS parameters aren't set properly or can't adapt to small changes**
- **Insufficient bandwidth (WAN)**
- **Voice clipping and similar codec issues**
  - Knowing the possible sources
  - Understanding the convergence of hardware and configurations

Quality  
Control



## Common First Year Problems

- **Mistakes configuring devices result in unforeseen issues and consequences**
- **Echo issues**
- **Accurately predicting impact of changes on voice and data flows**
- **Voice flaws are relatively “chaotic” and may shift for unforeseen reasons**

More  
Quality Control



## Common First Year Problems

Other  
Issues

- **Bugs, bugs, and bugs...**
  - Select a software version to install and stick with it (for both voice and data elements)
  - Have the vendor commit to “known good” versions
  - Verify interoperability with other products
    - Messaging, Call Accounting, E911...
- **Care and feeding...**
  - Consider the impact of changes on other products and environments
  - Subscribe to and review bug tracking websites and distribution lists
  - Know what features are being used



## Common First Year Problems

- **Carrier finger-pointing**
  - Everything is the new system's problem...
- **Finger-pointing between Voice and Data vendors and/or internal support groups**
- **Unexpected or new application flows cause bandwidth and quality issues**
  - Can you detect them early?
  - Do your management tools alert you?
  - Do your departments purchase their own software?

More  
Issues



## Essential Management Tools

- **Convergence adds complexity and calls for improved tools**
  - Do you want routine reports on call quality?
  - Do you need to be able to isolate and analyze specific application or call flows?
  - Do you want proactive notification of likely issues?
- **Selecting the right tools is more important than “just deploying something”**
  - Focus tool purchases on mission critical support goals
  - Involve support staff (heavily) in the selection process
  - Look beyond system manufacturer offerings!
- **Don’t just look at the tool – look at your support processes as well!**



## Before You Buy a Tool...

- **Adopt a “manage the service” approach**
  - Likely that you’ll need more than just raw performance statistics
  - Tie measured metrics to goals and service levels
  - Leverage reporting capabilities to provide visibility to management and key users
  - Remember, it’s the user experience that matters
- **Ensure your hardware reports the right data to the management system**



Before You  
Buy a Tool...  
(continued...)

- **Verify that systems have enough memory and processing power**
- **Once you've narrowed the field, check real-world references**
- **Understand custom report and view demands**
- **Demo your ability to create or modify reports**



## FCAPS

- **ITU based management framework**
- **Divides management functions into domains:**
  - **Fault Management**
  - **Configuration Management**
  - **Accounting Management**
  - **Performance Management**
  - **Security Management**
- **While domains address different functions, they are mutually related and supportive**
- **Select tools that help you “plug holes” in processes and/or staff relating to a domain**
- **Requires that you evaluate processes to address functional domains effectively**



## FCAPS Domains

Fault Management	Configuration Management	Accounting Management	Performance Management	Security Management
alarm handling	system turn-up	track service usage	data collection	control NE access
trouble detection	network provisioning	bill for services	report generation	enable NE functions
trouble correction	Auto discovery		data analysis	access logs
test and acceptance	back up and restore			
network recovery	database handling			



## What You Need to Know

- Use FCAPS to develop processes, not just guide tool selection
- Tools should supplement, enforce, and streamline processes
- Tools may (and are likely to) cross functional domains
- As your network grows you probably need to cover more FCAPS domains
- Cost for tools will increase as additional domains are addressed



## Applying FCAPS: **Fault Management**

- **Detect, isolate, and resolve faults**
  - Network monitoring software such as CiscoWorks (DFM), EpiCenter, and HPOV
  - Root cause analysis software such as EMC SMARTS
  - Resources capable of understanding the software, determining the resolution, and/or managing to resolution
  - Sound processes for detecting, isolating, and resolving faults
  - Fully documenting the fault for future reference is extremely important



## Applying FCAPS: **Fault Management**

What to  
Look For

- **Strong fault correlation**
  - Limits number of alarms/alerts
  - Provides good assistance with fault isolation
  - Preferably provides some automation for problem resolution activities
- **Ability to report and correlate “faults” that go beyond up or down status**
  - “Flapping” connections
  - Route table changes and/or issues
  - Performance issues
- **Ability to accept data from external sources**
  - IP PBX
  - Servers or specific processes
  - Network probes



## Applying FCAPS: **Configuration Management**

- **Manage the configuration of servers, gateways, routers, and switches**
  - Develop a process for configuration changes that is integrated with the change management process
  - Make sure automatic logging of ALL configuration changes is enabled
  - Perform frequent verifications of configurations, firmware versions, and software versions
    - Update the tracking information
  - Subscribe to update services to stay on top of new versions of software and firmware as well as any configuration improvements



## Applying FCAPS: **Configuration Management**

What to  
Look For

- **Enforcement of configuration management and/or change management policies**
  - Limited device access
  - Approval chains and processes
  - Alerts of changes or automatic rollback
- **Support for device templates**
  - Analysis of configurations against model
  - Automated application of templates to new devices
  - Bulk update of devices based on template changes
- **Archive of configurations**
  - Change review and manual rollback
  - Assist in problem analysis and resolution
- **Impact analysis: If we change this what will happen?**



# Management and Security Issues for IP-PBXs

## Lessons from the Trenches

### Session 2 of 2

PlanNet Consulting, LLC

Ken Agress, Senior Consultant

Craig Burness, Senior Consultant



## Applying FCAPS: **Accounting Management**

- **Document resources and utilization**

- Develop metrics to document the performance of the system (busy hour traffic, PRI utilization, number of calls dropped per hour, etc.)
- Populate database tables or spreadsheets with data that can be graphed in different ways based on need
- Possible use for chargeback
- Analyze collected data in relation to past trends and attempt to correlate questionable data with information from fault, configuration, and performance information



## Applying FCAPS: **Accounting Management**

What to  
Look For

- **Tracking usage or utilization**
  - Chargeback to departments
  - Detailed records of calls and connections
  - Bandwidth consumed by port and/or IP address
- **Call Detail Records**
- **Bill analysis and comparison**
- **Management reports**
- **Call routing reports**



## Applying FCAPS: **Performance Management**

- **Ensure overall performance**
  - Periodic tests to measure utilization, throughput, latency, delay, jitter, etc. should be performed
  - Analyze data in relation to accounting information to assess and ensure proper performance
  - Use collected performance and accounting information to judge the overall health of the system (i.e. Concord)
  - Data is useful to develop trending patterns
- **Many approaches available**
  - Network probes
  - Recovering from devices and/or streams
  - CDR details on performance



## Applying FCAPS: **Performance Management**

What to  
Look For

- **Critical metric reporting**
  - Latency
  - Jitter
  - Utilization
  - Availability
  - MOS/R-Factor
- **Usage trending**
  - Historical data
  - “Hot spot” identification
- **Performance forecasting**



## Applying FCAPS: **Security Management**

- **Processes to secure the environment**
  - Use AAA to authenticate, authorize, and account for user actions (RADIUS, TACACS+, etc.)
  - Utilize IDS sensors for monitoring activity and inspect alerts regularly
  - Use secure shell access (SSH) and secure management VLAN for remote console operations
  - Use VPN to remotely administer devices
  - Day 0 Attacks – Anomaly Detection
  - Physically secure equipment to make it harder for unauthorized personnel to tamper with systems



## Applying FCAPS: **Security Management**

What to  
Look For

- **Authenticated access and management**
- **Logs of access to resources**
  - Include user and source of traffic
  - Preferably can provide detail of activity
  - Alarms/alerts for failed attempts and unauthorized access attempts
- **Monitoring of core resources**
  - DHCP and DNS servers
  - Call processing platforms
  - Key servers and services
- **Identification of potential attacks**
  - Unexpected traffic flows
  - High traffic volumes
  - Correlation of events to assist in problem identification and resolution
- **Some degree of automation or intelligent response**



## Tools are a Requirement

- **View tools as a requirement to assist your staff in their role; not as a “luxury”**
  - Converged networks are more complex
  - Dependency on network for services increased
  - Support activities are more difficult without tools
- **Tools can assist your staff in following updated policies and procedures**
  - Particularly strong for configuration (change) management
  - Supports or allows use of Service Level Agreements
    - Availability (Service, System, Network)
    - Performance (Response Time, Call Completion %, MOS/R-Factor)
  - Can increase management visibility into network and/or staffing issues



## FAQ

- **How much should I budget for tools?**
  - “Minimal” Capabilities: \$50,000 (Fault, Configuration, and some Performance Management)
  - “Median” Capabilities: \$50-125,000 (Enhanced Performance, Accounting, Trend Analysis)
  - “Heavy” Capabilities: \$125,000+ (all domains with specialized coverage of key areas)
- **Organizations typically don’t budget adequately for tools in the initial deployment**
  - Many assume existing tools will suffice but make additional purchase within twelve months
  - General assumption that prior systems will suffice is usually not completely accurate
  - Even if existing tools do provide necessary capabilities you should budget for some customization (reporting)
- **Before selecting any package ask yourself, “Will this help manage my network as a service?”**



## Example: Good and Bad

- Engaged to provide configuration support to test equipment
- Relatively low-end management system deployed
- System provided Fault, Configuration, and limited Performance Management
- Test team began modifying switch and router configurations in order to execute test plans
- Within five minutes, configuration changes had “vanished”
- Loss of configuration changes detected when identical test was performed
- Management system detected modification to configuration files and pushed old configuration to device



Example:  
Good

- International carrier having difficulty reporting on their Service Levels
- Existing systems provided some performance insight but limited proactive notification of pending issues
- Management systems generally did not provide long term trends of performance data
- Reports provided to support staff and customers were generated from different systems which created communication issues
- Deployed new data collection/aggregation tool for performance management
- Reports customized to match SLA commitments
- Customers and internal reports on common system
- Alerts and notifications generated for internal support prior to SLA violation



## Securing Your System

- **The Bad: Converged networks introduce new vulnerabilities to your environment**
  - Voice and data traffic traverse a common network
  - In some configurations, separate logical networks cannot be maintained
  - Direct IP communications to partners, carriers, or via the internet for voice introduces new variables
  - IP-based services also create new vulnerabilities for carriers (billing review and audit implications)
- **The Good: Vendors are already releasing products to address vulnerabilities**
  - “SIP aware” firewalls
  - IDS/IPS with IP Telephony knowledge
  - Generally improved security products
- **The Ugly: We don’t know what we don’t know...**



## How Bad Can It Be?

- ***“We were well along in our deployment of IP-PBX’s, then along came the e-mail viruses – Sasser, Code Red, things that took our data network and crumpled it. Because our voice network rode on top of the network...we experienced some [voice] outages of anywhere from two to four hours before we could get access control lists in place [to block the attacks].”***
  - Vice President, major financial services firm  
(from Network World Fusion)



## “It’s Just an Application”– But it’s Not

- **You’ll do well to follow “standard” information security best practices, but...**
  - Will your firewall support QoS for processing/forwarding traffic?
  - Is your staff actively monitoring voice-specific security sites to understand emerging threats?
  - Do your supporting systems give you adequate visibility into “what’s going on?”
- **(Often) Network staff fails to treat voice with appropriate care and concern from users’ perspective**
- **(Often) Voice staff will want to “overprotect” voice traffic on the converged network**



## Things Not to Miss

- **When evaluating security systems and deployment**
  - Evaluate processing delays that create additional latency
  - Bias your selection towards solutions that react to QoS settings to minimize jitter
  - Ensure throughput supported by the device matches demand and system placement
  - Verify that the deployment does not overwhelm the security system capabilities
- **Carefully evaluate throughput relative to placement**
  - Verify that the device will not create a bottleneck
  - Ensure that traffic inspected will not exceed processing capability under normal or peak operations
  - Know the methods used to measure device performance



## Threats to be Aware Of

- **DHCP Starvation: (Un)Intentional allocation of all available IP addresses for one or more segments**
  - Phones and/or desktops cannot obtain addresses
  - May be caused by “rogue” router or access point
  - Can your switches/devices detect and address?
- **Spam over Internet Telephony (SPIT): Limited security issues (so far) but consumes bandwidth and resources**
- **Class of Service/Rate limit abuse**
  - (Un)Intentional “upgrading” of traffic to higher QoS setting
  - Can create quality issues for valid traffic
  - May result in DoS with sufficient traffic
  - Often unintentional due to changes to switches/routers



## Threats to be Aware Of (continued...)

- **Unauthorized phones**
  - Can anyone with a SIP handset make calls on your network?
  - Can anyone with a SIP handset appear to be a legitimate user for internal calls?
- **Viruses and Trojans**
  - None for handsets (as of yet)
  - Could compromise Softphones
  - Largest current threat is DoS
- **Unauthorized access to call processing servers**
  - Are you vulnerable to DoS here?
  - What connections should be explicitly allowed?
  - Are you alerted in the event of unauthorized access attempts?



## First Major Exploit of IP Telephony Reported

- **In June of 2006, two men arrested by the FBI and charges filed in New Jersey**
- **IP Telephony carrier hacked through brute force**
  - Hacker stole valid dialing prefixes
  - Provided prefixes to accomplice
  - Accomplice used prefixes to deliver traffic to carrier network
- **Exploit used to wholesale voice minutes to third parties**
- **Intermediate systems hacked to disguise actual source of traffic from carrier**
  - Workstations, Servers, and Routers



## What Can an Enterprise Learn From This?

- **While this exploit is more focused on carrier networks, there are “lessons” for the enterprise**
  - Encrypt call signaling traffic (with a quality algorithm)
  - Make sure you can detect suspicious flows
  - Make sure you are alerted to suspicious flows
  - Check your logs and configurations frequently
  - Be suspicious of all traffic to or from unknown hosts
- **Best practices would have helped (a lot)...**
  - Network devices not configured properly
  - Network devices not patched properly
  - Auditing bills would have speeded detection
- **Best practices have to cover both data and voice**



## “Defense in Depth”

- **Firewall at the internet access point is not enough**
  - Firewalls now secure multiple zones within a network
  - IDS/IPS systems seeing larger deployments
  - Internal threats recognized as significant exposures
- **Organizations must deploy technology and training to provide appropriate security**
  - Authenticated network access
  - Access restrictions by zone, segment, VLAN, system
  - More intelligent logging, reporting, and analysis
- **Look for “good” places to deploy security technologies**
  - Typically at aggregation points where flows converge
  - Be aware of issues caused by asymmetric routes/paths



## Mitigation Techniques

- **Is your firewall SIP aware?**
- **Can you completely segregate voice and data traffic into VLANs?**
  - Softphones can make this difficult or impossible
  - Integration of voice and data applications
  - Limiting voice access for authorized phones
- **Is your existing security posture sufficient?**
  - Default “deny all?”
  - Can you detect abnormal flows and port scans?
  - Have you examined your security policies and procedures with IP Telephony specifically in mind?
- **How will SIP trunking impact your security?**
  - This could be carrier specific
- **How will you handle VPN or internet-based VoIP?**



## “Proactive” Mitigation

- **Where required, deploy “voice aware” firewalls**
  - Prevents ports remaining open longer than required
  - Provides more granular examination of voice streams for identified attacks
  - Designed to meet specific requirements of voice
  - Do you need one firewall for converged traffic or two (one voice, one data)?
- **Ensure IDS/IPS provides the right alarms**
  - Voice-specific signatures
  - Traffic floods from one or more unknown hosts
  - “Unusual” traffic patterns
- **Examine and correlate log files**
  - Good tools available on the market today
  - If you don’t look then you can’t be sure you’re secure; set a regular schedule and stick to it (even with tools)



“Proactive”  
Mitigation  
(continued...)

- **Consider overall security posture**
  - Do you need 802.1x/Network Admission Control?
  - Can your phones authenticate to the network for admission?
  - Is your antivirus/personal firewall update process working effectively?
- **Encrypt where appropriate and possible**
  - Particularly signaling
- **Ensure encryption is sufficiently strong**
- **Train users to be aware of security**
- **Make it easy to for users to report security problems**



## Be Smart About Calls

- **Review your phone bills and CDR's**
  - IP Telephony does not eliminate the potential for fraud
  - Standard fraud prevention measures may alert you to holes in your perimeter
  - Adjust dialing rules to limit or eliminate unauthorized calling
  - Audit, audit, audit...
- **Think very carefully about acceptable sources of calls and implement rules/technologies to enforce**
  - Connecting to partners over a VPN?
  - Connecting to carriers over IP network?
  - Connecting via the internet?



## Protect Critical Services

- **Network devices should...**
  - Detect “rogue” DHCP servers
  - Limit number of hosts/port
  - Enforce rate limits appropriately (at wire speed)
  - Refuse participation in routing protocols with unknown hosts
  - Prevent “rogue” switches from participating in spanning tree
  - Alert on changes to critical topologies (routing, spanning tree)
- **Monitoring tools should...**
  - Test DNS resolution to detect unauthorized or unintended changes
  - Test DNS resolution to detect “zone hijacking”
  - Regularly verify availability of core servers and services
  - Preferably provide more details than “up/down” status for event correlation



## Regularly Assess Vulnerability

- **View security as a process; not a technology**
  - Threats evolve, change, and grow
  - Some “bad guys” are more focused on exploits that can make them money versus doing damage
  - Deploying devices and “walking away” will eventually result in exposures
- **Get into the practice of regularly examining your network for exposures**
  - Port mapping tools
  - Scripts and processes found on internet
  - Focused testing when exploits are reported
  - Outside parties when appropriate
- **Check for the “tried and true” methods**



## Don't Forget the Basics...

- **Apply standard toll fraud procedures**
  - Limit dialing plans according to roles and need
  - Require accounting codes for calls from “public” phones
  - Train users to avoid transfers to outside lines
  - Regularly review call details and audit bills
- **Carefully consider phones for public areas**
  - Can an analog or digital set suffice?
  - Check-in/check-out of speaker phones for conference rooms
- **Limit access to public ports**
  - Don't allow access to voice VLAN from publicly accessible network ports
  - Examine use of 802.1x, NAC, Guest portals
- **Merge with IT Security best practices**



## Things to Demand From Your PBX

- **Ability to encrypt streams**
  - Call signaling
  - Bearer traffic
  - Encryption should preserve Quality of Service settings
- **Two-way authentication**
  - IP PBX systems usually can authenticate endpoints
  - Can the endpoint authenticate the IP PBX?
- **Ability to detect and refuse common exploits**
  - DoS attacks
  - “Brute force” exploits
  - Some “man-in-the-middle” exploits
- **Support for certificates or similar PKI**



## If You're Going Outside "Your Network"

- **Require encryption using strong protocols for signaling and bearer traffic**
- **Demand network connections that are worthy of trust**
  - Endpoint to endpoint encryption
  - Encrypted tunnels between known (trusted) hosts
  - Remote access technologies that comply with best practices and security policies
- **Enhance your ability to view traffic streams and detect improper communications at network boundaries**
- **Ensure that firewalls and other devices/systems are "voice aware"**
- **Verify that the network design and encryption employed allow for preservation (and use) of QoS**



## Where to Go

- **SANS – SysAdmin, Audit, Network, Security Institute**  
<http://www.sans.org>
- **“Security Considerations for VoIP Systems”**  
<http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf>
- **ISSA – International Systems Security Association**  
<http://www.issa.org>
- **CERT – Computer Emergency Response Team**  
<http://www.cert.org>
- **Voice over IP Online Resource Guide**  
<http://www.networkworld.com/resources/voip055>
- **VOIPSA – Voice over IP Security Alliance**  
<http://www.voipsa.org>
- **NIST Computer Security Resource Center**  
<http://csrc.nist.gov>



## Lessons Learned

- **Updating security posture for convergence is a requirement**
  - Usually a critical service with high visibility
  - Voice-specific exploits have been identified
  - Any new application demands examination of rules, systems, and deployment
- **Don't let IP Telephony cost you real money**
  - Bad security could result in calls made by unauthorized parties “on your nickel”
  - Bad security could cause your organization to become an “unwitting accomplice”
  - Bad security could create service impacts that make voice communications difficult or impossible
- **Continually examine overall posture, policies, and procedures; be ready to quickly adjust**



## Good Security Gone Bad

- **Customer deployed IP Telephony and upgraded network hardware for multiple organizations**
  - One district office
  - Two affiliated campuses
  - Two distinct locations
  - Three different support staffs
- **Network architecture certified viable by manufacturer; including the firewall placement and capabilities**
- **When security was enabled the network crashed on a regular basis**
  - Traffic loads through the firewalls exceeded processing capacity
  - Firewalls participating in routing protocols caused invalid routes, route flaps, overall failure of routing process
  - Firewall placement and configuration required inspection of excessive traffic relative to security policy
- **Voice and Data network were unstable**
  - Required network redesign and hardware replacement