

November 27-29, 2012
South San Francisco Conference Center



Web **RTC**
CONFERENCE & EXPO



#web_RTC   

www.webrtcworld.com/conference/



November 27-29, 2012
South San Francisco Conference Center

Panel - Edges and Security

Jason Uberti
Software Engineer
Google
November 29, 2012



Panel Participants

- Patrick McNeil
 - Sr. Security Engineer
 - Acme Packet
- Mohan Palat
 - Product marketing
 - Sonus
- Jerry Ryner
 - CTO
 - Sansay



Web **RTC**
CONFERENCE & EXPO

November 27-29, 2012
South San Francisco Conference Center

Patrick McNeil, CISSP
Senior Security Engineer

ACME PACKET



acme *packet*

New 'access network' same session delivery challenges

Old challenges are new again ...

These may sound familiar if you experienced the first round of VoIP

- Mixing developers with Bob the telephone guy when he just got comfortable with the networking team
- Web developer understanding and use of security mechanisms in HTML5 and WS (failing since '93)
- Identity, authentication, authorization, and the notion of trust (IdP only part)
- Asset preservation while developing new revenue streams

and

Assuring Security, Service Reach, Service Assurance, and Regulatory Compliance – which are usually left until last!

The challenges to address...

sound suspiciously like gateway or SBC territory.

Security

- CORS enforcement
- Limit protocols (ex: SIPoWS, REST, ROAP, XMPP)
- HTTPS / WSS
- DoS / dynamic blacklisting
- Dynamic port management
- IdP token / session management

Service reach

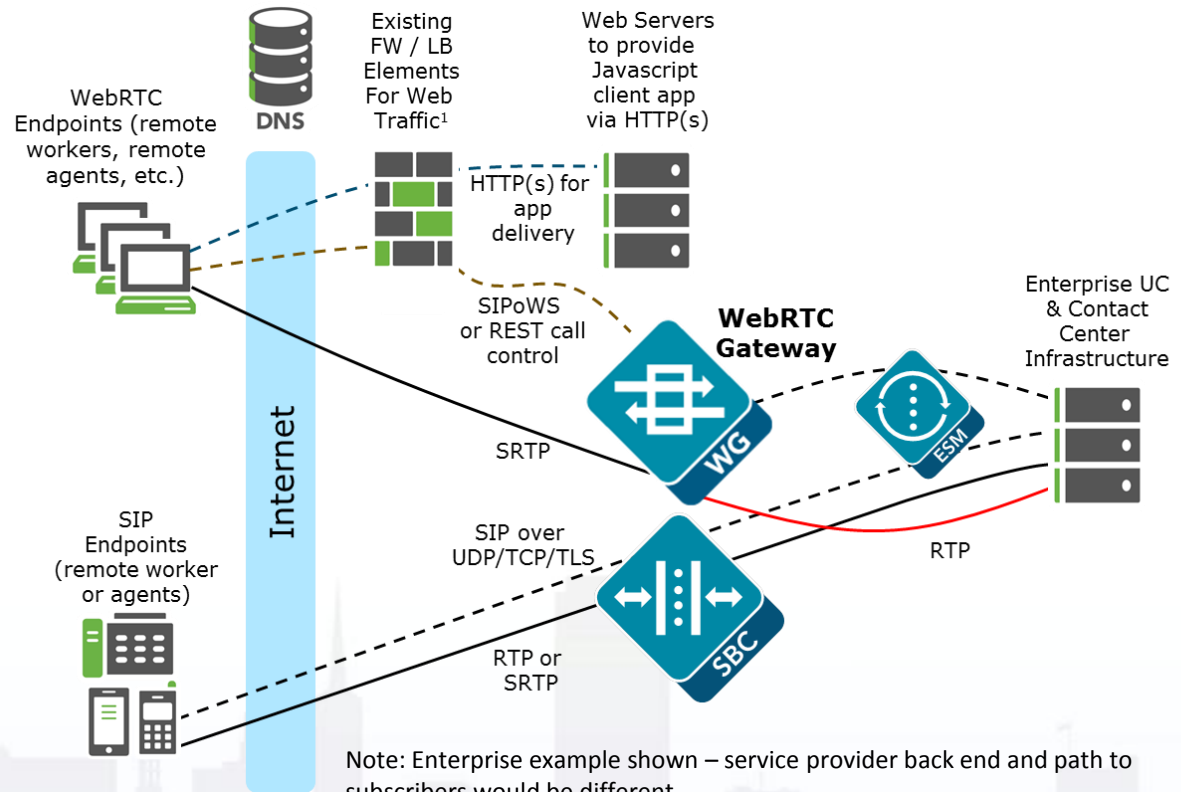
- Interwork to SIP
- Media – differing suppt. for ICE, STUN/TURN, transcoding
- IPv4 <-> IPv6
- NAT traversal

Service assurance

- HA & load balancing
- QoS, QoE

Regulatory compliance

- Direction to media recorders
- Call details, logging, etc at boundaries



Enterprise UC & Contact Center Core



Web RTC
CONFERENCE & EXPO

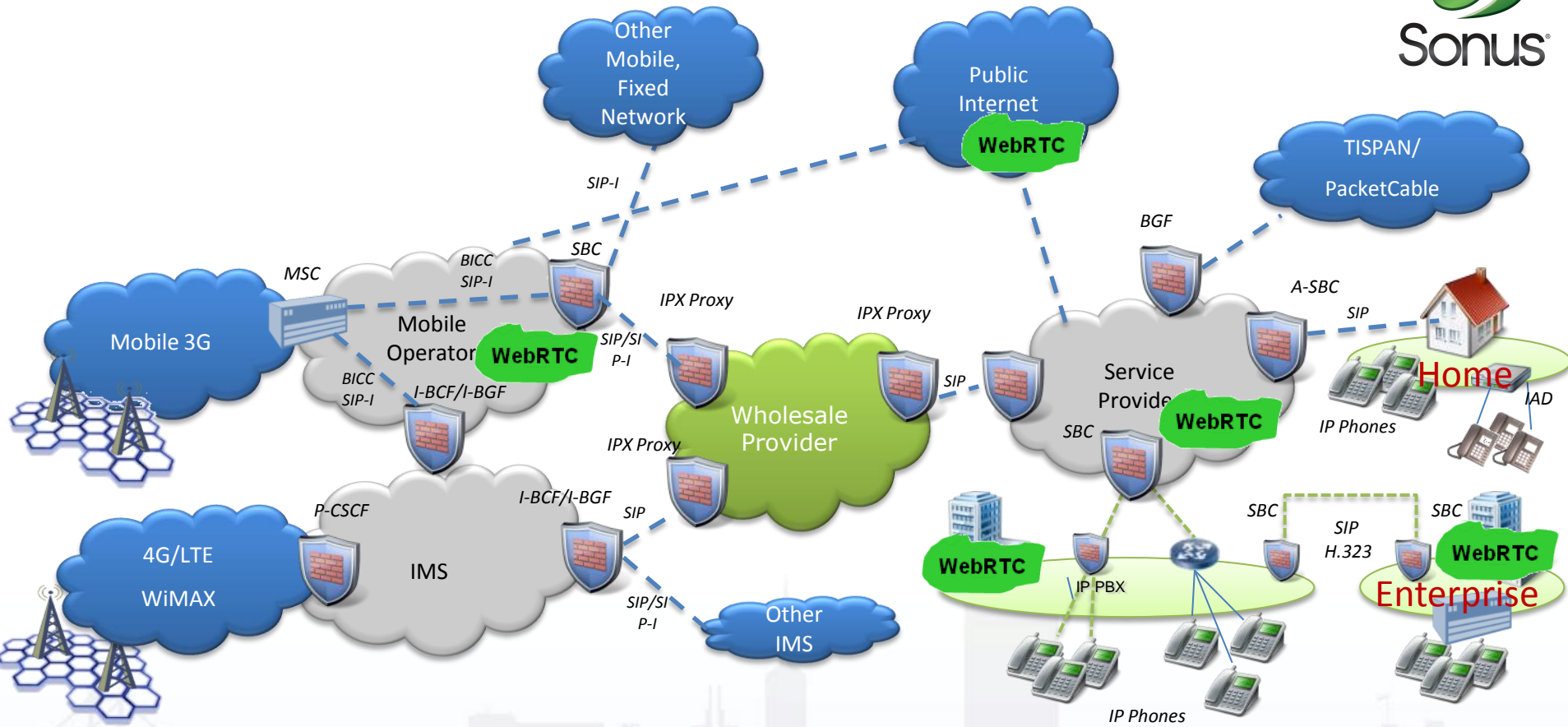
November 27-29, 2012
South San Francisco Conference Center

Mohan Palat
Senior Product Marketing Manager

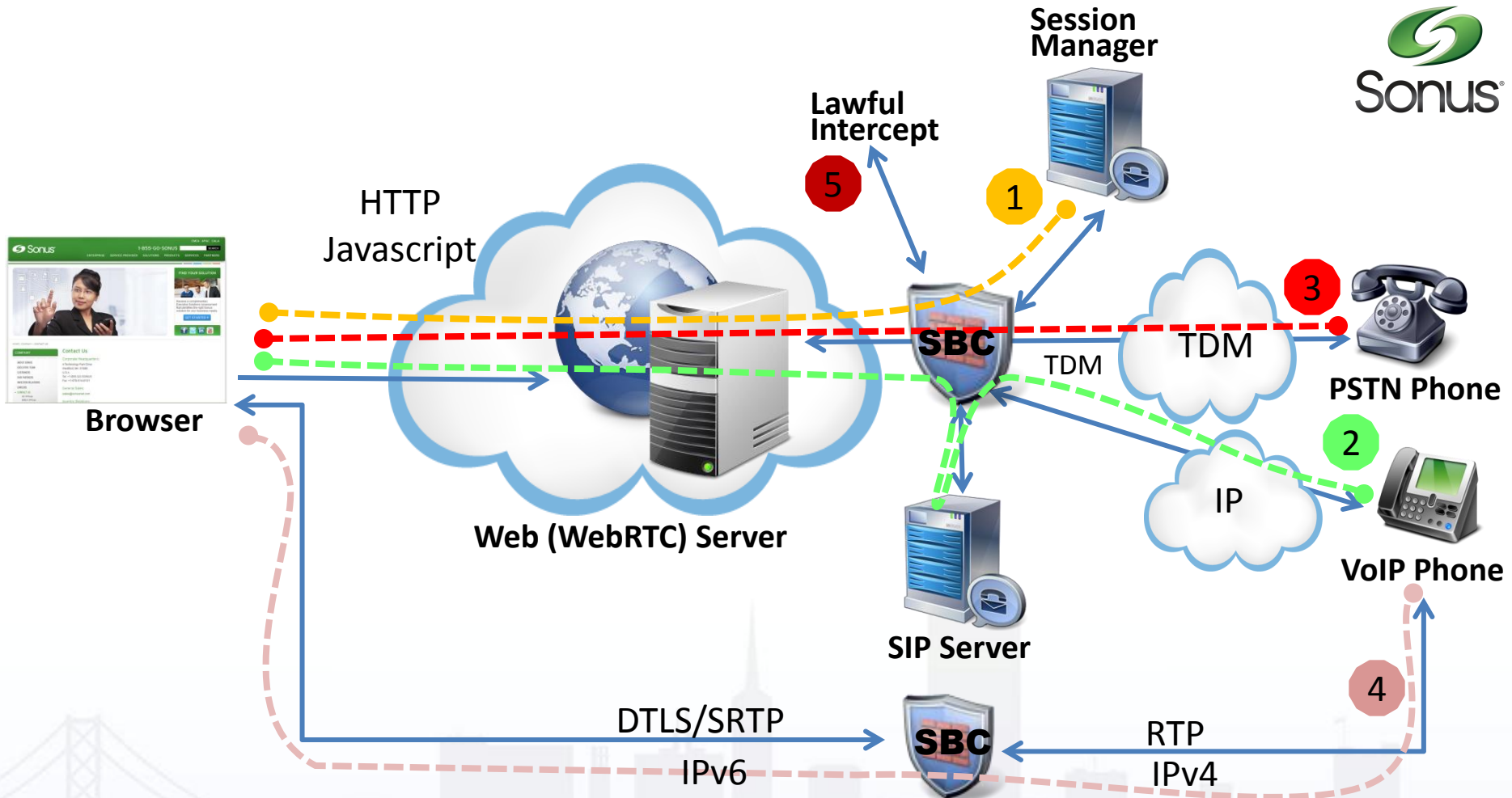
SONUS



Overlaying with WebRTC Deployment Areas...



SBC in WebRTC – Use Cases





Web RTC
CONFERENCE & EXPO

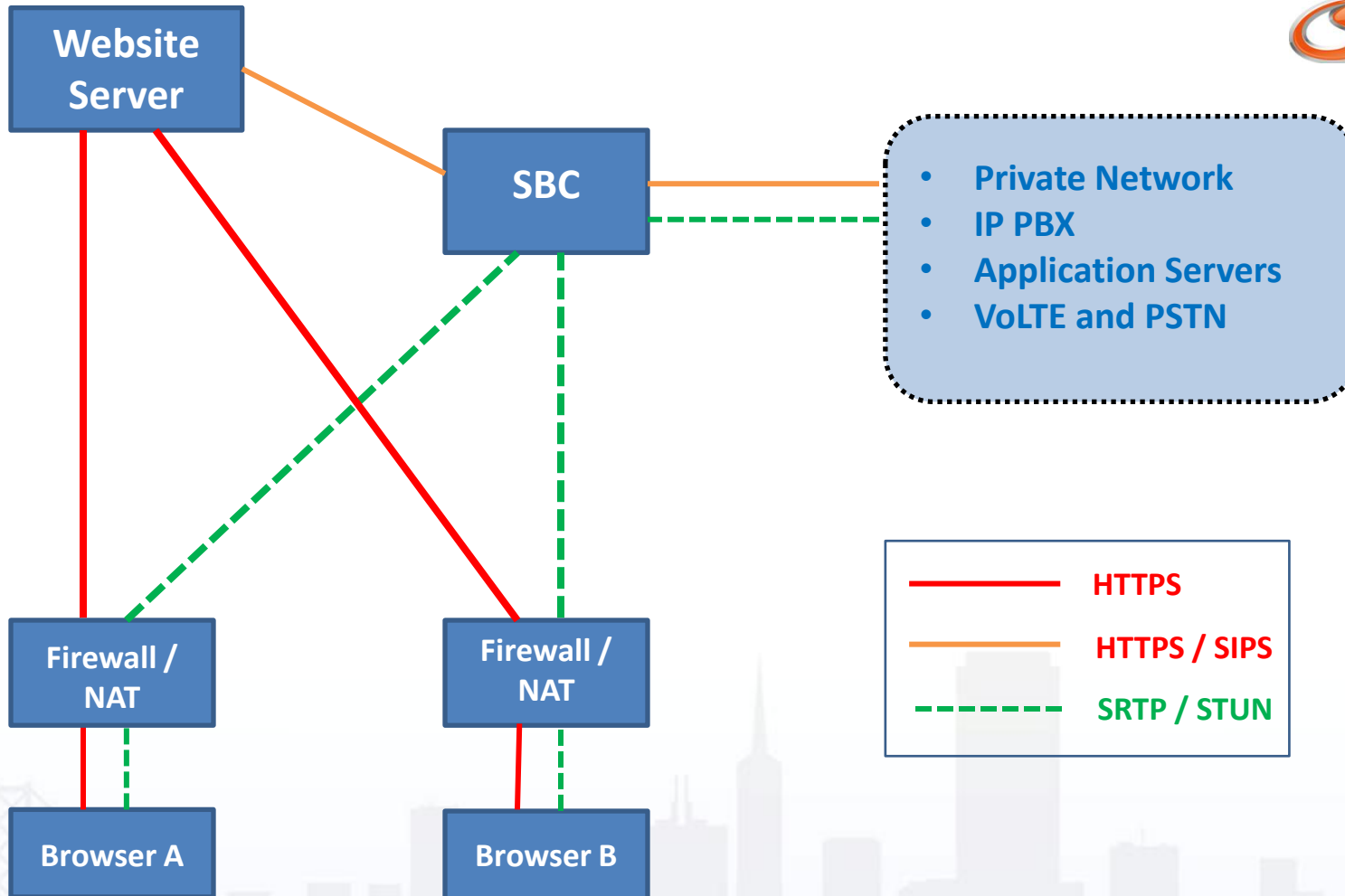
November 27-29, 2012
South San Francisco Conference Center

Jerry Ryner
CTO

SANSAY



WebRTC with SBCs



WebRTC Security and Protection

Theft of Service

- Eavesdropping
- Unauthorized Access

Solution

- HTTPS and SRTP
- Login Credentials and Certificates

Denial of Service

- Website DOS/DDOS
- SBC DOS/DDOS

Solution

- TCP/HTTPS Rate Limiting and IP Tracking
- Strict ACLs for HTTPS/SIPS Interface
- STUN Authentication for SRTP Interface

SBC vs. TURN

- TURN uses long term credentials and must accept client authentication requests
- TURN uses same interface for control and media and requires client media encapsulation
- SBC has strict control interfaces and does not require long term client authentication
- SBC media relay ports are not locked to any one interface and require no media encapsulation
- SBC has knowledge of media type, bandwidth, priority, and application treatment

Panel Questions

- What are the top 3 security vulnerabilities in WebRTC, and what are their implications?
- Does the SBC address all the WebRTC security needs? Or, do we need other security WebRTC elements/functions?
- What are the additional features that an SBC should have to support WebRTC?
- Is the SBC critical in securing WebRTC? Can WebRTC operate securely without an SBC?
- If I put a WebRTC server in the DMZ do I need an SBC?
- Do I need an SBC for client support in the enterprise, especially if it is designed to work in the open internet?
- Do SBC functions and media server functions need to come together for WebRTC?



November 27-29, 2012
South San Francisco Conference Center

Thank You

Jason Uberti
Software Engineer
Google

