Jeff Welton
Sales Manager, Central USA
Nautel

Kevin Trueblood
Associate General Manager
WGCU Public Media

Aaron Read
IT & Engineering Director
Rhode Island Public Radio

Alex Hartman
Broadcast Integration Specialist
Wisconsin Public Radio

TRANSMISSION TALK TUESDAY

Episode #62

IT Month

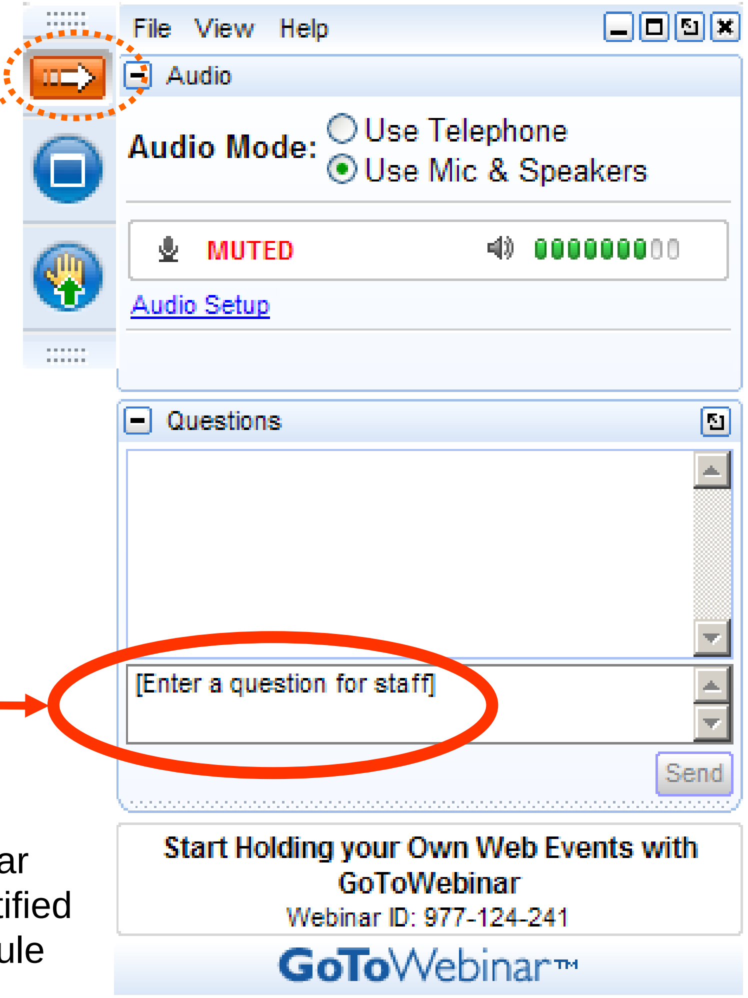
Configuring VPN

nautel
AM/FM Radio Transmitters

Your questions please?

(if you don’t see the control panel, click on the orange arrow icon to expand it)

Please enter your questions in the text box of the webinar control panel (remember to press send)



Audio Mode: ○ Use Telephone ● Use Mic & Speakers

MUTED

Audio Setup

[Enter a question for staff]

Send

Start Holding your Own Web Events with GoToWebinar
Webinar ID: 977-124-241

GoToWebinar™

Remember: The completion of a Nautel webinar qualifies for ½ SBE re-certification credit, identified under Category I of the Re-certification Schedule for SBE Certifications.

The non-IT folks real struggle with a reliable point-point VPN. I've been using a Netgear BR500 with mixed results. Ray

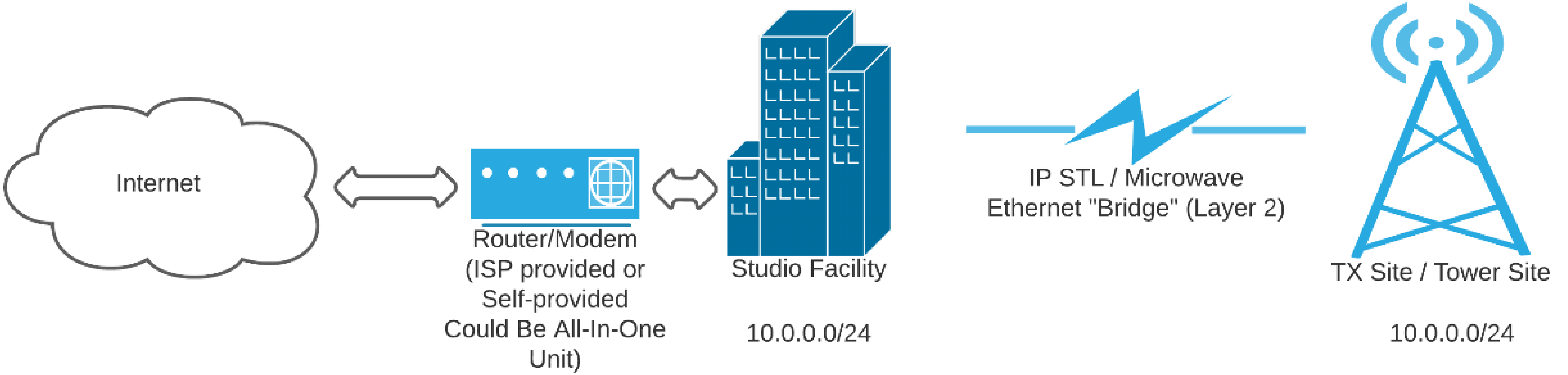
How about connecting to remote sites with CradlePoint devices?

Any recomended opensource router/firewall software and hardware, not everyone can afford Cisco.

Can a Dante AOIP network be on VPN or should that be a totally discreet network? It caused traffic issue with our phone system.

In addition to Cisco, how about here's how you do it with what Walmart, Best Buy, Office Depot has for an emergency

Would appreciate emphasis on open source and one-time payment owned systems, as opposed to the subscription model.



Internet

Router/Modem (ISP provided or Self-provided Could Be All-In-One Unit)

Studio Facility

10.0.0.0/24

IP STL / Microwave Ethernet "Bridge" (Layer 2)

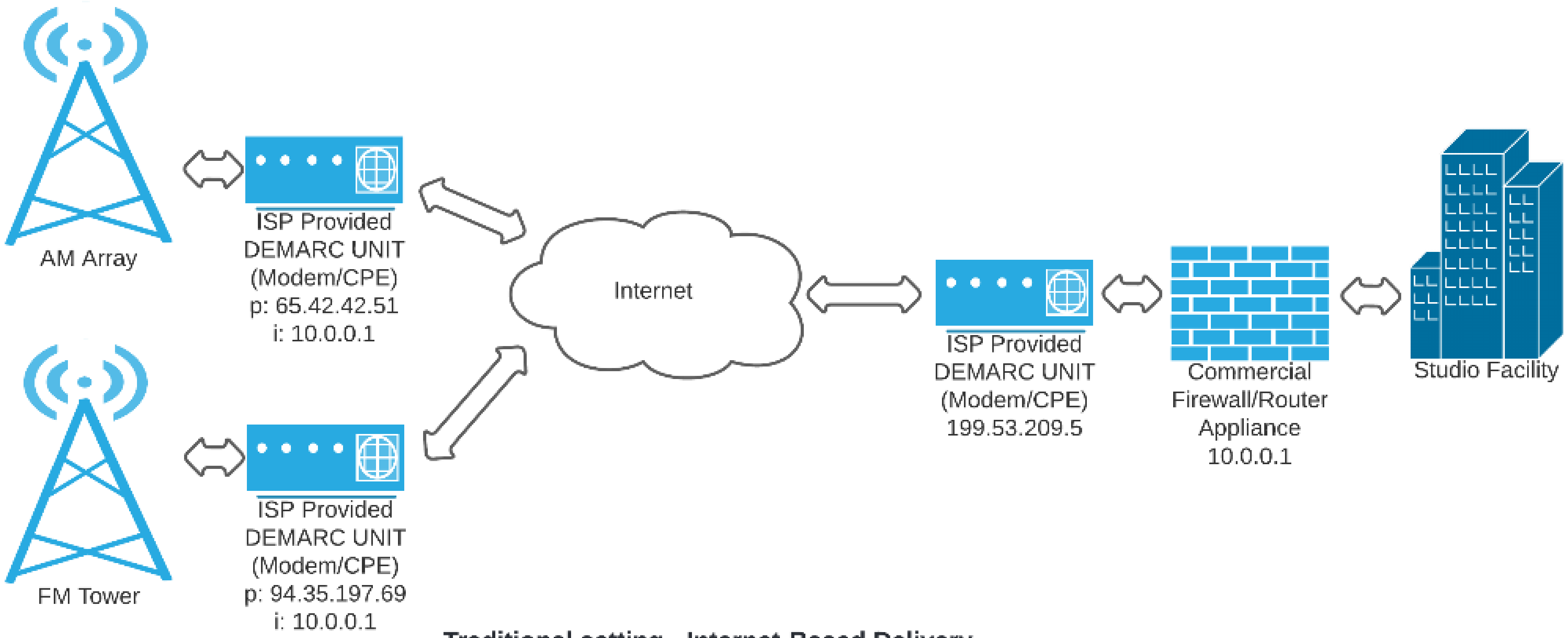
TX Site / Tower Site

10.0.0.0/24

Traditional setting - Ethernet Bridge

Both sites in the same logical Subnet
No routers between facilities
No VPN Capabilities
Router-based Firewall

https://www.lucidchart.com/pages/



Traditional setting - Internet-Based Delivery

Punch holes through firewalls to deliver audio
Punch holes through firewall to get telemetry
Punch holes through firewall for remote access

DON'T DO THIS!

https://www.lucidchart.com/pages/

What is a VPN?

Virtual Private Network

Can be a remote-access VPN such as a client

Can be cloud based to provide connectivity to multiple sites and users seamlessly

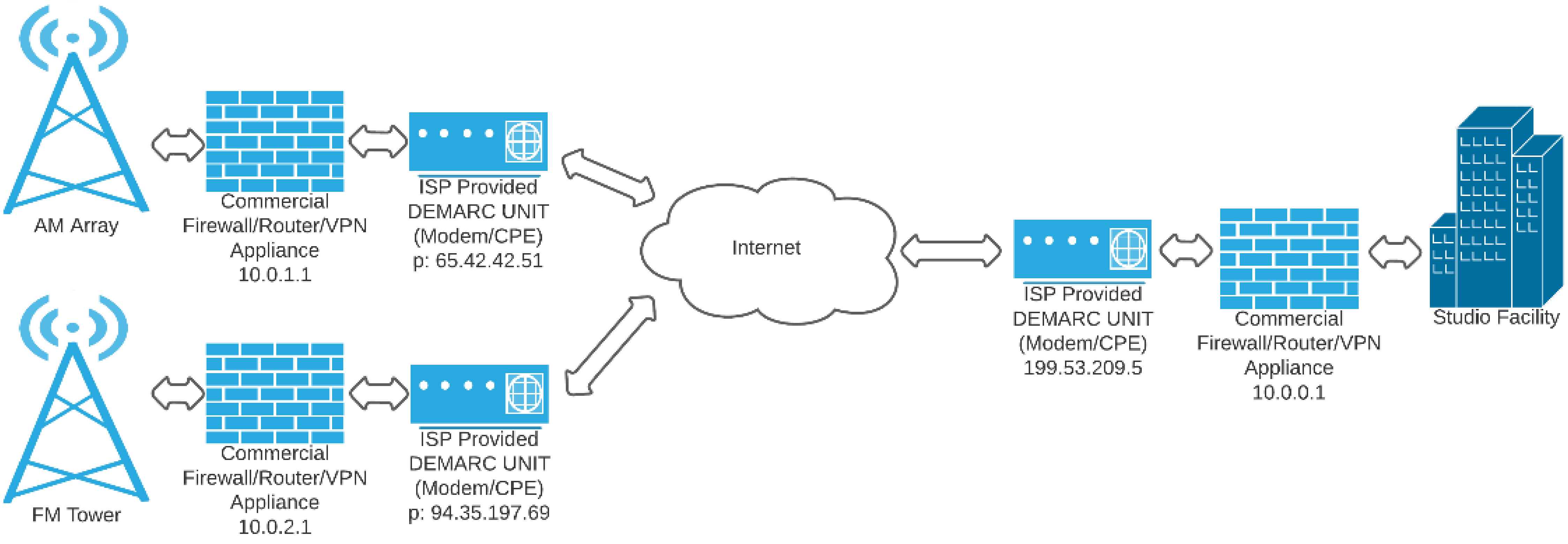
Can be site to site over public networks and extend your LAN to different locations

What is a site to site VPN

Allows independent networks to be interconnected over public internet

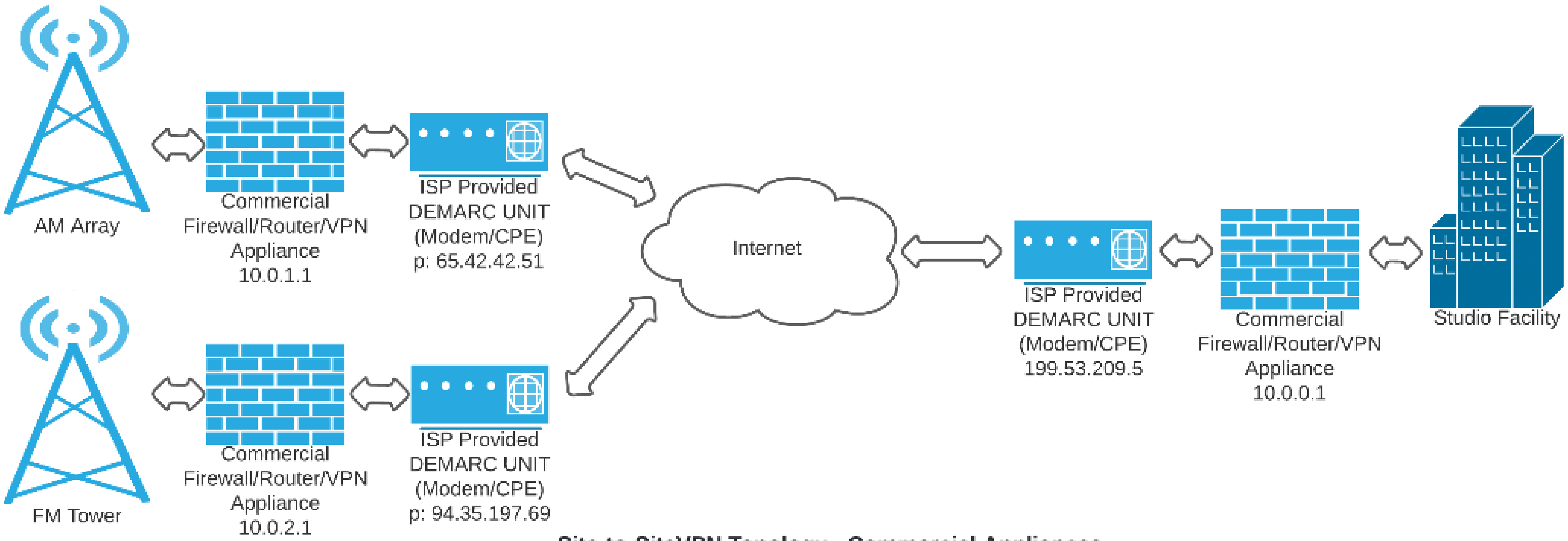
Can be a site two miles away. Can be a site two states away.

Allows you to create a wide area network where resources can be managed as though they are local


AM Array
Commercial Firewall/Router/VPN Appliance 10.0.1.1
ISP Provided DEMARC UNIT (Modem/CPE) p: 65.42.42.51
FM Tower
Commercial Firewall/Router/VPN Appliance 10.0.2.1
ISP Provided DEMARC UNIT (Modem/CPE) p: 94.35.197.69
Internet
ISP Provided DEMARC UNIT (Modem/CPE) 199.53.209.5
Commercial Firewall/Router/VPN Appliance 10.0.0.1
Studio Facility

Site-to-SiteVPN Topology - Commercial Appliances

All Internet Traffic through VPN tunnels
No externally visible ports
All traffic is inspected by the home firewall if internet access is required (No "Split-tunnel")
All sites authenticated


AM Array
Commercial Firewall/Router/VPN Appliance 10.0.1.1
ISP Provided DEMARC UNIT (Modem/CPE) p: 65.42.42.51
FM Tower
Commercial Firewall/Router/VPN Appliance 10.0.2.1
ISP Provided DEMARC UNIT (Modem/CPE) p: 94.35.197.69
Internet
ISP Provided DEMARC UNIT (Modem/CPE) 199.53.209.5
Commercial Firewall/Router/VPN Appliance 10.0.0.1
Studio Facility

Site-to-SiteVPN Topology - Commercial Appliances

Studio IP: 199.53.209.5
Inside network: 10.0.0.1/24
VPN Tunnel IP to FM: 10.254.253.1/30
VPN Tunnel IP to AM: 10.254.252.1/30

FM Tower IP: 94.35.197.69
Inside network: 10.0.2.1/24
VPN Tunnel IP: 10.254.253.2/30

AM Array IP: 65.42.42.51
Inside network: 10.0.1.1/24
VPN Tunnel IP: 10.254.252.2/30

Why do this?

It’s secure. Does not require opening ports in firewalls

Convenience. Everything appears to be part of a local LAN

Resources can be easily accessed from either location

Applications in a broadcast environment

Extend studio LAN to transmitter sites

Interconnect multiple studio locations

Applications in a broadcast environment

Connect audio CODECs as local connections

Send now playing information

Send HD data

Extend studio VOIP system

Device UI management

If you have SNMP-enabled equipment, you can have one remote control system monitor parameters at all locations

Drawbacks

If all traffic runs through one central place, if central place goes down connectivity to other sites goes down as well.

What do you need?

Need hardware capable of establishing VPN protocols.

Most commonly incorporated into firewall and router appliances

Most common hardware appliances include Cisco and FortiNet

Static IPs on each end

Appliance Companies:

Cisco
Juniper
Palo Alto
Aruba
Fortinet

Software-based VPN:

EtherVPN
Windows Networking (yes,that Windows)
Linux PC (ipfw/iptables, super advanced nerds only apply here)
OpnSense/PfSense

Pros of HW

- Appliance based - Usually can have some kind of support contract
- Dedicated hardware
- Multiprotocol support

Cons of HW

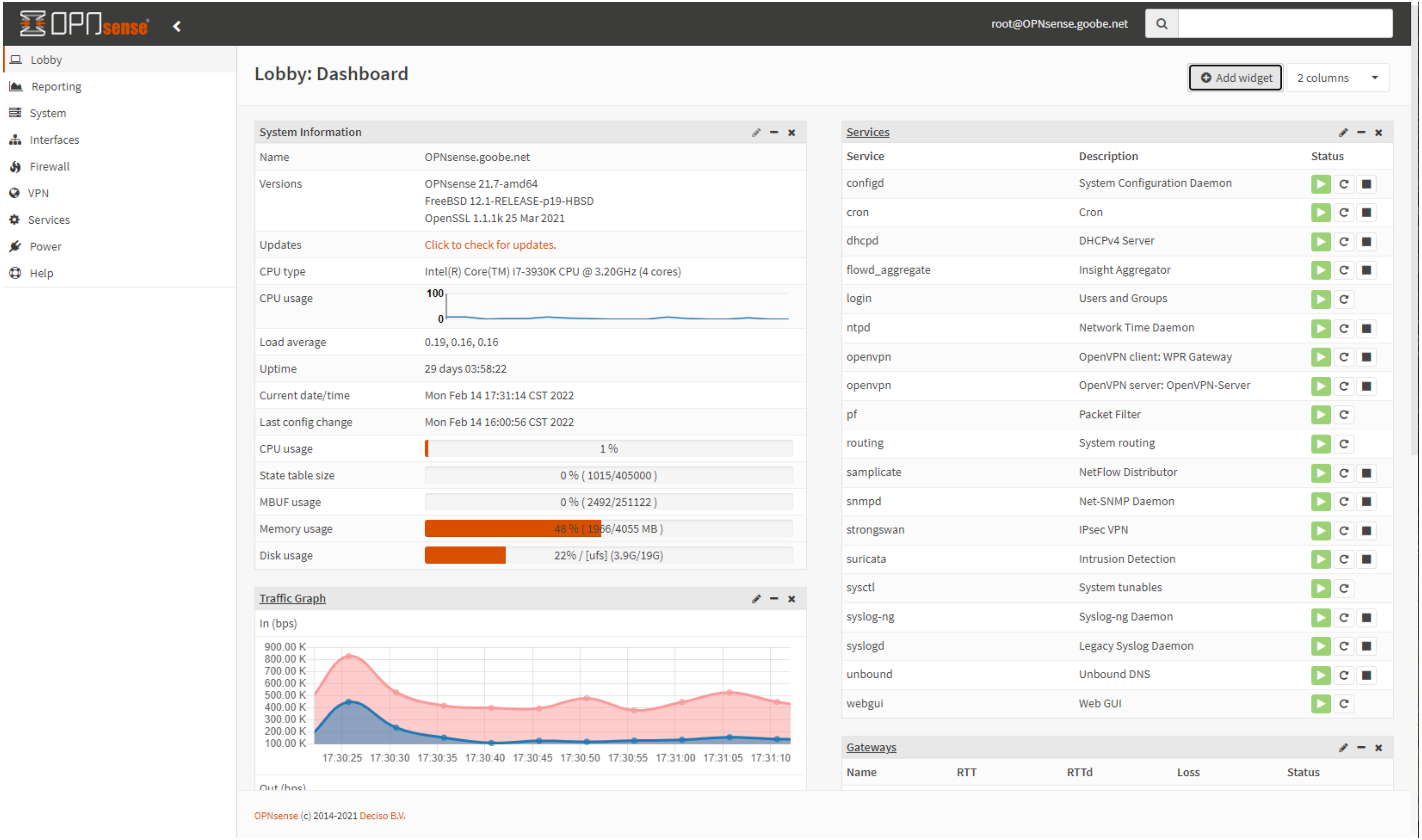
- Can be limiting in advanced network topologies
- Cheaper units cannot support lots of remote sites/users
- Can sometimes require a separate authentication system to maintain

Pros of SW:

- Configurable, multiprotocol support
- Installation can be quite simple
- Easy to rollback using snapshots (if enabled, different webinar)
- Can be locked down to single hosts

Cons of SW:

- Gets a little tricky when trying to share with other devices on your networks
- Can be limiting depending on topology
- Requires a little under the hood work at times to implement
- At the mercy of the PC if running critical infrastructure



Lobby: Dashboard

System Information

Name	OPNsense.goobe.net
Versions	OPNsense 21.7-amd64 FreeBSD 12.1-RELEASE-p19-HBSD OpenSSL 1.1.1k 25 Mar 2021
Updates	Click to check for updates.
CPU type	Intel(R) Core(TM) i7-3930K CPU @ 3.20GHz (4 cores)
CPU usage	100 0
Load average	0.19, 0.16, 0.16
Uptime	29 days 03:58:22
Current date/time	Mon Feb 14 17:31:14 CST 2022
Last config change	Mon Feb 14 16:00:56 CST 2022
CPU usage	1 %
State table size	0 % (1015/405000)
MBUF usage	0 % (2492/251122)
Memory usage	48 % (1966/4055 MB)
Disk usage	22% / [ufs] (3.9G/19G)

Traffic Graph

Services

Service	Description	Status
configd	System Configuration Daemon	▶ ↻ ■
cron	Cron	▶ ↻ ■
dhcpd	DHCPv4 Server	▶ ↻ ■
flowd_aggregate	Insight Aggregator	▶ ↻ ■
login	Users and Groups	▶ ↻
ntpd	Network Time Daemon	▶ ↻ ■
openvpn	OpenVPN client: WPR Gateway	▶ ↻ ■
openvpn	OpenVPN server: OpenVPN-Server	▶ ↻ ■
pf	Packet Filter	▶ ↻
routing	System routing	▶ ↻
samplicate	NetFlow Distributor	▶ ↻ ■
snmpd	Net-SNMP Daemon	▶ ↻ ■
strongswan	IPsec VPN	▶ ↻ ■
suricata	Intrusion Detection	▶ ↻ ■
sysctl	System tunables	▶ ↻
syslog-ng	Syslog-ng Daemon	▶ ↻ ■
syslogd	Legacy Syslog Daemon	▶ ↻ ■
unbound	Unbound DNS	▶ ↻ ■
webgui	Web GUI	▶ ↻

Gateways

Name	RTT	RTTd	Loss	Status

OPNsense (c) 2014-2021 Deciso B.V.

TRANSMISSION TALK TUESDAY

Doesn’t have to be expensive!

Many prosumer devices can do this.

Manufacturers include TP-Link, Zyxel, Linksys, Ubiquiti, Netgear, Mikrotik

Online Information

Webinars
https://www.nautel.com/resources/webinars/

Nautel Waves Newsletter
https://www.nautel.com/newsletters/

YouTube
http://www.youtube.com/user/NautelLtd

Online Info, such as the Broadcasters' Desktop Resource
https://www.thebdr.net/

THANK YOU!

TRANSMISSION TALK TUESDAY

nautel
AM/FM Radio Transmitters