

PROTECTION FOR VoIP VULNERABILITIES

Everyone knows that Voice-over-IP (VoIP) has been experiencing rapid growth. Even still, you might be surprised to learn that:

- 10% of all voice traffic is *now* transmitted with VoIP technology (IDC)
- AT&T will have VoIP service available to the top 100 US markets by the end of the first quarter 2004 (AT&T)
- It is estimated that 7 million IP Phones will be in circulation by 2007 (InStat/MDR)

The Problem (or at least the one most recently identified)

The mass deployment of this new technology also brings along with it many challenges – one area being the security of your network. “Because IP networks are subject to sophisticated, automated attacks, voice traffic on those networks is more vulnerable” says David Fraley, author of “Cyberwarfare: VoIP and Convergence Increase Vulnerability”. In fact, the U.K.’s National Infrastructure Coordination Centre (NICC) recently released findings (<http://www.uniras.gov.uk/vuls/2004/006489/h323.htm>) that equipment from many vendors who have implemented the H.323 protocol standard for IP Telephony contains flaws that can be exploited by attackers. According to tests commissioned by NICC, these vulnerabilities can leave products open to:

- Denial-of-Service (DoS) attacks
- Buffer-overflow attacks
- Insertion of malicious code into the compromised equipment

According to CERT Advisory CA-2004-01 (<http://www.cert.org/advisories/CA-2004-01.html>), companies affected by these vulnerabilities include:

- | | | |
|--------------|--------------|-----------|
| • Cisco | • Secure | • Extreme |
| • CheckPoint | • Computing | • Foundry |
| • Netscreen | • Cyberguard | • Fujitsu |
| • Nokia | • Symantec | • Hitachi |
| • Microsoft | • Stonesoft | • Intel |
| • Nortel | • WatchGuard | • Juniper |
| • Avaya | • 3COM | • NEC |
| • Alcatel | • AT&T | |
| • F5 | • D-Link | |

As just one example, Cisco alone has many products that contain vulnerabilities in the processing of H.323 messages (<http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml#process>):

- All Cisco products that run Cisco IOS software and support H.323 packet processing
- IOS Firewall
- IOS Network Address Translation
- Call Manager
- Conference Connection
- 7905 IP Phone
- BTS 10200 Softswitch
- Internet Service Node
- H.323 Gateway, H.323 Gatekeeper
- ATA18x Series Analog Telephony Devices

In some cases, Cisco does not plan to fix the vulnerabilities that have been identified.

CERT Recommendations

Carnegie Mellon University operates the CERT Coordination Center, which is a major reporting center for Internet security problems. CERT was founded by the Defense Advanced Research Projects Agency (DARPA) and they provide technical advice and coordinate responses to security compromises, identify trends in intruder activity, work with other security experts to identify solutions to security problems, and disseminate information to the broad community. The CERT/CC also analyzes product vulnerabilities, publishes technical documents, and presents training courses.

In the CERT Advisory referenced above, recommendations are issued to help companies protect their networks from these vulnerabilities. Among their recommendations are the following:

1. Block access to H.323 services on devices that do not need to be exposed
2. Limit access to only those machines that use H.323 for critical business functions, and limit access of any type to only those areas of the network where they are needed
3. Consider disabling application-layer inspection of H.323 packets by Firewalls
4. Coordinate among telephony, application, network, and desktop staff to assess the threat in individual network segments

How Ranch Networks Can Help With This Problem

Ranch Networks products provide multiple layers of security and many performance-enhancing functions in a single, low-cost device. These products were designed to easily overlay on top of your existing network, without requiring the reconfiguration of your current network infrastructure. This combination of security and performance capabilities integrated into a single, low-cost device is unparalleled in the industry.

CERT Recommendations 1 and 2 above state that special security precautions should be taken with devices that support H.323 interfaces, furthermore H.323 devices should be protected and separated from the non-H.323 devices to lower the risk of attack. Due to Ranch's Secure Virtual Zones, our products are designed to solve the problem of internal security by seamlessly enhancing your existing network.

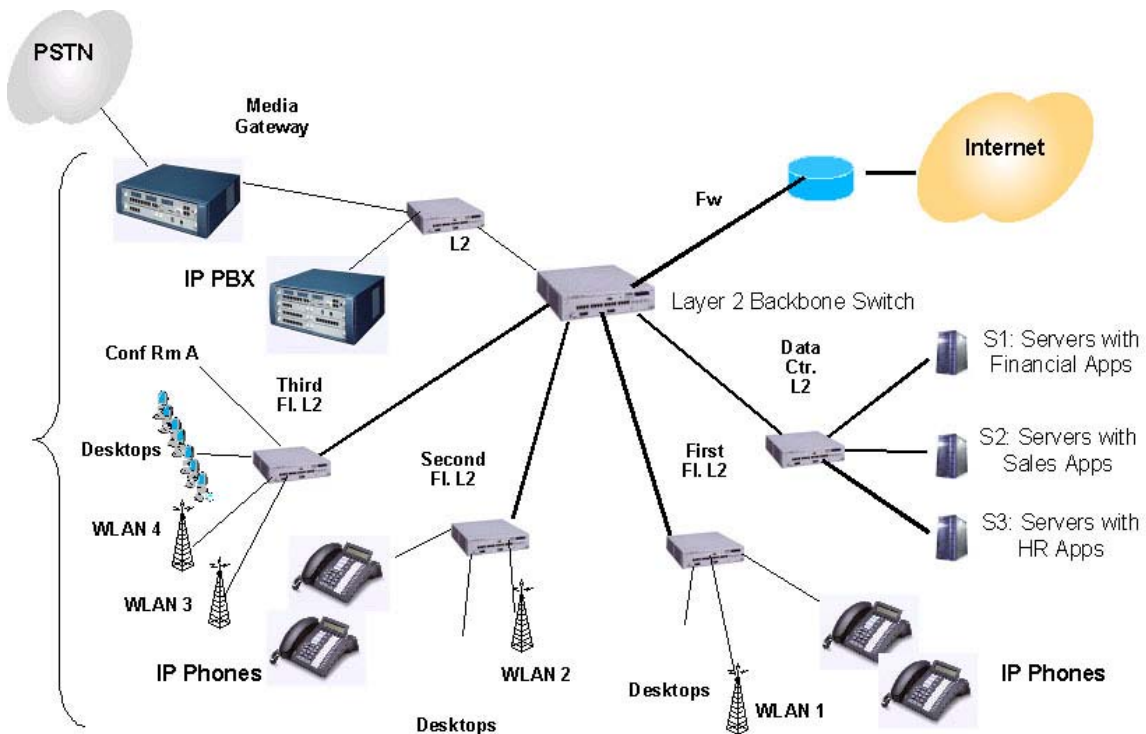


Figure 1 – Converged Enterprise LAN with IP PBX

Figure 1 shows a typical IP PBX installation where a single LAN infrastructure is used for both voice and data. This office has a Perimeter Firewall, a Layer 2 Backbone Switch, a Data Center, an IP PBX, and IP Phones sprinkled throughout the LAN, intermixed with Desktops, Wireless LAN Access Points, and other network devices.

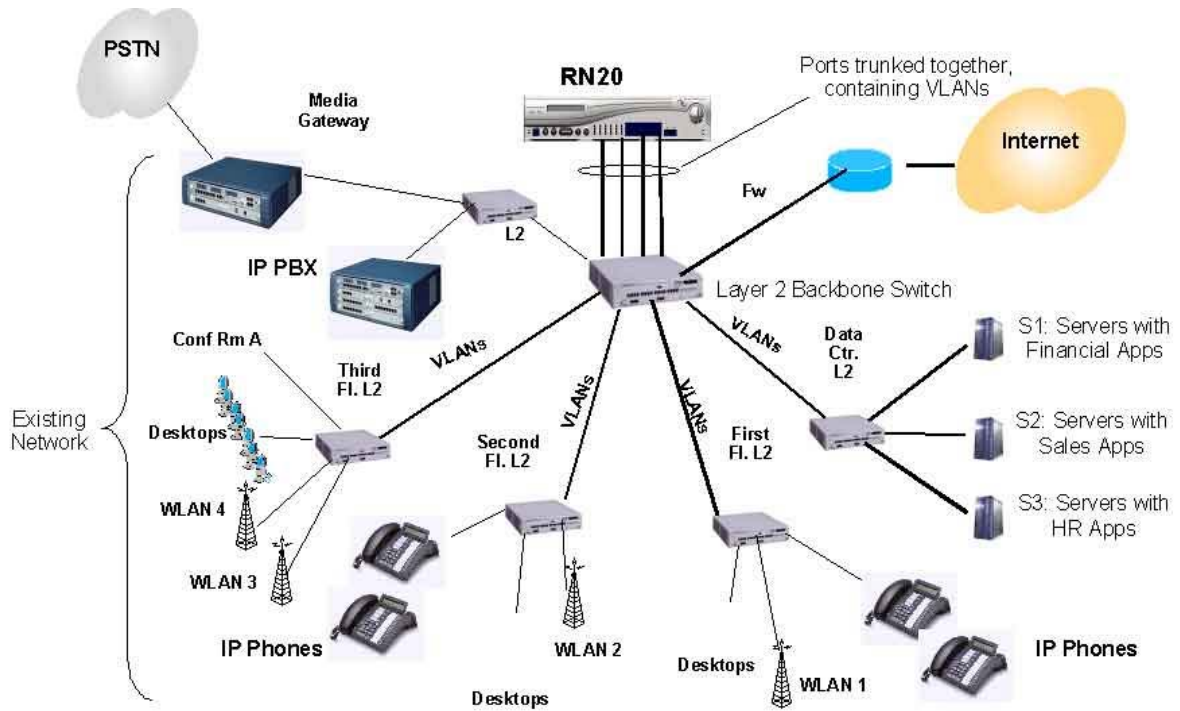


Figure 2 – Converged LAN with Ranch security overlay

As illustrated in Figure 2, a Ranch Networks product can be added as an overlay on this network to provide many security and performance-enhancing functions. The existing network can be subdivided into logical segments by using VLANs. The VLANs are brought back to the Ranch product, where they can be grouped into Secure Virtual Zones, each of which represents an “area of trust” within the network. So for instance, the LAN can be divided according to various parameters such as organizational structure, voice vs. data, and guest areas vs. non-guest areas. The table below describes one approach for how the example network might be divided.

Zone Number	Zone Description
1	IP Hard Phones and Soft Phones
2	IP PBX and Media Gateway
3	Wireless LAN Access Point & Conference Rooms
4	Internet
5	Accounting Desktops
6	Accounting Servers/Applications
7	Sales and Admin Desktops
8	Sales Servers/Applications
9	Human Resources Desktops
10	Human Resources Servers/Applications

So what has this accomplished relative to CERT Recommendations 1 and 2? First, H.323 devices, such as the IP Phones, are not exposed to the outside world. In fact, they are only exposed to the other devices with which they must communicate. Second, since all of the voice products have been segmented into their own Secure Virtual Zone, different security policies can be implemented for voice devices vs. data (non-voice) devices. One example of a policy unique to the voice zone is that it is necessary to leave TCP ports open for H.323 to perform call set-up between the various voice devices. Similarly it is necessary to leave UDP ports open for the media stream traffic on voice devices - more on this below. Correspondingly, voice ports for data devices, or any non-voice device, would be blocked. The segmentation of the network provided by Ranch allows this to be easily accomplished. As a result, H.323 ports are open only where absolutely necessary, and only to other devices meeting these same criteria.

What about CERT Recommendation #3 – to disable application-layer inspection of H.323 packets by Firewalls? To understand the implications of this recommendation lets first review why some Firewalls inspect H.323 messages in the first place. In IP Telephony, call set-up messages are separated from, and handled differently than, the media streams that actually carry the voice conversation. Call set-up messages typically use only a single port (although this may vary by vendor), just like data services (for instance, HTTP's use of port 80). However the VoIP media streams generally use port numbers across a wide range (dynamically assigned) – since there can be many simultaneous streams. The specific ports that will be used for the media streams vary on a call-by-call basis and therefore cannot be secured with a static firewall rule.

Given this uncertainty, how do the media streams get through a Firewall? In today's networks, one of two approaches are typically used: (1) the range of potential IP addresses & protocol port combinations are left open *permanently*, leaving a huge gaping security hole, or (2) the Firewall uses application-layer inspection of the call set-up messages in an attempt to discern which IP addresses & protocol port combinations to allow so that a call may pass through the firewall. *This is precisely the function that CERT is now recommending to be disabled.* With this second alternative unavailable, Network Administrators face a choice between leaving the ports open permanently or shutting off VoIP traffic into their LAN entirely.....

There is however a third alternative that effectively solves the dilemma – install a Ranch Networks device as shown in Figure 2. Rather than employing application-layer inspection at the firewall to open and close ports, Ranch takes a different approach, which is to receive SNMP messages from the IP PBX – the very device that should be controlling where and when calls are to be placed and terminated. The SNMP messages instruct the Ranch unit to open and close the ports corresponding to the beginning and end of each phone call. In addition to solving the recently identified H.323 vulnerability, the Ranch approach has other advantages.

Some of Ranch Networks advantages are:

- It is not necessary for the Ranch Firewalls to understand the myriad versions of signaling protocols and proprietary extensions used by various IP Telephony vendors.
- It is not necessary for the Ranch Firewalls to be modified in the field every time one of the IP Telephony vendors changes their proprietary extensions.
- Firewall performance is superior with the Ranch approach since it is not slowed down by application-layer protocol inspection
- IP PBX's implement complex call control algorithms, which are influenced by features such as multi-party conferencing and third-party call control. Tracking call state in this environment can be complex and difficult. A PBX is specifically designed to do this whereas a Firewall is not. If call state tracking is not performed properly, calls can be dropped mid-stream. The application-layer approach suffers from this problem whereas the Ranch approach does not.

Additional Benefits of the Ranch Solution

In addition to the above benefits, Ranch products also provide many other valuable capabilities. Our security capabilities include:

- The LAN is subdivided into multiple Secure Zones with each Secure Zone having its own independent security policies. The RN20 provides up to 12 Secure Zones, with separate Firewalls between each pair of Zones in both directions. A full range of NAT options is available.
- Separate Zones for Voice and Data
- Denial of Service protection is provided between each pair of Secure Zones.
- Authentication can be enabled so that it is required to enter or exit a Secure Zone. This means that no packets from a user will be allowed through the Ranch device until the user first enters their Username and Password. Once the user is authenticated, they are then permitted to only enter those areas of the network to which they have been authorized. This enables a **Single-Sign-On** approach: once the user is authenticated by the Ranch device, they can be allowed access to those applications to which they are permitted – without further sign-on if desired.
- Security breaches can be automatically or manually isolated and quarantined within a Zone.
- Wireless LANs can be separated into their own Zone, with stricter security policies applied to this Zone.
- Network hiding is provided between each pair of Secure Zones
- Rate limiting and port mirroring can be configured for any Zone.
- Security based on MAC addresses
- Outgoing connections and port scans from a Zone can be denied
- Low latency and high throughput

In addition to security functions, Ranch products include the following non-security capabilities:

- Overlay without reconfiguration - Ranch products can be added as an overlay to upgrade an existing LAN without needing to (1) rewire the LAN to achieve Secure Zones, or (2) reconfigure IP addresses.
- Quality of Service
 - Bandwidth Management / Traffic Shaping - Guaranteed, minimum, maximum, and burst bandwidth can be allocated based upon Source or Destination Zone, IP address (or range), MAC address, or Port number (or range). Thus it is possible to prioritize traffic on a per-user or per-application basis.
 - Full support for end-to-end QoS can be provided by (1) setting TOS or DiffServ priority for outgoing traffic and (2) classification and prioritization of incoming traffic based on TOS or DiffServ.
- Health Monitoring - Any device with a reachable IP address, within the LAN or elsewhere, can be monitored via:
 - ICMP ping verification (Layer 3)
 - TCP connection verification (Layer 4)
 - Link monitoring (Layer 2)
 - Web (HTTP) and FTP servers can also be monitored at Layer 7
 - An HTTP server can be requested to perform a database query into another server. If this database query is not successful an alarm will be sent.
- Server Load Balancing
- Multicasting and Switching
- Accounting
- Remote Management

Summary

Converged networks are complex and drive the need for increased security and performance requirements. New security vulnerabilities in complex VoIP equipment will continue to be found. The power, low cost, and flexibility of Ranch Networks products make them the ideal choice for mitigating these risks.