IP Technology Labs

Always Connected™

Always Connected.

The Most Reliable & Cost-Effective way to Securely Connect your Remote Networks, IoT/M2M devices, & Cloud Applications

Agenda

IP Technology Labs

Who we are
Background

3 Market Forces
The Difficult Problem <u>Only</u> We Solve

IpTL's Unfair Advantage
Our Secret Sauce

Reference Applications

IP Technology Labs

Always Connected™

FastLane™ VPN Tunneling gateways provide the **most reliable, cost-effective** way to **use any Internet** to securely **connect** your **remote IoT/M2M** devices and applications site-to-site.

We Design & Manufacture IP/Ethernet Appliances

Founded in 2009, HQ Baltimore, Maryland USA

Technology: Patents, Trade Secrets, Know-How

We do it: Engg, Manufacturing, & Logistics

Over 100+ Years in Access Networking Design

Global from the start – used in 71+ countries

7,300+ end points across every industry

Go to Market: Sell globally – Support locally

Three Market Forces – The Network has Left the Building
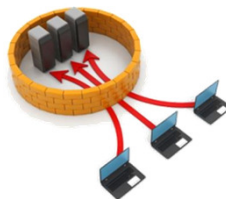
Social Forces
(emerging behavior)

Economic Forces
(financial impact)

Technology Forces
(persistent evolution)

- Devices, Apps, Users are Mobile and no longer "tied" to the office

- Internet is cheap and available
- Apps moving to the Cloud
- MPLS $$$. VPN's don't work
- All are in-secure

- Aggressive provider filtering
- Connectivity breaks networking *Dynamic IP, NAT's, Firewalls*
- No Printers in the Cloud!

What is So Hard about Networking IoT/M2M Devices & Apps

Connectivity lags behind performance innovation

Fragmented, one-off, siloed implementations

Devices & Apps always "assume" connectivity

1st wave was compute;
2nd wave was storage;
3rd wave is **?????**
(put the latest hyped-TLA of the day here: SDN? NFV? NB-IOT? Web App?)

FAIL miserably when they don't have Access IoT/M2M devices aren't WAN enabled

Security is an afterthought and weak

Links are aggressively blocked
IPsec is broke

Devices aren't Web apps
Cloud access is unsupported

5 Facts About IpTL FastLane Appliances You Should Know

When connecting **remote IoT/M2M devices** to your datacenter or cloud

IpTL's FastLane Gateways <u>gives</u> you the most

1 **Absolutely Reliable Links**

2 **Secure Edge-to-Edge networking**

3 **Cost-Saving – Opex & Capex!**

For all your devices, apps, & sites **over any Internet** connectivity

- Works with Dynamic IP/DHCP networks

- Secure and automatic redundant connectivity over multipath

- Fully transparent end-to-end networking. Open-sky for your apps

- IpTL gives your Cloud Virtual Applications seamless and truly secure access without blocks or hassles or "provider" dictated VPN's

- Out-of-the-Box Strong Security

IpTL's Unfair Advantage – Our Secret Sauce

We work were others can't - *Not a VPN*

We tightly integrate the **3 most important** elements of successful remote access networking into our appliances

- Advanced Path, Packet, & Content switching

- Automatic Transparent, Hidden, & Secure Tunneling

- Seamless L2 & L3 Network and Element Integration

only IpTL Has…

AutoConnect™

RealTimeResouce™

SystemMonitor™

HotelApp™ **Captive Portal** ™

DHCPMangling™

BlackNoise™

IPshare™

FastLink™

FlexPath™

Dynamic Path-switching Algorithms	→	Endpoint Tunneling Services	→	Access Connectivity Technologies

IP Technology Labs

Scalable 1 to 1,000 of Networks- Endpoint, Server, & Virtuals

	Wired+Wi-Fi	Cellular LTE			Virtual
Mobility	Workgroup	M2M/DR-BC	Networking	Access+	Cloud / DC
	1 Tunnel →		1-12 Tunnels	1-25 Tunnels	1,000's Tunnels

Model 7   **Model 7111**   **Model 7151**   **Model 7501**   **Model 770**   **Model 79R**

1U Rack Mount
- 1U form Factor
- 1,000's of users
- 6x GigE ports

Hi-Performance Remote Site
- 1-12 Connections
- IP Camera Backhaul
- VoIP/UC Connectivity

4X GiG Aggregator
- 1-25 Connections
- Connections are license scalable
- Office VoIP UC
- Expandable for additional sites

Wi-Fi + Wired Eth
- Single User
- USB for power
- Multi Device Support

Wi-Fi + Wired Eth.
- 802.11 b/g/n
- Target 100 Users/Devices
- Single Tunnel Lic expandable

LTE + Wi-Fi + Wired Ethernet
- Integrated LTE
- Internet Access
- Auto Backup Failover
- All ports can be used for tunnels

Model 70v
- VMWare ESXi
- Amazon AWS AMI
- Virtual Box
- Hyper-V/Azure

Users

IpTL Hardware Appliance

Applications

Devices

Multiple Redundant links

IpTL Model 79R or Virtual 70x Secure Access Servers (redundant)

One or More LANs

WWW

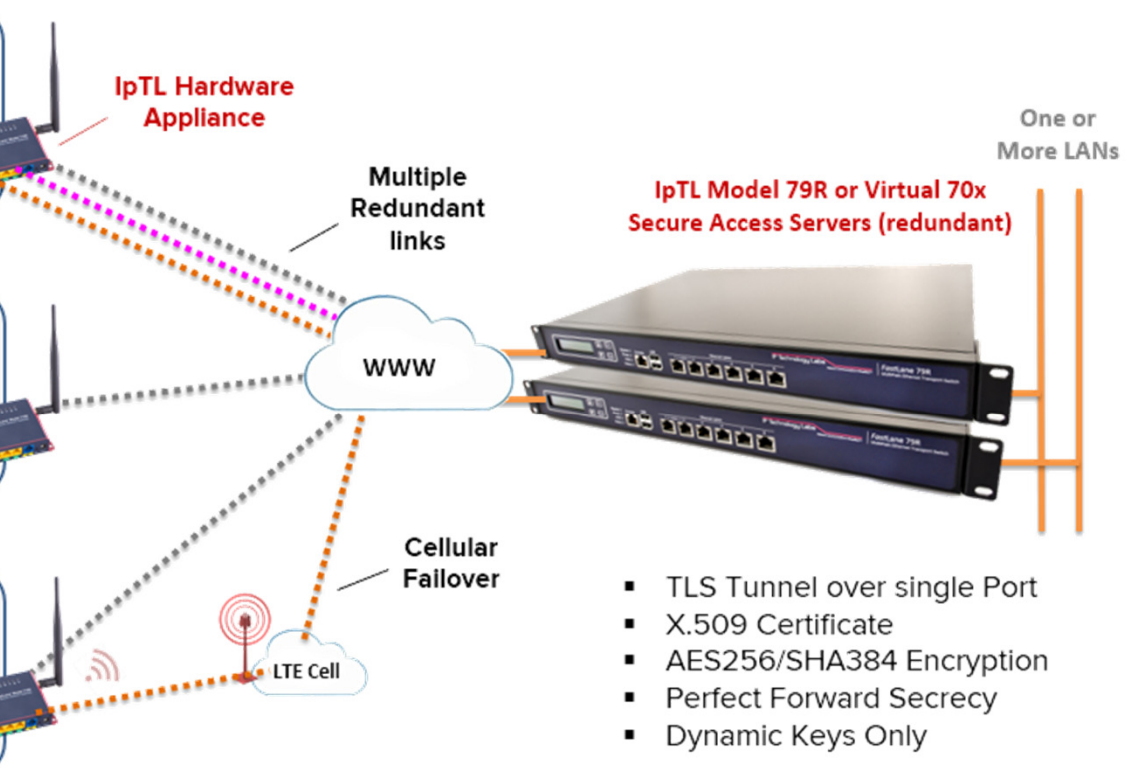Cellular Failover

LTE Cell

- TLS Tunnel over single Port
- X.509 Certificate
- AES256/SHA384 Encryption
- Perfect Forward Secrecy
- Dynamic Keys Only

Secure & Private Ethernet-to-Ethernet Connection

IP Technology Labs

9

About IpTL *Fast*Lane™ Appliances – Quick Snapshot

- CE Mark, FCC, Canada, AUZ/NZ, UAE & Oman TRA certified
- **Works with Dynamic IP** – even on <u>both</u> ends of the link
- Can be installed <u>behind</u> a NAT on both ends
- Supports VLANs and VLAN trunking over IP networks
- **Data <u>always</u> goes between your devices**
- You can implement <u>your own security</u> & lock-down
- Client Independent - No software installed
- You can deploy with <u>100% Touchless</u> deployment
- Not a service –You create your own link
- No recurring feature licenses
- **All endpoints are locally and remotely <u>manageable</u>**
- Designed, built, and shipped from the USA

Telecom Equipment Registration Certificate

Testimonials

"I just want to say "THANK YOU". Today I ran over 30 concurrent calls over tunnel and it worked perfect without any lag and issue. - Amir, VoipLeaders

"Tunnel is solid! no issues at all." - Sandeep, Dragon Oil

"Very Clever! ...the system worked without any glitches."
- Diaa, Honeywell

"an excellent product at a very attractive price level." - Amer, Sony Dist

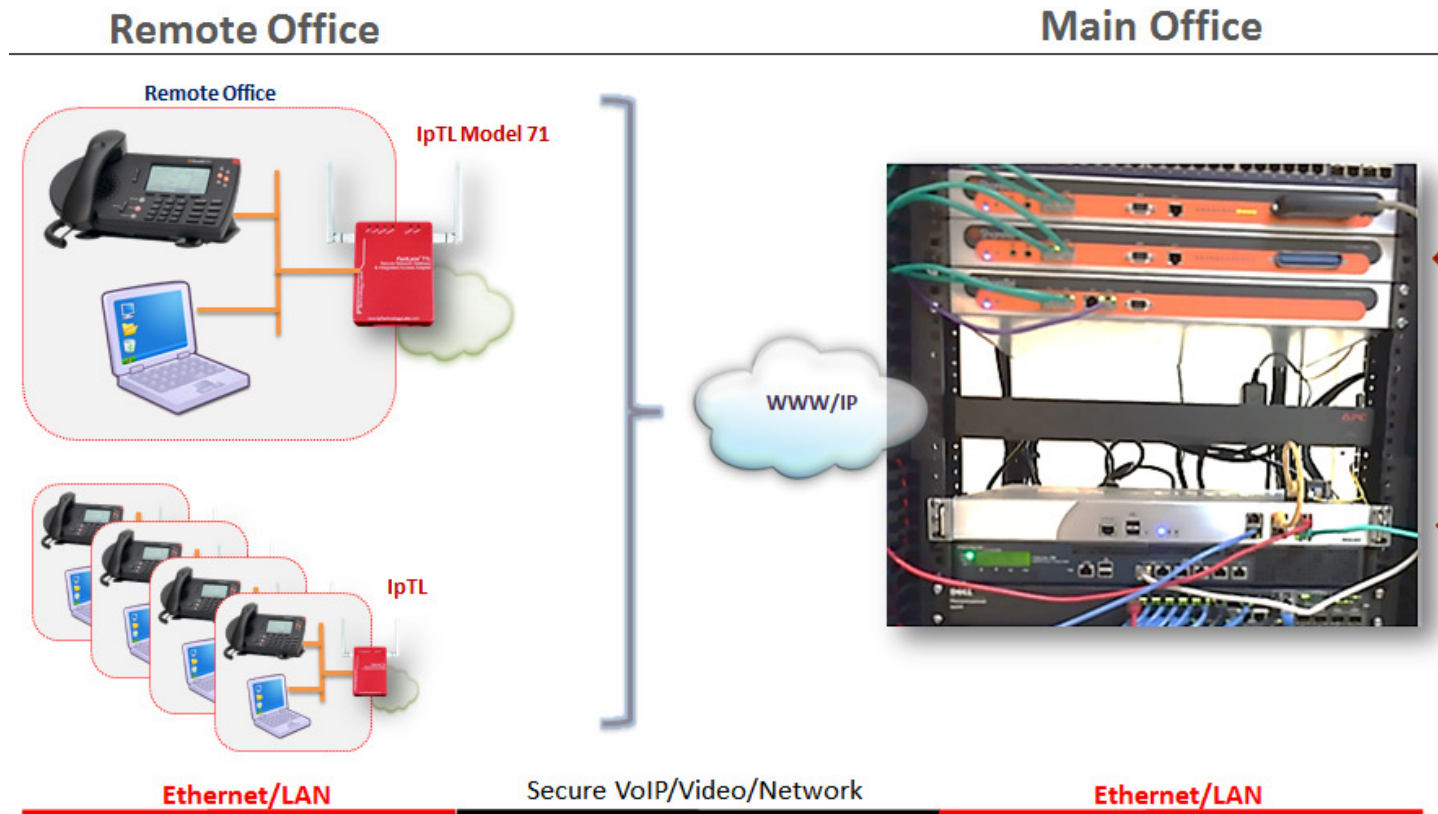"Saved the Day-- Your redundancy kicked-in twice when I was on holiday."
- Dr. Robin, Veterinary Clinics

AVAYA

G4S

du

Honeywell

HSC Health and Social Care in Northern Ireland

GHENT UNIVERSITY

Dragon Oil

MOTOROLA

FORTUNE
ENGINEERING & ENERGY SERVICES

YMCA

GENERAL DYNAMICS

Remote Office

Main Office

Remote Office

IpTL Model 71

WWW/IP

IpTL

Ethernet/LAN   Secure VoIP/Video/Network   **Ethernet/LAN**

IpTL provides a secure LAN based connection for remote VoIP and Data users without change to devices, applications, or process.

IP Technology Labs

Remote IP Camera Backhaul

Field Metering

LoRa/NB-IOT Mesh

SmartMeter
LoRa/NB-IOT

Eth

LTE IoT Gateway

Cellular

Cellular WAN
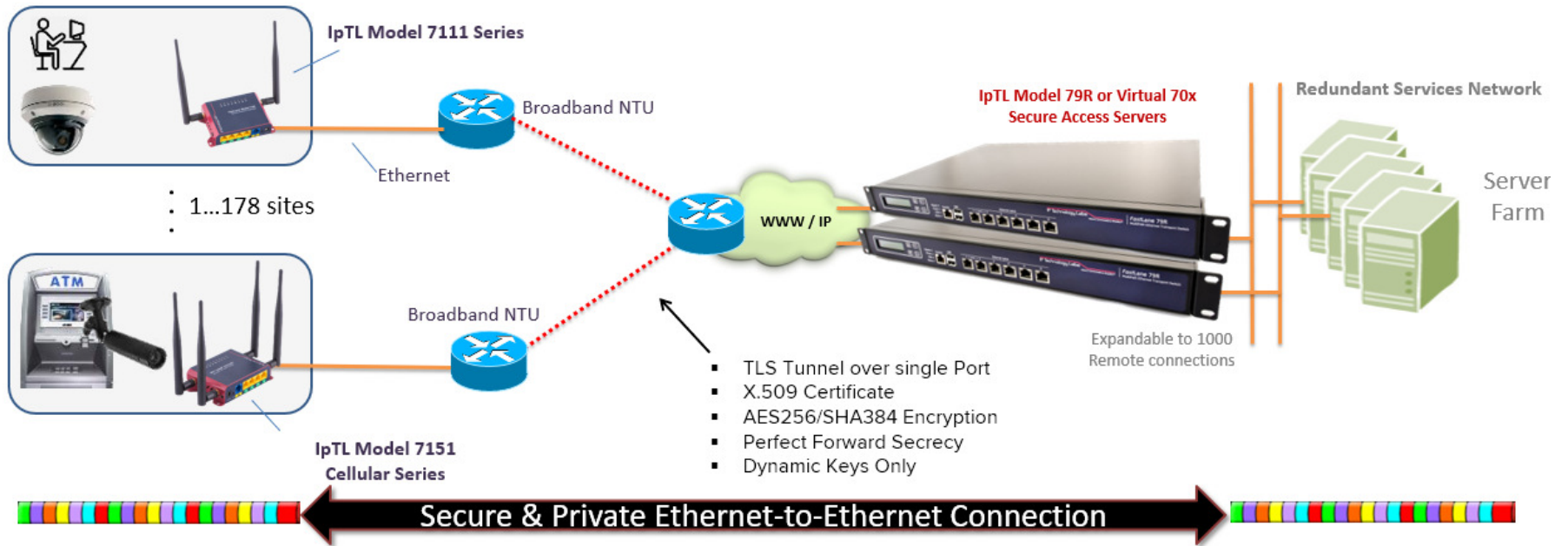
IpTL Model 7151
Secure IoT Gateway

Central Cloud Platform

Example VMWare Hypervisor

IpTL eGate 70v VM
(ESXi) (redundant)

70v

Other VM's
Applications

10.10.x.x/16

172.17.x.x/16

Customer Application
M2M Data

Secure & Private Ethernet or IP Tunnel Connection

Customer Application
M2M Data

- Secure TLSv1.2 Tunnel (ECDHE AES256GCM/SHA384)
- Perfect Forward Secrecy and X.509v3 Certificate security
- TLS Auth HMAC (locks TLS to units/Anti-DoS & Scanning)
- Dynamic TX/RX Key; Time & data triggered re-key
- DataPath Fingerprint Obfuscation (S3=Rolling XOR keycodes)

14

M2M PLC Integration – Industrial Water Monitoring

End-to-End Connections

Remote RAIN Sites

A8

MY 27

Site X

Secure End-To-End Data

RAIN Central Site

Data Acquisition, Conversion, &Push to RAIN WWW

RainMatters.org Web site
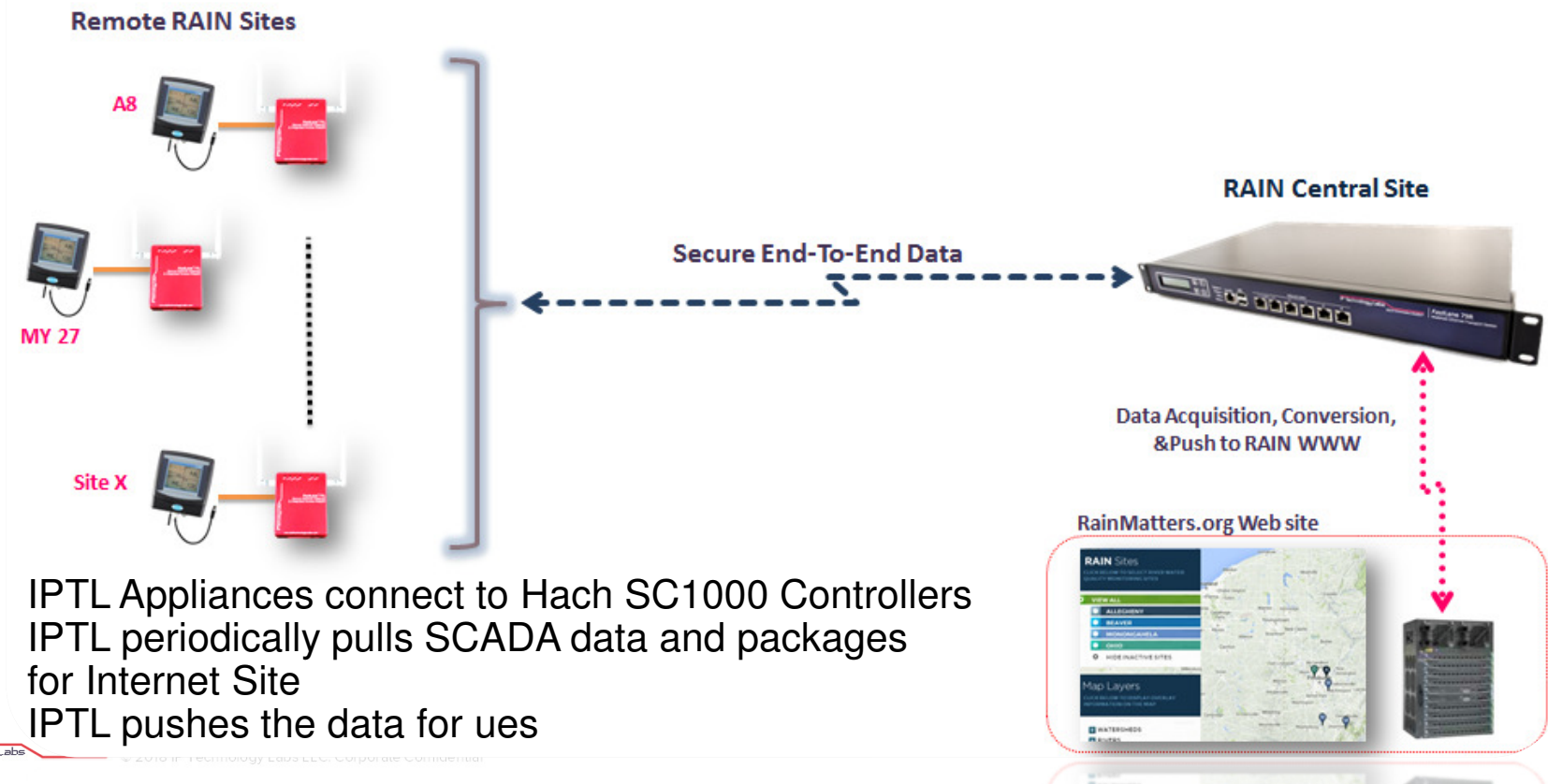
- IPTL Appliances connect to Hach SC1000 Controllers
- IPTL periodically pulls SCADA data and packages for Internet Site
- IPTL pushes the data for ues

Quick Case Study – M2M Access Control

Challenge
Consolidated Personnel Identity Management over large geographic location

- Construction site access control for 10,000 personnel growing to 120,000+ personnel in 9 months
- Personnel housed at 26+ different towns each run by a different contractor
- General datacom facilities not universally available, not standardized, or add large overhead expenses; many sites in "dark zones"

Solution
IpTL Model 71 with Integrated 3G Model for Secure & Redundant Connectivity

- IpTL solution provides transparent, redundant, and secure connectivity for Access Panels regardless of physical location or infrastructure
- Each remote location uses generic cellular data infrastructure from one or two Tier-1 Service providers
- Standardized solution without requiring modification to customer or contractor systems

Outcome
Efficient and low-cost Worksite, Personnel, & Operations Management

- Credentialed personnel are permitted/denied access to the work-site prior to approaching facility (workers are simply dropped off at the worksite)
- Consolidated IT infrastructure eliminates duplicate systems; is independent of contractor, housing site size or available communications infrastructure
- Honeywell solution scales as personnel requirements expand and contract with lowest-cost operational overhead
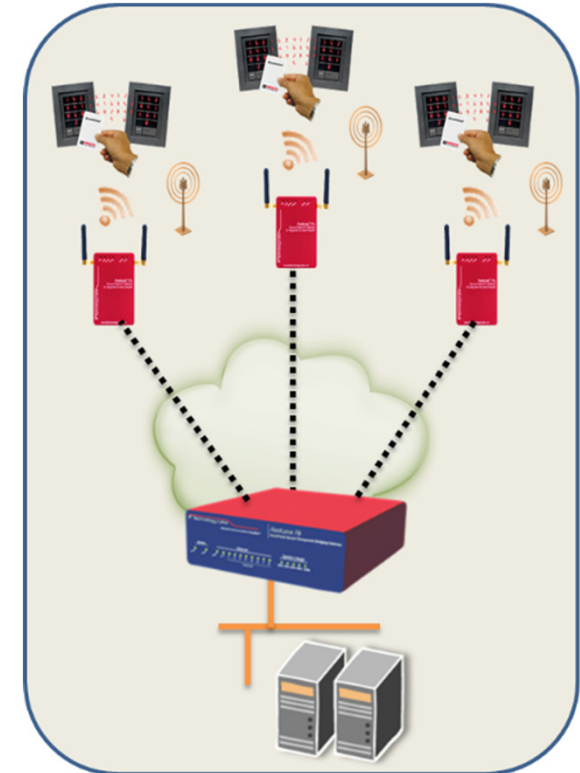
Hybrid Cloud Access – Physical Remotes to VPC

Remote Sites

Cloud

IpTL Model 7111

Broadband NTU

Ethernet

Remote sites

Broadband NTU

IpTL eGate 70v (ESXi)

70v

Other Customer VM's

192.168.0.2/16

example: 192.168.x.x/16
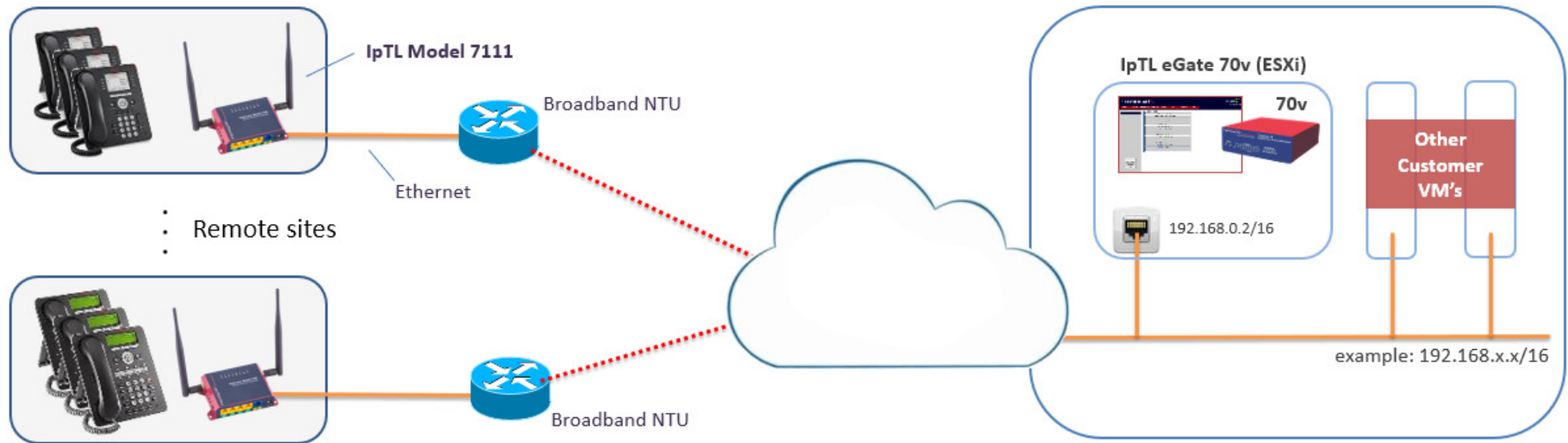
Physical Remotes

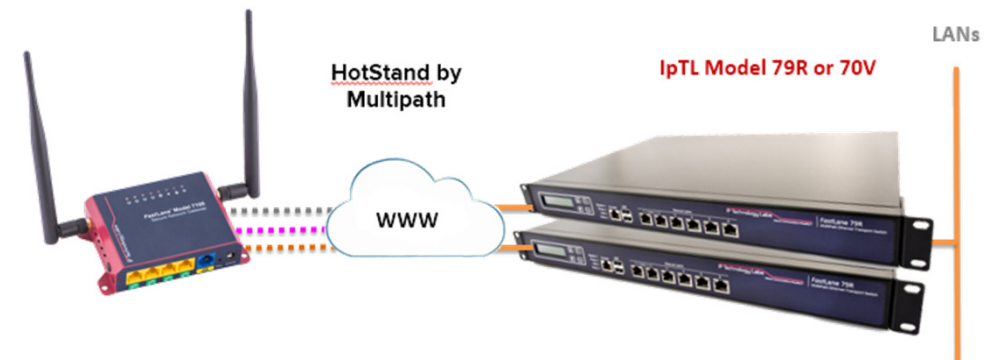**Cloud/Datacenter**

Secure & Private Ethernet-to-Ethernet Connection

Remote NON BLOCK TUNNEL BOND Multipath HotStandby

- **3 tunnel ports from remote**
  - 1201 UDP
  - 1200 UDP "S3" BlackNoise
  - 443 TCP "S1" BlackNoise

- **All Tunnels are UP**
  - Only one active at a time "Primary"

- **Automatic failover in order if Primary goes down**

- **Automatic restore back to primary**

- **ALL TRANSPARENT TO USER**

Active Tunnel Profiles

Remote:	Port:	Protocol:	Cipher:	Cipher Support:
1: 02-02-79-C_____	1201	UDP ▾	AES 256 bit CBC ▾	☐ S1 ☐ S2 ☐ S3
2: 02-02-79-01-__ _____	1200	UDP ▾	AES 256 bit CBC ▾	☐ S1 ☐ S2 ☑ S3
3: 02-02-79-01-__ _____	443	TCP ▾	AES 256 bit CBC ▾	☑ S1 ☐ S2 ☐ S3

HotStand by Multipath

IpTL Model 79R or 70V

LANs

WWW

IP Technology Labs

- Large concentration of remote users at the central site.

- When 100% guaranteed access to the central site is required.

- Protection from Link, Provider, & Equipment failure is required *at the same time*.

- Positive indication that the backup is available and active. (e.g. Hot Active) even when it is not being utilized.
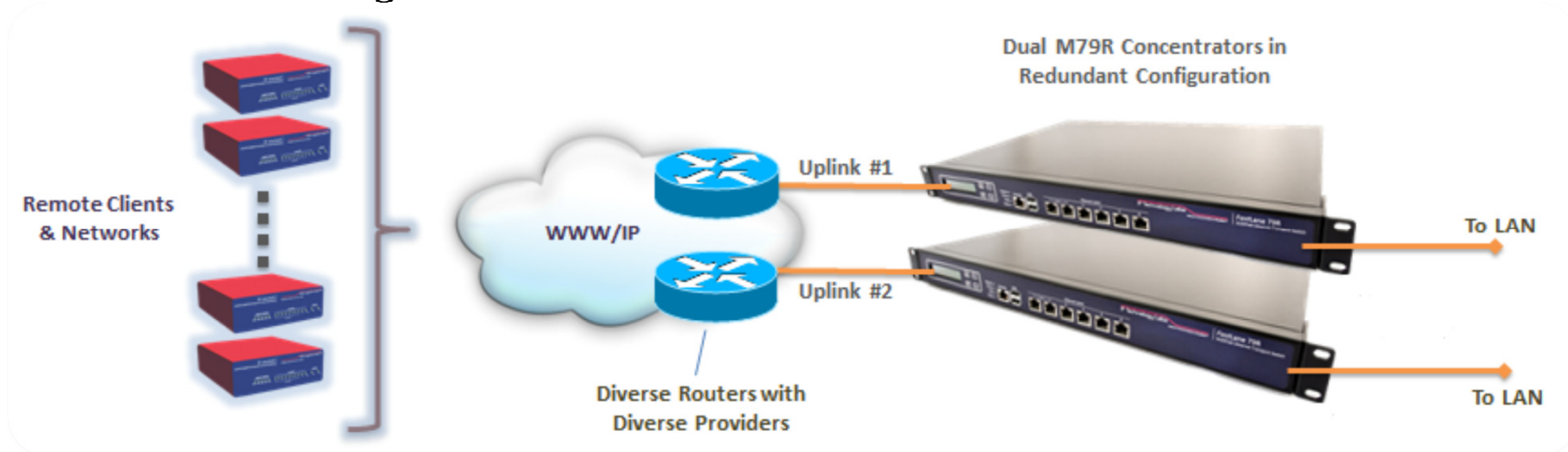
Leased Line Replacement

- Competitive carrier offering hosted Video conferencing needs easy and secure connectivity

- International connection over Commodity Internet

Solution Highlights

Challenge
- Provide remote access for users of hosted Polycom telepresence and conferencing regardless of location
- Video/UC blocked by NAT or country proxies – Traditional VPN didn't work due to dynamic IP
- MPLS or Leased-Lines expensive or not universally available
- Incomplete Security, Privacy & Control

Solution
- Redundant IpTL Model 79R servers in data center
- Model 75 end-points at remote sites.

Results
- Transparent and secure Ethernet from remote Video clients to hosted MCU service
- Plug-and-play quick deployment
- Use any Internet connection with no network, NAT, firewall or provider blockages. Works with Dynamic IP on both ends of the link – No Static Public IP required
- Full End-to-End manageability for quick support and provisioning.
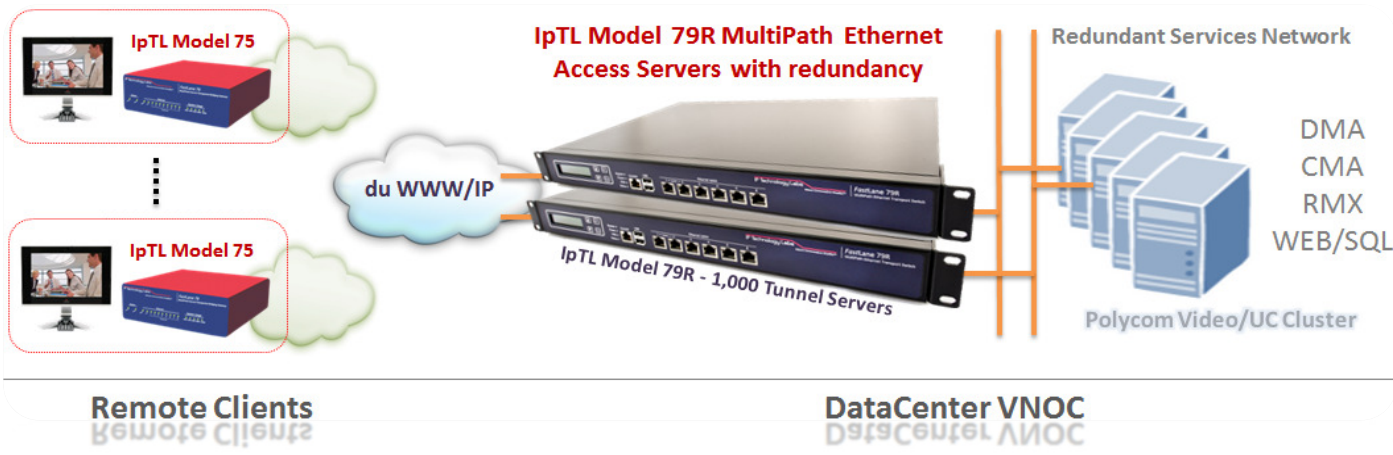
Price Performance Leader

Vendor ->	IpTL	Cisco Systems	SonicWALL	Telecom	Avaya
Solution ->	FastLane	ASA 5506-X	TZ/Soho	MPLS	ONA (Cloud only)
Total cost per link (25 link / 3 years) price	$667.18	$2,311.90	$698.86	$360,000.00	$3,345.00
Live Engineer Setup Support	Yes	No	No	No	No
Presales response within 1 hour	Yes	No	No	No	No
Postsales response within 1 hour	Yes	No	No	No	No
Full Proposal Creation on Request (presales/channel/customer)	Yes	No	No	No	No
Free Lifetime Software Updates	Yes	No	No	No	No
Custom OEM Opportunities	Yes	No	No	No	No
Free 30 day evaluation/return option	Yes	No	No	No	No
Spare-in-Air RMA process for in warranty items	Yes	No	No	No	No
2 year warranty hardware warranty standard	Yes	No	No	No	No

Lowest per-link

No recurring costs for licenses or features use

BEST support of any vendor!

SEE FULL XLS SPREAD SHEET FOR OVER 200 MATRIX ITEMS!

How Does It Compare?

ROBUST Access Router and Endpoint

BEST Tunneling/VPN Connectivity

HIGHEST Availability & Redundancy

HIGHEST Security & Privacy

BEST Device Management

BEST Mobile Secure "Hardware" Connectivity

5 Facts About IpTL FastLane Appliances You Should Know

When connecting remote IoT/M2M devices to your datacenter or cloud

IpTL's FastLane Gateways <u>gives</u> you the most

1 **Absolutely reliable**

2 **Secure Edge-to-Edge networking**

3 **Cost-effective**

For all your devices, apps, & sites over any Internet connectivity

1. Works with Dynamic IP/DHCP networks

2. Secure and automatic redundant connectivity over multipath

3. Fully transparent end-to-end networking. Open-sky for your apps

4. IpTL gives your Cloud based or Virtual Applications seamless and truly secure access without blocks or hassles or "provider" dictated VPN's

5. Out-of-the-Box strong security

IP Technology Labs

Always Connected™

Thank you for your Attention!

Scott Whittle
Email: Scott@IpTechnologyLabs.com
Tel: +1 301 570 6611 x601
Mbl: +1 301 339 3237

Agenda

IP Technology Labs

How to Sell

When you have **IoT, VoIP/,Video, UC, LAN Networking**, or solutions such as **IP Cameras, Digital Signage, Access control**

IpTL eliminates the difficulties of VPN/Remote Access connectivity: Lack of End-to-End Communications Security; Recurring costs of MPLS or VPN's; Delays or Blockages to Deployment

Your Benefits when **deploying IpTL** as part of your solution

Works over any IP network Securely	Lower costs for your Solution Deployment	You Control Your Security	Deploy now without rip-out or change	Users and Applications Work properly	Scalable with Top Support

What's my Pitch

- **YOU NEED:** Remote access, S2S VPN/, or Secure Tunnel which unblocks & securely connects your networks over low-cost Internet, *easily*

- **IpTL Provides:** networking appliances which enable complete and fully functional network connectivity easily, securely, and automatically

- What are we: **The World's Longest Ethernet Cable**

- The IpTL Difference are features <u>not found</u> in a single provided solution big-box or software vendor in the market today.

How to Sell - Customer Approach

Who are my target customers?

- **IT managers are always seeking CONNECTITVITY**
  - How do get User/App/Server/Site to talk to the mothership
  - Always say they <u>want</u> security; but they WON'T BUY security (exception: Gov'ts and bad guys)

- **IT network guys (the acutal engg's) don't know how their network really works.**
  - The big bosses know even less!
  - Get the support services contract – it is your value add

Who are my target customers?

- **Medium to Large Enterprises with <u>MULTIPLE LOCATIONS</u> - Site-2-Site (S2S)**
    - Medium to Large enterprise *(soho/robo)*
    - Banks – *(branches, ATMs)*
    - Gov't Agency's *(remote offices)*
    - Utilities – *(IoT/M2M)*

- **Small Enterprises have a need but <u>little money</u>**
    - Capture annual support contract or pass;
    - Wants IT support for free…knows the value –but always trying to slip-it-in as part of the deal
    - Scale is small but can be lucrative

How to Sell - Customer Approach

- **Customers moving to Cloud Hosted Apps**
    - By definition makes remotes out of everyone who needs to connect
    - It's really Hybrid-Cloud (public or private)
        - Public Cloud = AWS, Azure
        - Private Cloud = VMWare, Hyper-V (own DC)

- **The problems with Cloud hosted Apps**
    - How do I have my office users PRINT locally? *(peripheral connectivity)*
    - How do I have security for my data-in-motion? *(keep my privacy)*
    - How do I ensure redundancy/availability? *(keep my users productive)*

    Options today from Amazon, MS, VMWare & others – "do an IPsec VPN" or buy our leased line services – *you are on your own.*

How to Sell - Customer Approach

- **Leased-Lines/MPLS users**
  - Generally professional organizations employ
  - Used to like the "SLA" piece but in reality doesn't deliver – down is down
  - Active market shift away from carrier

- **Problem**
  - Carrier Services are really expensive
  - Are not redundant – just buy 2x lines then; no cellular option "diverse path"
  - Bandwidths are typically a fraction of cheap commodity Internet links

- **Opportunity**
  - Lower costs
  - Gain Functionality – both S2S, Cloud, Redundancy, and Applications
  - Control of connectivity – Why wait 8 weeks to get provisioned?
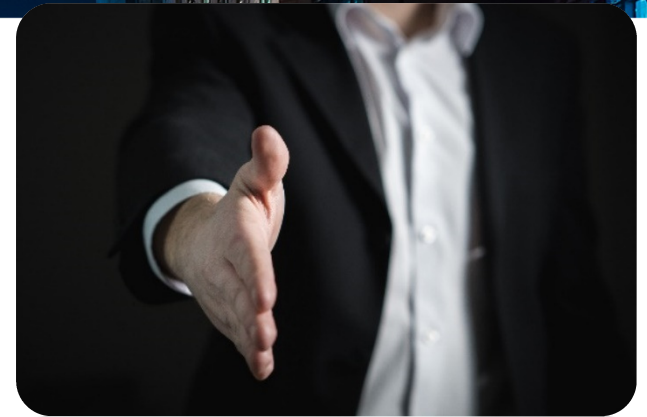
How to Sell - Customer Approach

- **Remote Access – S2S – VPN**
  - Mobility Remote Access/ BYOD
  - Network Extension – LAN over Internet

- **Problem**
  - ERP and Database connectivity
    - Oracle, NetSuite, SAP
  - Multisite Integration blocking business processes
  - Single point of failure a business driver – *7151 Cellular Opportunity!*
  - Can't use IPsec...The Dynamic IP Issue

- **Opportunity**
  - Fixing broke IPSec VPN – Drops & Blocks
  - Dynamic IP
  - Integration of compute sites and users
  - Gain Functionality – both S2S, Cloud, Redundancy, and Applications

How to Sell - Customer Approach

- **Internet of Things – IoT/M2M**
  - Sensors, VoIP/UC, Access Control, IP Cams
  - Non-existent or constrained security (scary!)
   - https://www.youtube.com/watch?v=RoOqznZUCll

- **Problem**
  - PLC's are often not networking agile – locked subnets
  - Single point of failure a business driver
    - *7151 Cellular Opportunity!*
  - Can't use IPsec...The Dynamic IP Issue

- **Opportunity**
  - Securing critical infrastructure
  - IP cameras & Access Control Connectivity & Security
  - Integration of compute sites and users
  - Gain Functionality – both S2S, Cloud, Redundancy, and Applications
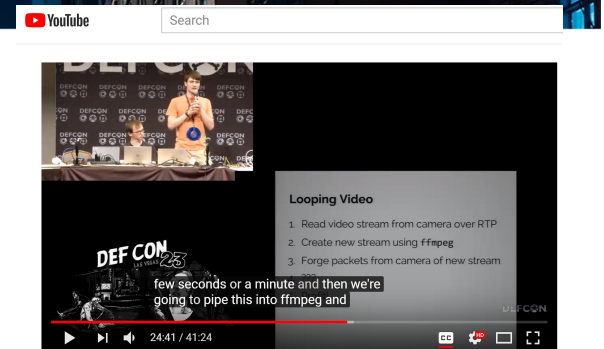
DEF CON 23 - Van Albert and Banks - Looping Surveillance Cameras through Live Editing

How to Sell - Customer Approach

- **VoIP/UC**
  - IP Phones (Avaya, Cisco, Shoretel, Polylcom)
  - Video Conferencing/Teleconferencing/UC

- **Problem**
  - Voip likes to be on the "same network"
  - WAN issues with NAT traversal & VLAN cause headachs
  - IPsec a problem...The Dynamic IP Issue
  - Filtering & proxy's cause legal connectivity issues

- **Opportunity**
  - Integration of remotes to headend – truly unified
  - Availability and Security
  - Permits not just VOIP hones but whole office connectivity back to HQ

- **I can just do that with IPsec (No you can't.)**
  - IPSec needs a public (real) IP on at least the server side (HQ) – this is what breaks dynamic IP
  - IPsec is L3 only and uses the IP address as part of the security association
  - Is routed only with no route distribution protocol (extra)
  - Has about 15% overhead penalty – lost bandwidth
  - L2 or VLANs need GRE + IPSec – extra overheads, complications, etc.
  - Dynamic crypto keys requires an entirely parallel configuration
  - Is an easily filtered "IP PORT"
  - MTU do-not-frag issues for TCP
  - Extremely difficult to configure AND maintain security
    - Most people just use Pre-Shared Keys (one time)
  - Usually a "vendor religious" choice – technically inferior today.

I can just do that with IPsec (No you can't.) CONT'd

- **IpTL Advantage**
  - We use TLSv1.2 (next gen standard) as the transport
  - X.509v3 certs standard
  - IpTL can be installed on private IP – on both ends of the link
  - IpTL can use DYNAMIC IP Links
  - DYNAMIC KEYING Standard -- NO PRESHARED KEYS.
  - Can use any port UDP or TCP (our standard is 5150)
  - About a 6-7% overhead before our compression!
  - User defined connection key (TLS-Auth) for closed user group
  - User defined and control of "rekeying" times
  - Perfect Forward Secrecy standard (rolling private keys!)

  - See our **TLS vs. IPsec White Paper** for breakdown

Customer Questions, Objections, and Answers

- **What encryption do you run? Can someone see my data?**
    - Our standard data encryption is AES256/SHA1 HMAC
        - NOTE: No different than IPsec when using AES cipher options
        - Moving to AES256GCM / SHA3 *next gen efficiencies*
    - No, someone can't see your plain data or understand what you are sending.
    - Also, based on our X.509v3 certs a Man-in-the-Middle attack will fail as you can't fake back-to-back certs (e.g. SSL strip tool)

- **Isn't this just HTTPS?**
    - No, HTTPS can use a range of security options such as SSL, TLS, etc. There is NO cipher negotiation with IPTL. You are assured of the highest level of security connection.

Customer Questions, Objections, and Answers

- **What is your Support Server? Can someone see my data?**
  - Support Server is our own out-of-band management portal
    - We use if for tech support
    - Customers can purchase subscriptions for fielded device management
    - Customers can purchase their own Support Server to remain completely independent if so desired.

  - No, it is only configuration of the unit and there is no access to customer data.

  - Additionally, a customer may TURN OFF Support Server connectivity at any time.

© 2018 IP Technology Labs LLC. Corporate Confidential

Customer Questions, Objections, and Answers

- **What do you do to keep from getting blocked?**
  - Blocks happen for a variety of reasons – Gov't/Political/Cutural; Carrier-to-Carrier peering issues; firewalls; misconfiguration; you name it.

  - Basic TLS tunnel obfuscation
    - IpTL has three "S" modes to statically or dynamically remove any TLS fingerprints from stream. (Important for China, Iran, Turkmenistan, etc)

Cipher Support:		☐ S1 ☐ S2 ☐ S3 ☐ S4

  - Advanced Packet obfuscation
    - IpTL also has packet based compander which ensure the packet sizes are automatically expanded to a larger size and then shrunk on the headend. Prevents "traffic analysis" type filtering

  - Advanced Stream obfuscation
    - IpTL can cap the bandwidth of a stream so that bandwidth level filters don't trigger

- **I'll just get a Mikrotik or config my own Linux VPN**
  - Mikrotik is cheap – but no serious IT manager will go with this way
  - Very well known and established in the Wi-Fi market
  - You have to config each one manually, troubleshoot, linux-like
  - Limited VPN automation – drops, blocks, etc.
  - Hardware has high-failure rate – warranty is just throw-away
  - Doesn't have the IPTL anti-blocking features such as AutoConnect, Obfuscation, MAC based DNS, or System Monitor Redundancy
  - Latvian vs. USA --- You decide.
  - No PCI cert! – IpTL is the only PCI 3.2 100% passing!
  - "Limited support service might be provided by e-mail for 30 days"
  - Warranty: "Term of twelve (12) months from the shipping date"
  - Throw-away if failed – *customer down time*?
  - Did I say cheap...

  My question to the market: "*If Mikrotik is so great, then why does anyone still buy Cisco, Juniper, Sonicwall, etc..*"

Action: Move to demo and win the mind first then the heart

The Process for an Interested Customer

- **Identify Need**
  - Multisite; Connectivity issues; Cost reduction cycle; LL/MPLS

- **Information & Education**
  - Send 3x Security White Papers
  - Proforma design proposal

- **Demo/POC**
  - Show them the IpTL Solution working (you should have already done the basic Magic Show to our demo server)
    - Do a simple LAN extension Point-to-Point
      (http://doccentral.iptechnologylabs.com/index.php/doc/iptl-hardware-quick-start-guide/#2195)
    - Manage the expectations here – Conditional PO for multisite

- **Quote, Close, & Install**
  - Let us help! – Proposal creation, Customer Conference calls, Competitive

Why Partner with IpTL?

- **Connect us with your solutions team**
  - Field-Application-Engineers
  - Pre-Sale Solutions Architects
  - Sales Teams

- **IpTL Enable's your Multisite Requirements**
  - Recommend IpTL for remote site requirements
  - We are not marketing for rip-out or substitutions
  - Complimentary to your Solutions

- **Customer Satisfaction**
  - IpTL will create RFQ/RFP proposals and content
  - Let us provide your live hands-on technical support
  - AccessEdge™ partner programs protect your projects

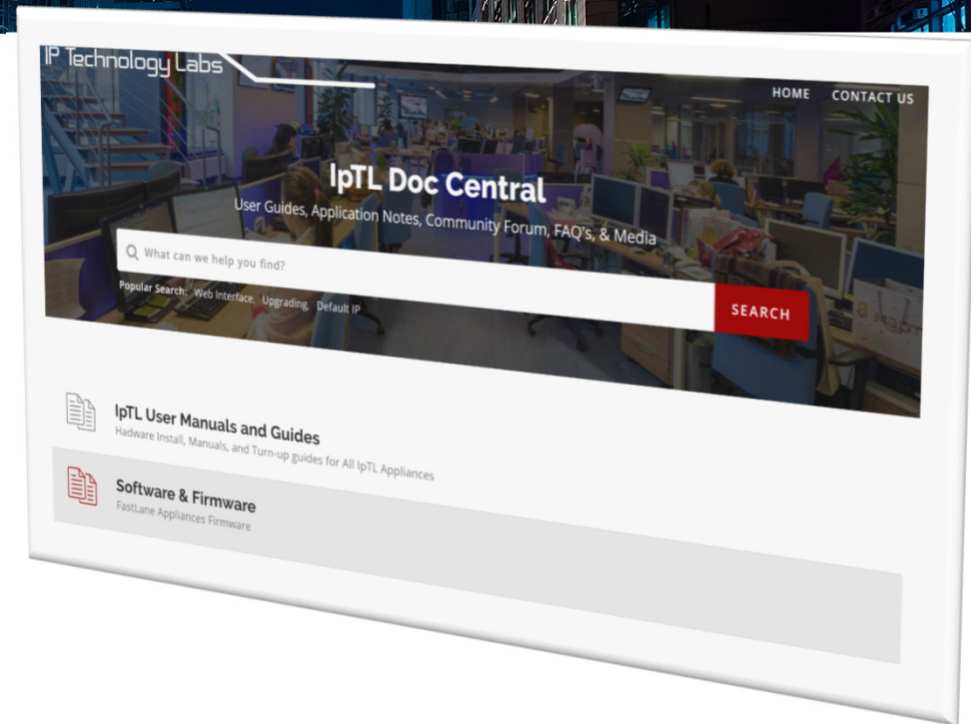## Additional Resources

- **FastLane Forum –**
  http://doccentral.iptechnologylabs.com
  - App Notes
  - Marketing Info
  - Community Questions & Answers
  - Proposal Templates

- **IpTL Demo Server**

http://demo.IpTechnologyLabs.com

User = monitor
Pass = monitor

Thank you for your Attention!

Scott Whittle
Email: Scott@IpTechnologyLabs.com
Tel: +1 301 570 6611 x601
Mbl: +1 301 339 3237