Encrypt the Data, Not the Network

Jon Callas
CTO/CSO and co-founder

Overview

- **There are no easy solutions**
  - **If there were, we'd be using them**
    Network protection
  - **Why this is necessary**
  - **Why this not sufficient**
- **Protecting the data**
  - **Data in motion**
  - **Data at rest**
  - **Peripatetic data**

Why Networks Need to Be Protected

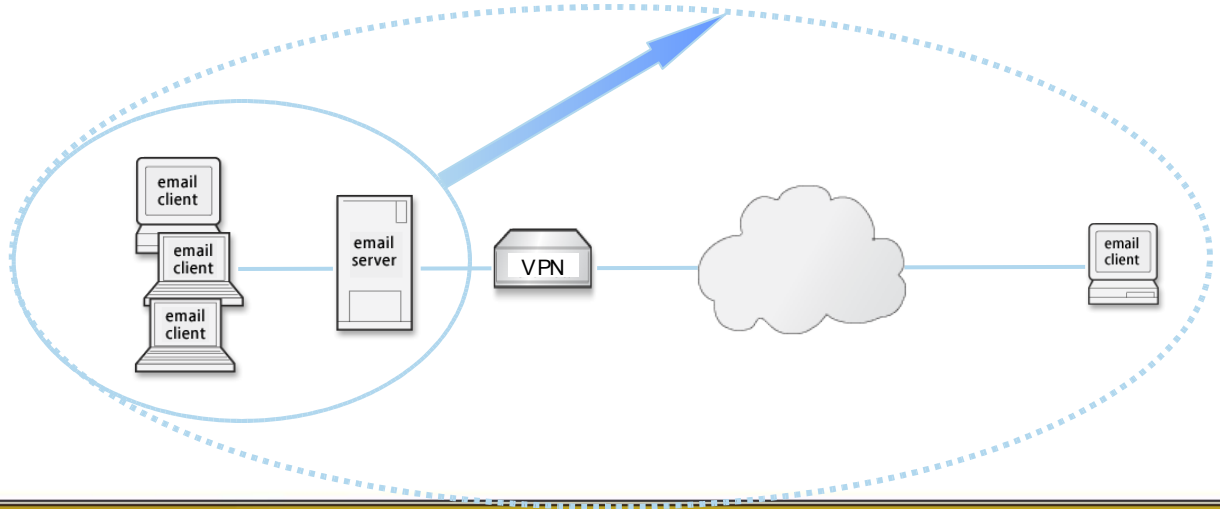
- **Sniffers exist**
- **Anyone, anywhere can read the packets as they go by**
- **However**
  - **It is harder to do this in the middle of the network than you'd think**
  - **A bad actor will be tapping the network near an end, not in the middle**
  - **There are legal protections for network security — tapping a link is wiretapping**

VPNs

- **Low-level network encryption of the packets as they move across the network**
- **May be considered a virtual interface that is secure**
- **Usually goes host-to-host, not network-wide, as originally planned**
- **Operates as a tunnel or a route**
- **Each has different security characteristics**

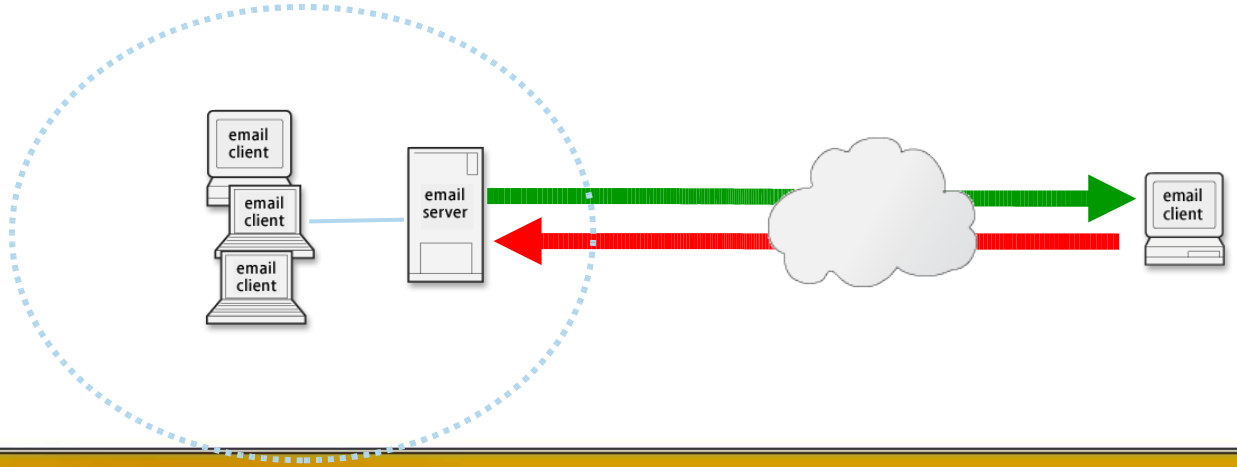
Two Ways a VPN Can Work

- **Tunnel**
  - **All traffic routed through VPN server**
  - **Like teleporting into a walled city**
  - **Security perimeter expands to include remote host**



Two Ways a VPN Can Work

- **Route-level**
  - **Only ports bound for protected domain go there**
  - **Remote host is both in and out (or neither in nor out)**
  - **Security perimeter doesn't include remote host**



SSL/TLS

- **Encryption and authentication for TCP-level connections.**
  - **TLS is the IETF-standard version of what is commonly called SSL.**
- **Other protocols are run through TLS**
  - **SMTP, LDAP, IMAP, POP, SOAP, etc.**
- **Improves the existing protocol without needing infrastructure change**

SSH

- **Provides "secure telnet" access**
- **Provides TCP-level tunneling**
- **Similar function to SSL in this way, but with VPN features**
- **Used mostly by techies**
- **Embedded transparently into other systems on occasion**

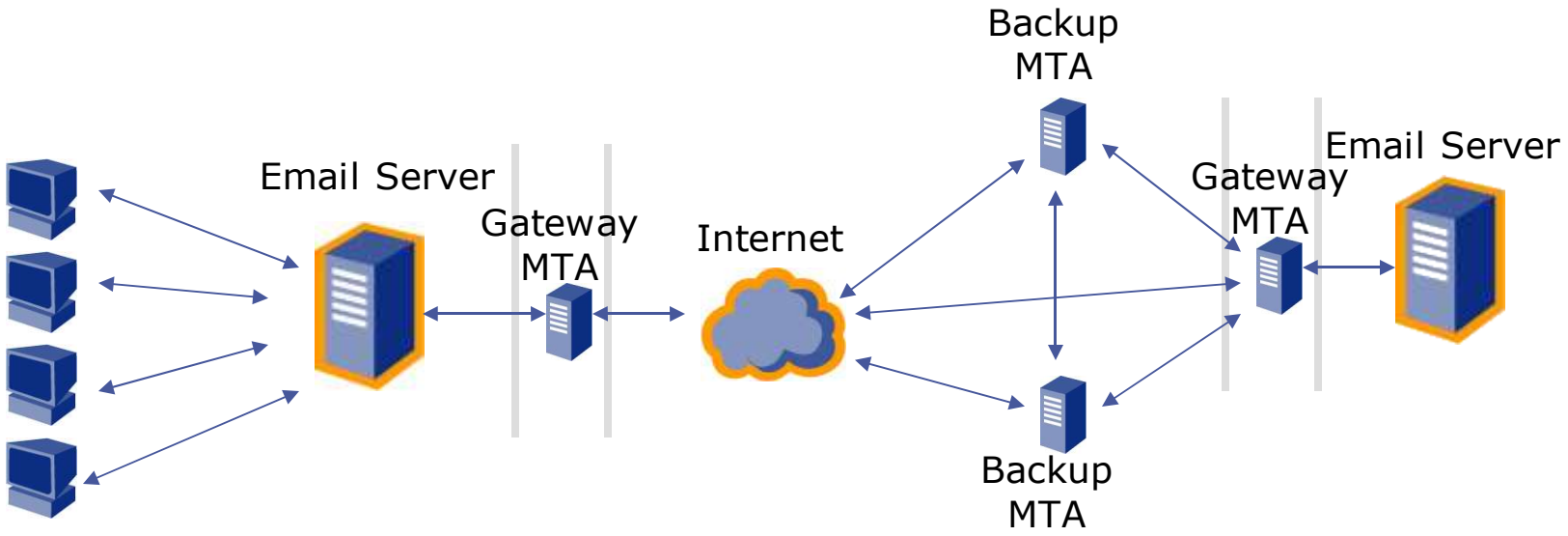
SSL VPNs

- **Not a true VPN**
- **Can be considered a "Resource Router"**
- **Project and re-present services in a browser ("clientless")**
  - **File servers may become web pages**
  - **Email access through a web client**
- **May also contain SSH/SSL-like port forwarding**

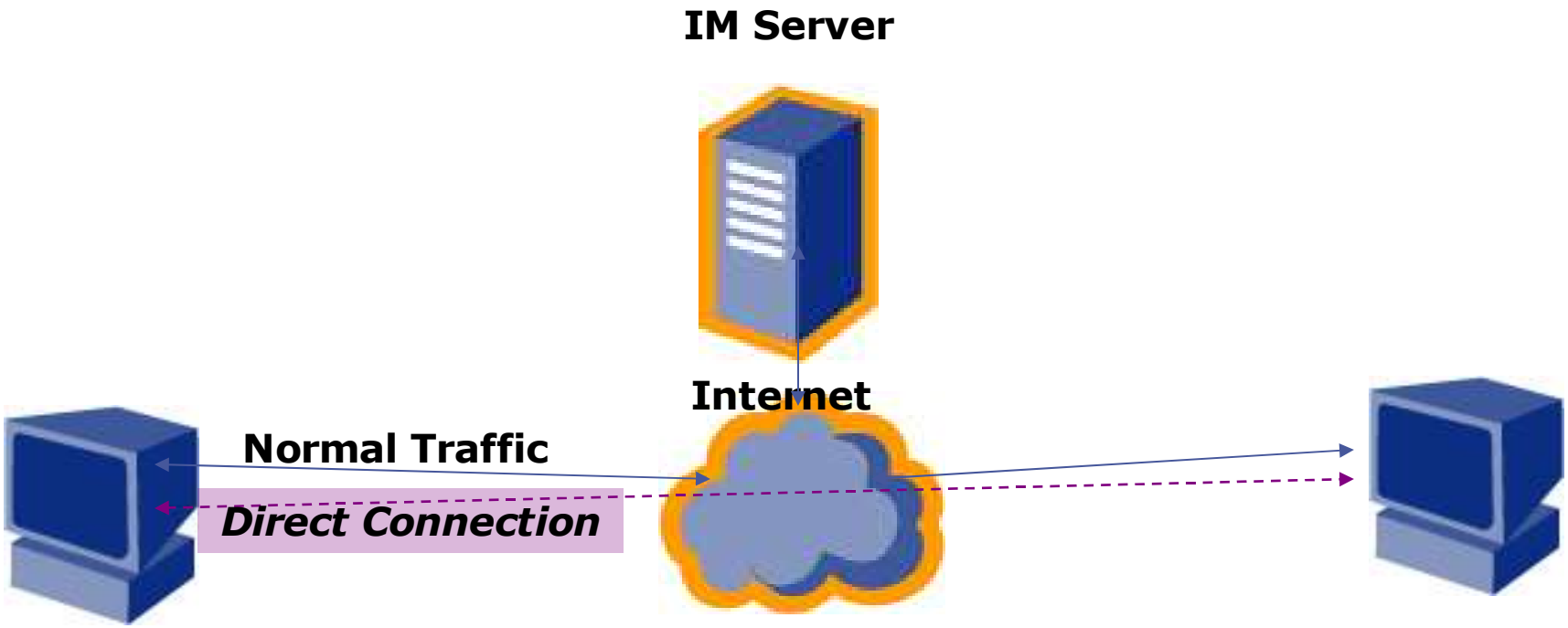
Why this isn't good enough

- **The network is the least vulnerable place**
- **The network has the best legal protections**
  - **Recent legal decisions interpret wiretapping laws to only apply to wires**
  - **It's possible that tapping at a firewall or router is legal**
  - **Tapping email is legal**
- **This is adequate for "direct" protocols (e.g. http)**
- **Many protocols are store-and-forward, or star-routed**
  - **Email, IM, Voice**
- **Still necessary, still good, merely not sufficient**

How E-mail Works

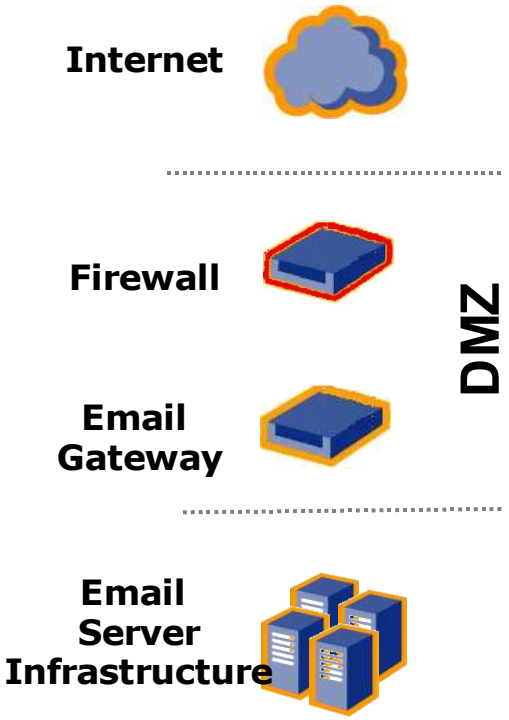


How Instant Messaging Works

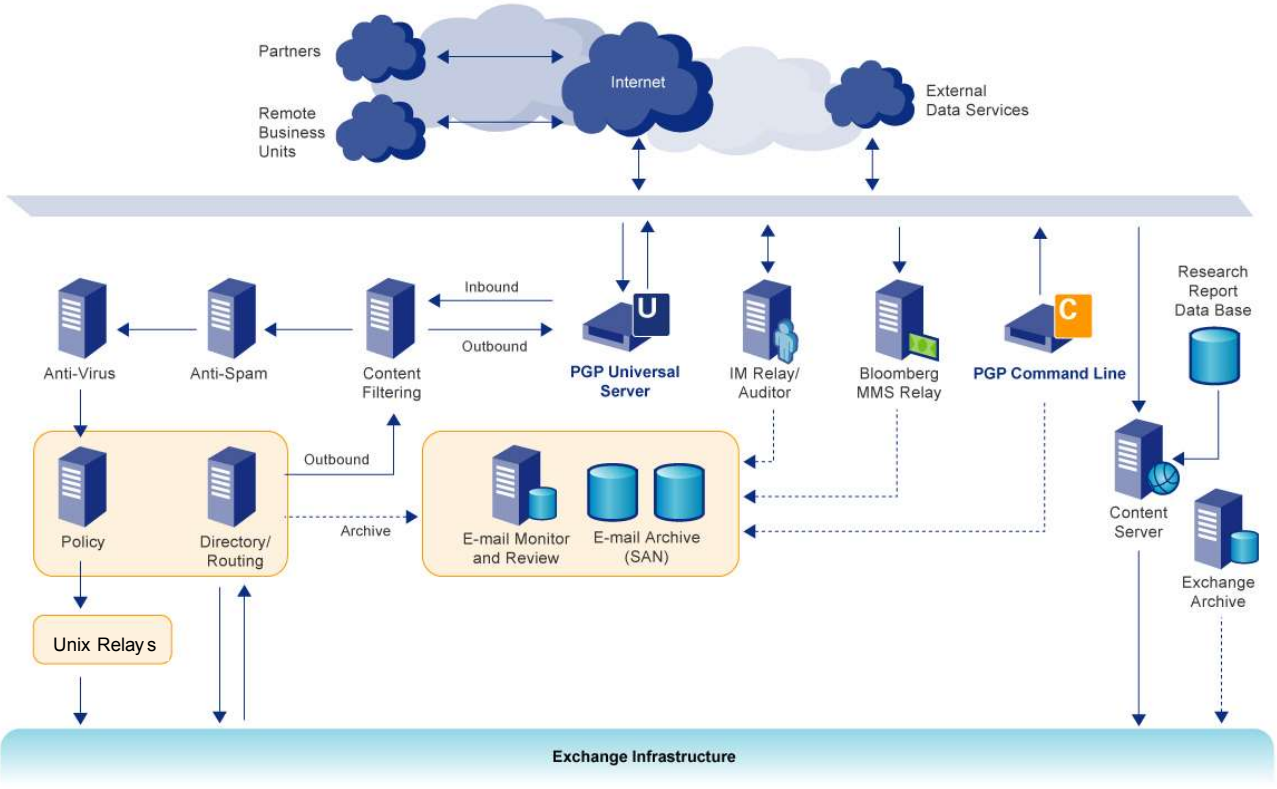


DMZ: Perception vs. Reality

Perception



Reality



Necessary But Not Sufficient

- **Networking security is always good to have**
- **We at PGP use TLS/SSL whenever possible**
- **We must go beyond to protect the actual data**

Seal the Envelope

- **Two standards exist for encrypting data payloads**
  - **OpenPGP**
  - **S/MIME**
- **Think of them like GIF and JPEG for pictures**
  - **They're similar but different**
  - **They solve the same problem**
  - **They have slight differences that matter to whom they matter to**
- **Each has their own proponents**
- **Continued work merges them closer together**
- **Bottom line: You have to do both**

Basic Construction

- **Data is formatted**
- **Data is compressed**
- **Data is signed**
- **Data and signature encrypted with session key**
- **Session key encrypted with recipient(s) public key(s)**
- **Message formatted further, certs added**

Finding Keys and Certificates

- **Can be found in directories (OpenPGP, S/MIME)**
  - **Advantage: smaller messages, easier caching**
  - **Disadvantage: extra work needed when processing messages**
- **Can be sent with messages (S/MIME)**
  - **Advantage: no further protocol needed**
  - **Disadvantage: bootstrapping harder to new recipients**
- **Usage Profiles**
  - **"Preferences" (OpenPGP) "capabilities" (new S/MIME work)**
  - **Allows user to state how messages should be made in the certificate**

Not just for e-mail

- **Encrypting data is most obvious for email**
- **Also used in SIP, Jabber, other IM, SAML, XKMS, XRML, etc.**
- **Any protocol where there are "hops" that the data must traverse, instead of being in a stream.**

Limitations

- **It is good to combine data encryption with network encryption**
- **OpenPGP and S/MIME do not encrypt headers**
  - **Subject, from, to, date, etc.**
- **Internal email structure may be revealed by some implementations**
  - **Extra care needed to make sure that an attachment is XXX.pgp not Secret-Plans.doc.pgp**
- **These issues exist on other protocols like SIP, VOIP**
- **But these are relatively small problems**

Data Access

- **Needed for regulated industries, and others with tight requirements**
- **Two mechanisms possible:**
  - **Backups/copies of the keys that encrypt.**
  - **Multiple encryptions, one to a protected additional decryption key.**
- **Each has places where it is good and not good**
- **Reasons may be technical, procedural, or legal**
  - **Archival, anti-virus, content scanning, etc.**

Defense in Depth

- **What happens when the data gets to a disk?**
- **Different models of data protection.**
  - **Static Data**
    - **Sitting on servers, other controlled locations**
    - **Sitting on desktop systems**
  - **Peripatetic Data**
    - **Walks around on laptops, cell phones, removable media, pdas, cameras, music players....**
    - **There's more of it than you think, it's more sensitive than you think**

Don't Confuse Risk and Reality

- **Some people have seen the risk of peripatetic data and tried to ban it**
- **King Canute and Dirty Harry knew their limitations**
- **Understand the power of sensible policy, and managing risk**
  - **Banning productivity tools makes you less productive**
  - **Don't be an agent of "brightsizing"**
- **The bad guys are going to succeed sometimes**
  - **Don't let them cloak themselves with breaking bad policy**
- **As always, there are obvious exceptions**
  - **Regulated organizations are regulated and protected to shield them from market forces!**

Why do we protect the data?

- **Law and regulation is requiring this.**
  - **California again leads the way to Florida, NY, and to NZ, EU and others**
  - **There will be more of these requirements**
- **Details may not be what we like, but the principle is good.**
  - **If you carelessly lose data entrusted to you, you are responsible for it**
  - **Be glad policies aren't dictated! Remember the trouble of SOX, HIPAA, etc.**
- **This mirrors requirements in other parts of our lives.**
  - **A burglar can easily break into your house, but you have to have a lock on the door to make the insurance company happy**

How do we protect this data?

- **Separation of servers**
- **Separation of access**
  - **If backups are encrypted, that cuts off a path for the bad guys**
- **Encrypt**
  - **Databases**
  - **Virtual storage**
  - **Removable storage**
  - **Portable systems**
- **User Hardware Security Modules where it makes sense**

But this isn't easy!

- **If our jobs were easy, someone else would be doing them for less**
- ***My*** **hard job is to make this easier for you.**
  - **Look at not only products, but architecture, direction, and vision**
- **Move at all due speed**
  - **Plan ahead, budget ahead**
  - **Recognize trends, move with the tide**
  - **Make is easy to follow policy, easy to know when users are doing the right thing**
  - **Don't make policy at odds with business practices, just because there's risk**

Summary

- **Network protection has uses, and you need it too**
  - **Remote access control**
  - **External spy protection**
  - **Virtual Private Lines**
- **Data protection has uses**
  - **Data in users' hands needs protection**
  - **Network architecture makes network protection necessary but not sufficient**
- **You have to do both**
  - **Your customers, your business, the law will make you**