

RSA CONFERENCE 2014

FEBRUARY 24 - 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

Why SSL is better than IPsec for Fully Transparent Mobile Network Access

SESSION ID: SP01-R03

Aidan Gogarty

HOB Inc.
aidan.gogarty@hob.de



What are we all trying to achieve?

- ◆ Fully transparent network access
- ◆ Network access with highest possible security
- ◆ Access where, when and how we want it

A quick question.....

- ◆ What is better for you, SSL or IPsec?
- ◆ Why?

RSA[®]CONFERENCE2014

FEBRUARY 24 - 28 | MOSCONE CENTER | SAN FRANCISCO



SSL vs. IPsec Is There A Winner?

Features of SSL

- ◆ Session key exchange
- ◆ Perfect forward secrecy possible
- ◆ Data/message encryption
- ◆ Works on transport layer (Layer 4)
- ◆ Application used need not be specifically designed for SSL
- ◆ Good for high volume of sessions

Advantages of SSL

- ◆ Already included in all browsers and most web servers
- ◆ Ease of use for end users
- ◆ Web browser acts as client (clientless)
- ◆ Client mobility (device and platform independent)
- ◆ Free of connection restrictions (HTTPS)
- ◆ Low rollout and maintenance costs
- ◆ High scalability

Disadvantages of SSL

- ◆ Network access not fully transparent
- ◆ Not suitable for VoIP
- ◆ Sessions may need multiple handshakes, making a computationally heavy load for client and SSL devices
- ◆ The security of any client connection must be closely scrutinized
- ◆ Requires Java or ActiveX for access to non-web enabled applications
- ◆ Few applications support out-of-the-box web-based access

Features of IPsec Encryption

- ◆ Encrypts data flows
- ◆ Works on internet layer (Layer 3)
- ◆ Supports multiple encryption algorithms (AES, DES, RC4 – same as SSL)
- ◆ Application used need not be specifically designed for IPsec
- ◆ Good for high volume of sessions

Advantages of IPsec

- ◆ Fully transparent network access
- ◆ Common solution for site-to-site VPNs
- ◆ Same security levels as SSL
- ◆ Economical if running few clients

Disadvantages of IPsec

- ◆ Inflexible - practical for site-to-site VPNs only, not mobile access
- ◆ Installation and updates necessary (drivers, applications) - expensive if running many clients
- ◆ Firewalls and proxies interrupt connection (port forwarding necessary)
- ◆ Data compression can make data transfer impractical (connectionless)
- ◆ Network address translation (NAT) issues
- ◆ Unless properly terminated in DMZ or firewall, IPsec effectively makes a hole in your security – access to whole network, not specific servers

Comparing SSL & IPsec

◆ SSL

- ◆ Device and platform independent
- ◆ High scalability, low maintenance
- ◆ Not suitable for VoIP
- ◆ Heavy load for client and SSL devices



◆ IPsec

- ◆ Good solution for site-to-site VPNs
- ◆ Expensive if running many clients
- ◆ Must be properly terminated at both ends



RSA[®]CONFERENCE2014

FEBRUARY 24 - 28 | MOSCONE CENTER | SAN FRANCISCO



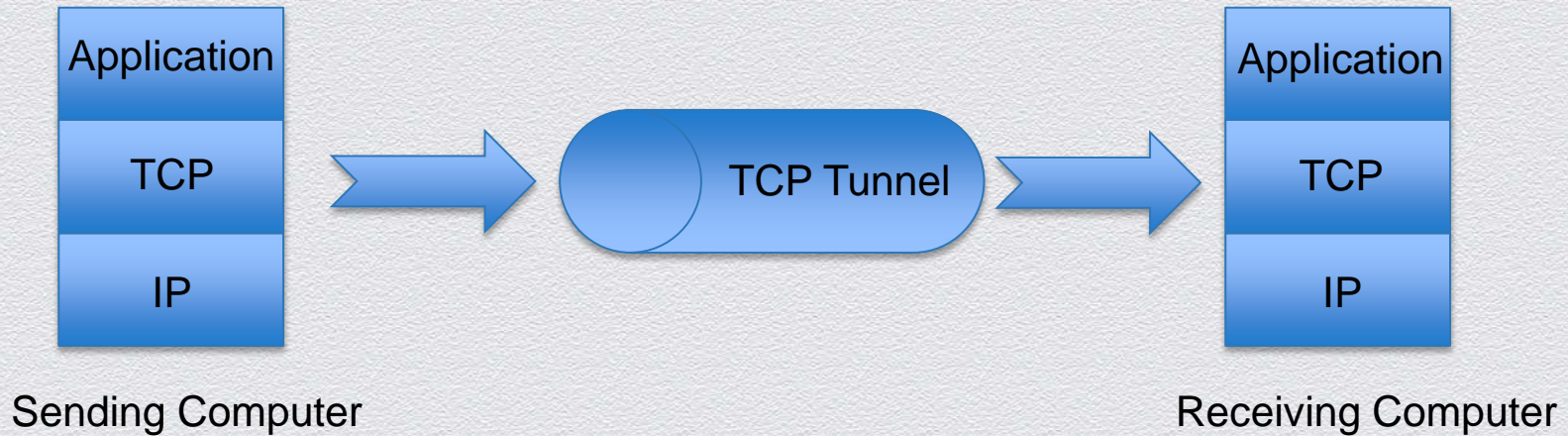
Using Tunnels

A bit about Tunnels

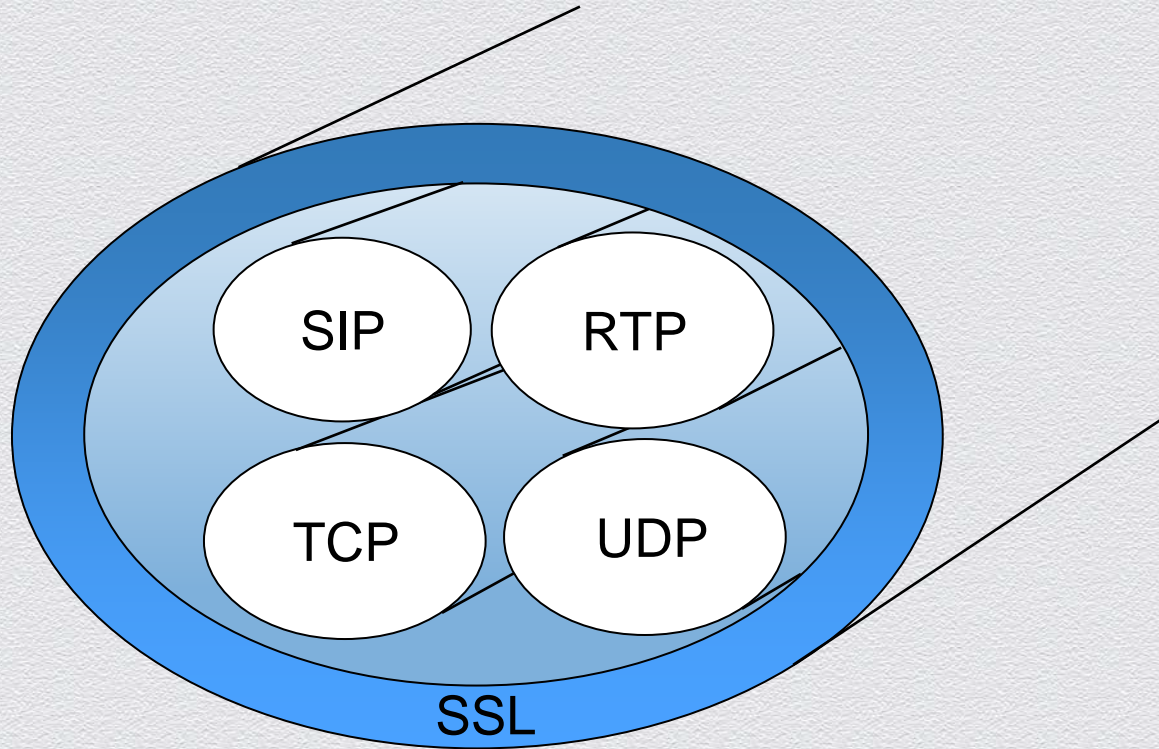
- ◆ Tunnels deliver the communications
- ◆ Tunnels are direct and secure
- ◆ Tunnels mostly use TCP – a connection-oriented protocol
 - ◆ Compression is more efficient in TCP
 - ◆ Data does not get lost using TCP
 - ◆ TCP ports are normally open in firewalls
- ◆ Can cause bottlenecks

How does the TCP Tunnel work?

- ◆ Encapsulates the TCP sessions



What is in the Tunnel?



SSL Tunnel vs. IPsec Tunnel

- ◆ SSL Tunnel – gives a secure tunnel to your application
- ◆ IPsec Tunnel – gives a secure tunnel to your network
 - ◆ SSL tunnel is easier to use, as Wi-Fi routers and other equipment see it as normal TCP/UDP traffic for which they were built
 - ◆ An IPsec tunnel needs special support in the Wi-Fi routers and other equipment used

Why both TCP and UDP?

TCP:

- ◆ Included in SSL encryption
- ◆ Proof against packet loss and disorder
- ◆ Possible delays and stream interruption



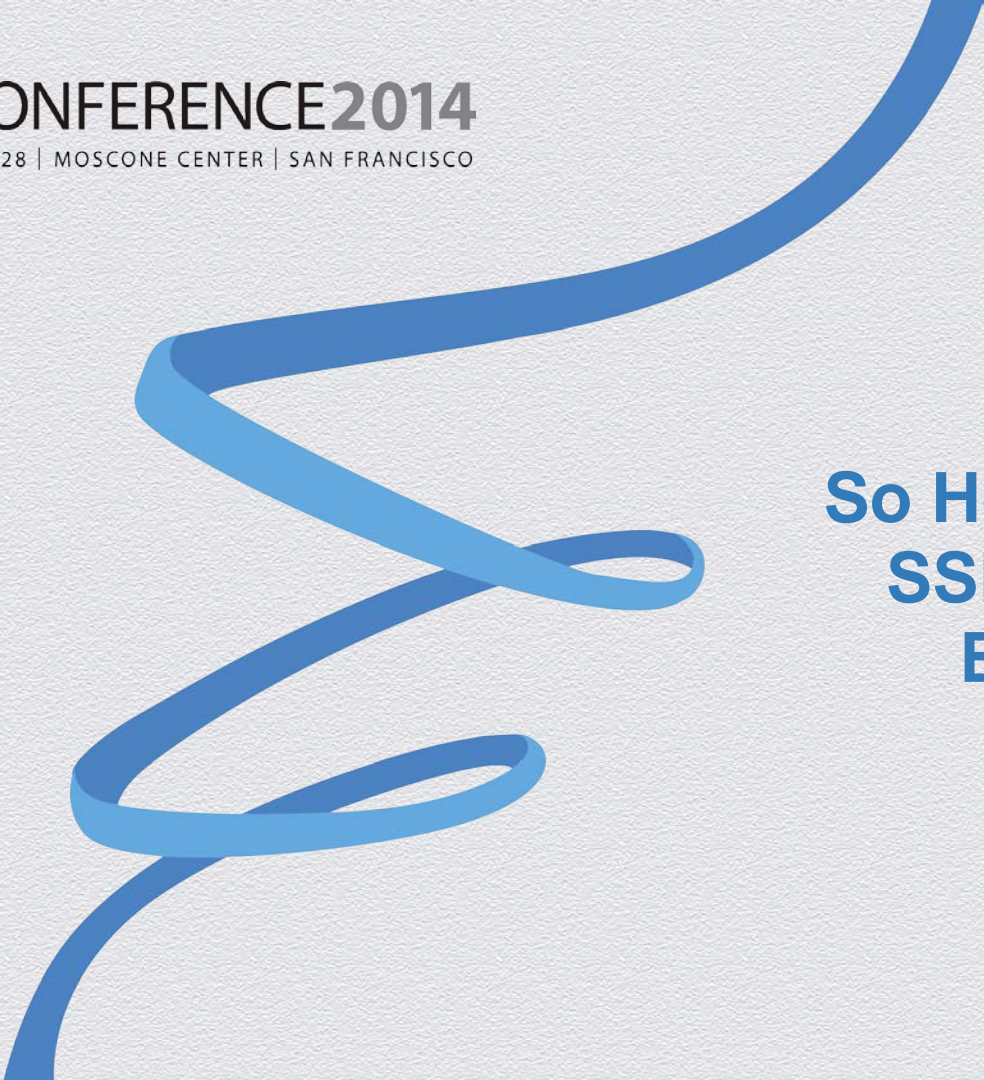
UDP:

- ◆ Maximum throughput for streaming (VoIP) data
- ◆ No built in encryption mechanism
- ◆ Packet loss or disorder may affect transmission



RSA[®]CONFERENCE2014

FEBRUARY 24 - 28 | MOSCONE CENTER | SAN FRANCISCO



**So How Can We Use
SSL & IPsec In A
Better Way?**

What can we do?

- ◆ Retune your system to regulate the buffer size
- ◆ Add 2 TCP/IP Stacks

RSA[®]CONFERENCE2014

FEBRUARY 24 - 28 | MOSCONE CENTER | SAN FRANCISCO



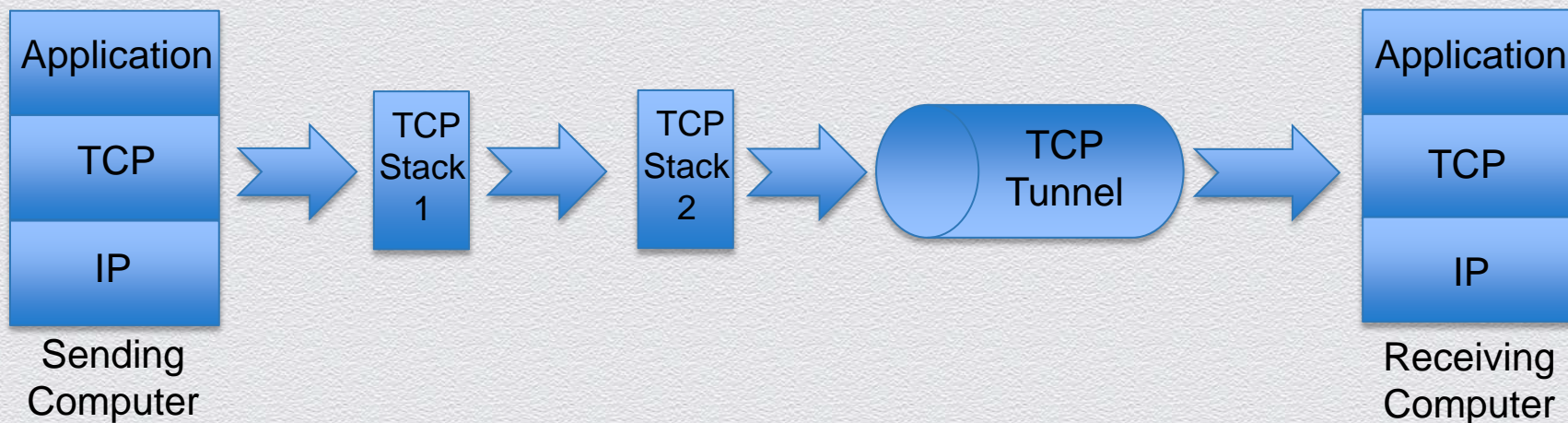
Using TCP Stacks To Improve Efficiency

What is a TCP Stack?

- ◆ Links the application to the network interface
- ◆ Terminates the TCP connection
- ◆ Establishes the TCP Tunnel
- ◆ Handles the network headers and packets
- ◆ Handles Flow Control

Tunnel with additional TCP Stacks

- ◆ The TCP Stacks regulate the data flow



So what does TCP Stack 1 do?

- ◆ TCP Stack 1:
 - ◆ Receives SYN request from sender application, sends to receiving application
 - ◆ Assesses the amount of data and compares it to the buffer size
 - ◆ If the allowed buffer size is not exceeded:
 - ◆ Sends End Zero Window command to TCP Stack 2
 - ◆ If the allowed buffer size is exceeded:
 - ◆ Sends Zero Window command to TCP Stack 2
 - ◆ Waits for an acknowledgement ACK from receiving application

So what does TCP Stack 2 do?

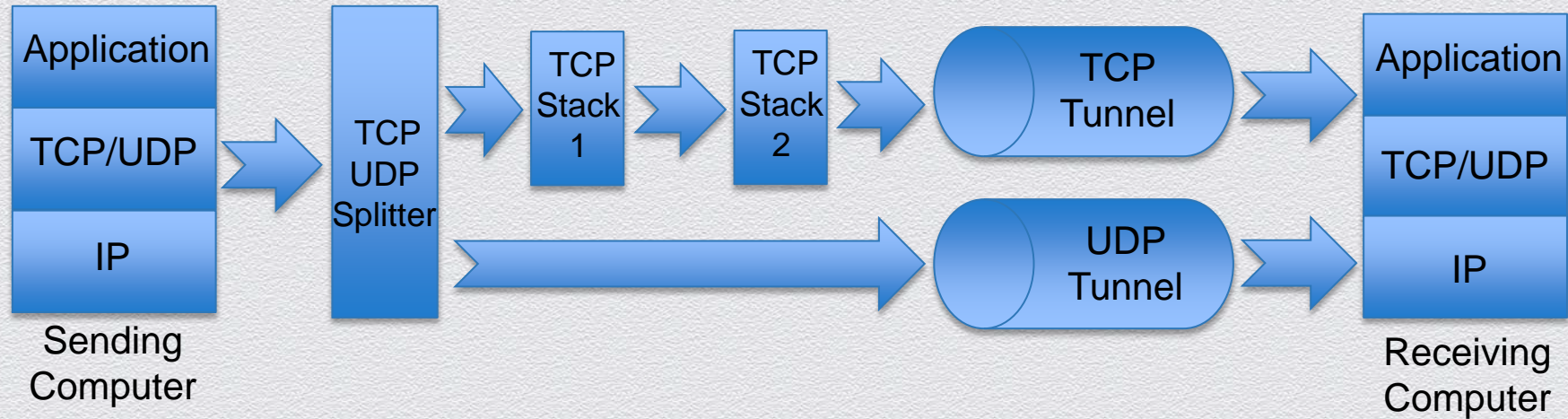
- ◆ TCP Stack 2:
 - ◆ Receives data from TCP Stack 1
 - ◆ Sends the data through an SSL tunnel to the receiving application

What about Real Time Streaming?

- ◆ Sending application performs a UDP discovery (sends a UDP packet to explore the network and see if blocked by firewalls)
- ◆ Receiving side also performs a UDP discovery
- ◆ TCP/UDP Splitter can now establish a TCP or UDP tunnel
- ◆ Sending application can apply SRTP encryption to the UDP stream
- ◆ If no UDP, then must use TCP
- ◆ Keep-alive packets must be regularly sent to keep connection open

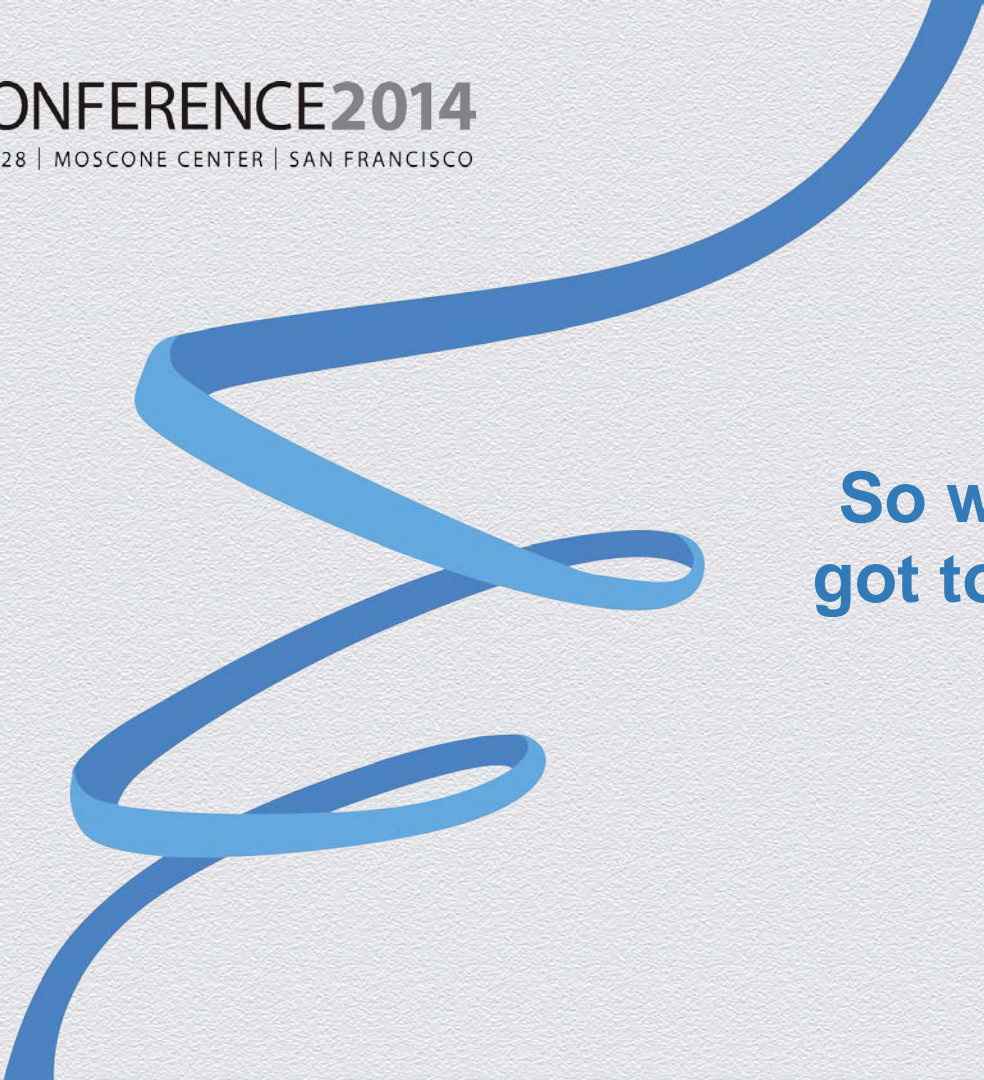
The TCP/UDP Splitter establishes a UDP Tunnel

- ◆ The TCP/UDP Splitter establishes a TCP and/or a UDP tunnel









RSA[®]CONFERENCE2014

FEBRUARY 24 - 28 | MOSCONE CENTER | SAN FRANCISCO



**So what has all this
got to do with SSL or
IPsec?**

What this means for IPsec communications...

- ◆ Inflexible - practical for site-to-site VPNs only, not mobile access? 
- ◆ Installation and updates necessary - expensive if running many clients? 
- ◆ Firewalls and proxies interrupt connection (port forwarding necessary)? 
- ◆ Data compression can make data transfer very slow? 
- ◆ Network address translation issues? 
- ◆ Unless properly terminated in DMZ or firewall, IPsec effectively makes a hole in your security – access to whole network, not specific servers? 

What this means for SSL communications...

- ◆ Computationally heavy load for client and SSL devices?
- ◆ Not as secure or as fast as IPsec?
- ◆ Network access not fully transparent?
- ◆ Not suitable for VoIP?



So what do you have now?

- ◆ All data traffic flows are fully regulated by the TCP stacks
- ◆ No bottlenecks or TCP meltdown
- ◆ Communication goes through an SSL-secured TCP/UDP tunnel
- ◆ Access from devices outside the network to the network application
- ◆ Access is fully network transparent

RSACONFERENCE2014

FEBRUARY 24 - 28 | MOSCONE CENTER | SAN FRANCISCO



How To Put This Into Practise

All this in real life

- ◆ Add the TCP Stacks to a tunnel endpoint in the network
- ◆ Let the TCP stacks regulate the data flow
- ◆ The TCP Stacks split the connection using built-in TCP/UDP Splitter
- ◆ Data is delivered directly, securely and transparently to the receiving network application
- ◆ No loss of data packets or VoIP transmissions

RSA CONFERENCE 2014

FEBRUARY 24 - 28 | MOSCONE CENTER | SAN FRANCISCO



Any Questions?