
The Pros and Cons of SSL:

Your Content's Hidden, But Your Content's Hidden

Michael Valladao - Product Management, Network General
Pete Davis - VPN PLM, Cisco Systems, Inc.

Agenda

- Background trends and history regarding Web encryption and cryptology
- Why SSL is becoming pervasive and a critical component of the networking infrastructure
- The associated drawbacks (mostly troubleshooting)
- A review of how SSL works & how to capitalize on it
- A look at VPN as a model for the future
- Suggested methodologies to best utilize SSL in your environment

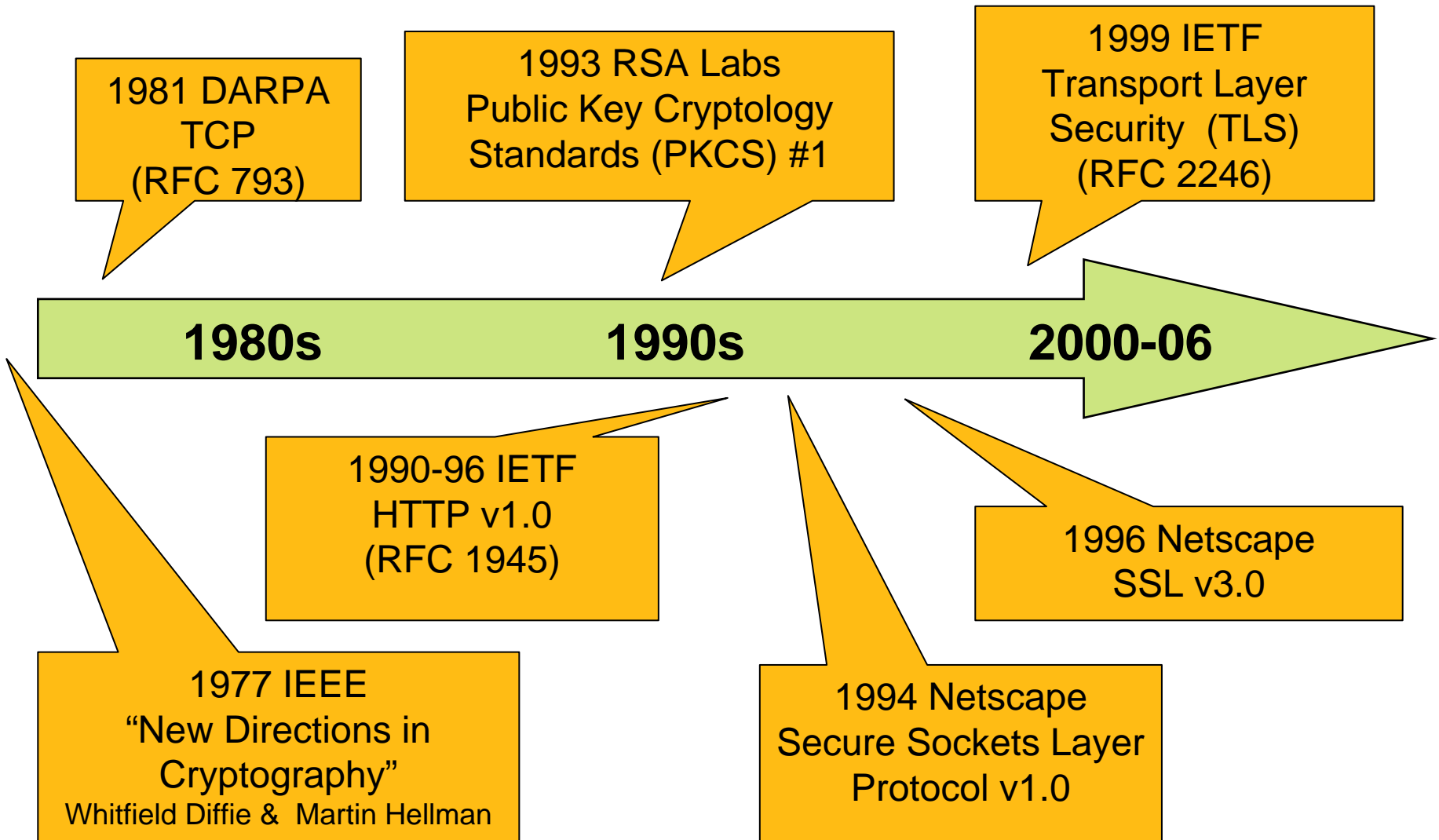
Quick Overview

- SSL (Secure Sockets Layer) is:
 - Often used as a generic term, but is actually a Netscape protocol that was improved in the IETF
 - Used to transmit private data across the Internet in a secure format
 - Supported on almost every browser
 - *Normally* is used with HTTP but sent over port 443
 - TLS (SSL 3.1) is approved by the Internet Engineering Task Force (IETF) as a standard
 - Easily identified to the user

 <https://www.aa.com/apps/AAdvantage/ViewMyMiles.jhtml>;



Historical: How did we get here w/ SSL?



SSL Benefits: *(Your Content's Hidden)*

- Rapidly becoming the favored secure Remote Access (RA VPN) method
 - Provides a secure channel for communication
 - The data is encrypted, usually with RC4 or 3DES
 - Provides protection from: interception, impersonation, eavesdropping
 - Accessible from many locations, not just the user's normal PC
 - Clientless easy to use when IPsec VPNs are overkill
 - Less setup

SSL Benefits - continued

- SSL is well suited for:
 - Finance, e-business, sales records, and HR
- Provides for an element of “customer trust”
- Helps meet the needs of regulatory requirements
 - Sarbanes Oxley (SOX)
 - Health Care (HIPAA)

SSL Drawbacks: *(Your Content's Hidden)*

- Heavy resources are consumed to encrypt and decrypt the data on the corporate gateway



- In addition to credit card information, critical **troubleshooting** components are also hidden...

- For example, you cannot see:

- URL path
- SQL queries or responses
- Passed parameters
- Application breakouts

```
Summary
TCP: D=3020 S=80 SYN ACK=565096535 SEQ=4213665515 LEN=0 WIN=0
TCP: D=80 S=3020 ACK=4213665516 SEQ=565096535 LEN=0 WIN=0
HTTP: C Port=3020 GET /slv/v4/2.html?.pc=&.a=0&.ta=cgnone,co
SSLv3: Application Data
TCP: D=443 S=3021 SYN ACK=0 SEQ=565132542 LEN=0 WIN=65535
TCP: D=3021 S=443 SYN ACK=565132543 SEQ=1239443992 LEN=0 WIN=0
TCP: D=443 S=3021 ACK=1239443993 SEQ=565132543 LEN=0 WIN=0
SSLv3: Handshake(Client Hello)
SSLv3: Application Data
SSL: Continuation of frame 57: (1/6) 1460 Bytes of data
SSL: Continuation of frame 57: (2/6) 1460 Bytes of data
SSL: Continuation of frame 57: (3/6) 1460 Bytes of data
```

Troubleshooting Drawbacks -continued

- These drawbacks apply to more than just SSL
- Anytime data is encrypted or obscured by tunneling (or even compression), it impedes analysis
- This applies to SSL, IPsec, multicast, and various forms of non-secure tunneling
- The techniques used to overcome these obstacles are the same

How SSL VPNs work

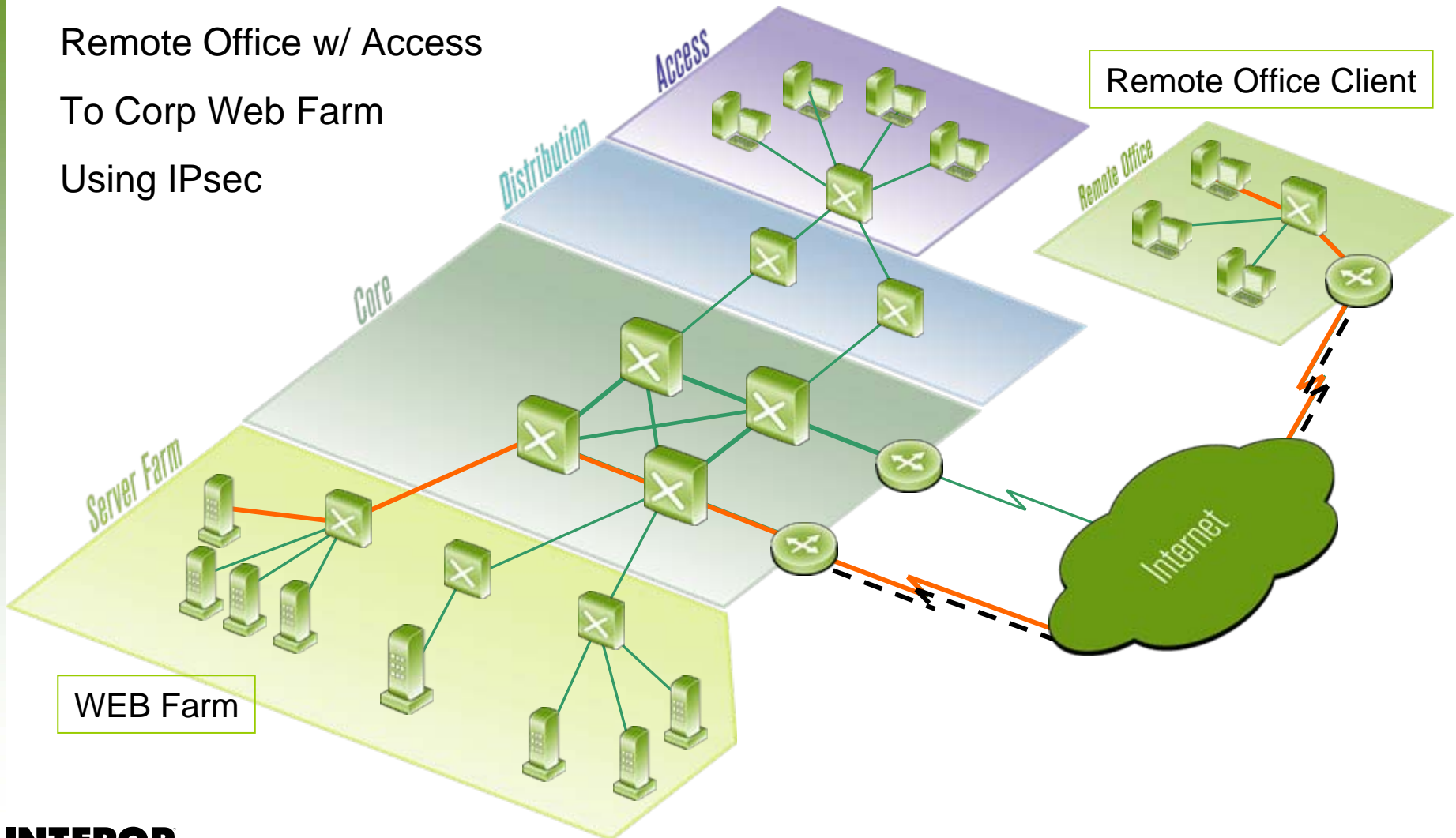
- Clientless SSL remote access VPNs are usually sophisticated “reverse proxies”
- They terminate both SSL and HTTP in the gateway, and act as proxies for web servers on the LAN
- The hardest thing here is to re-write all the internal URLs so that the remote user has a seamless web experience
- Clientless SSL VPNs don't provide full LAN access, just access to some services, like web pages and webified file shares
- Most modern SSL gateways offer dynamic SSL VPN clients that let them look a lot more like IPsec gateways, but these are more work to manage than true clientless access

VPN as an SSL Model

- Virtual Private Networks (VPN) utilizing SSL as the transport are widely available from vendors
- Those deploying e-business, financial, HR, or healthcare related web applications can benefit from SSL VPNs
- SSL VPNs utilize TCP port 443 for traffic instead of Protocol-50 (ESP) and UDP-500 (IKE) for typical IPsec traffic, making them more compatible with extranet firewall and proxy configurations

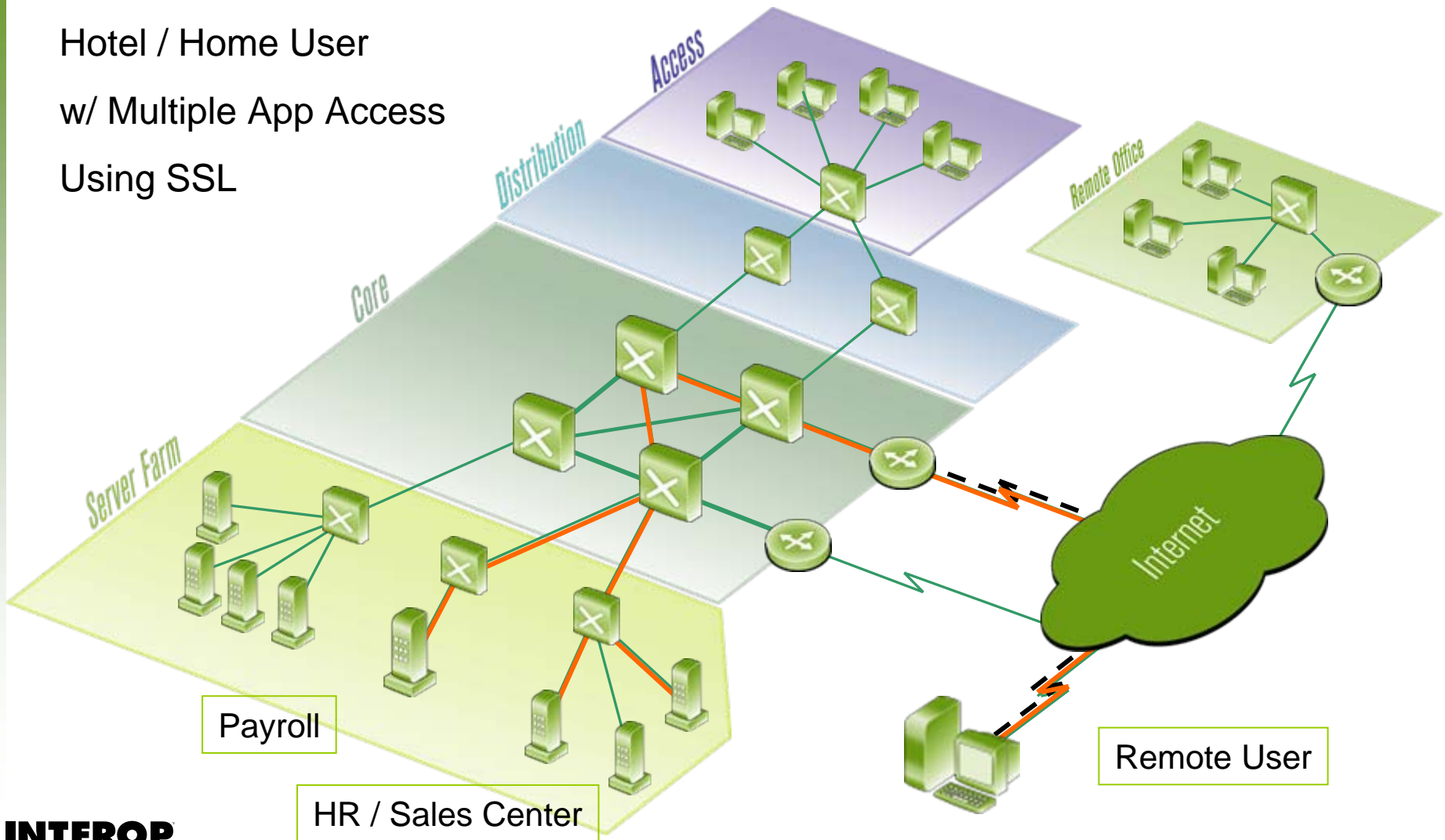
VPN Deployment Scenario #1

Remote Office w/ Access
To Corp Web Farm
Using IPsec



VPN Deployment Scenario #2

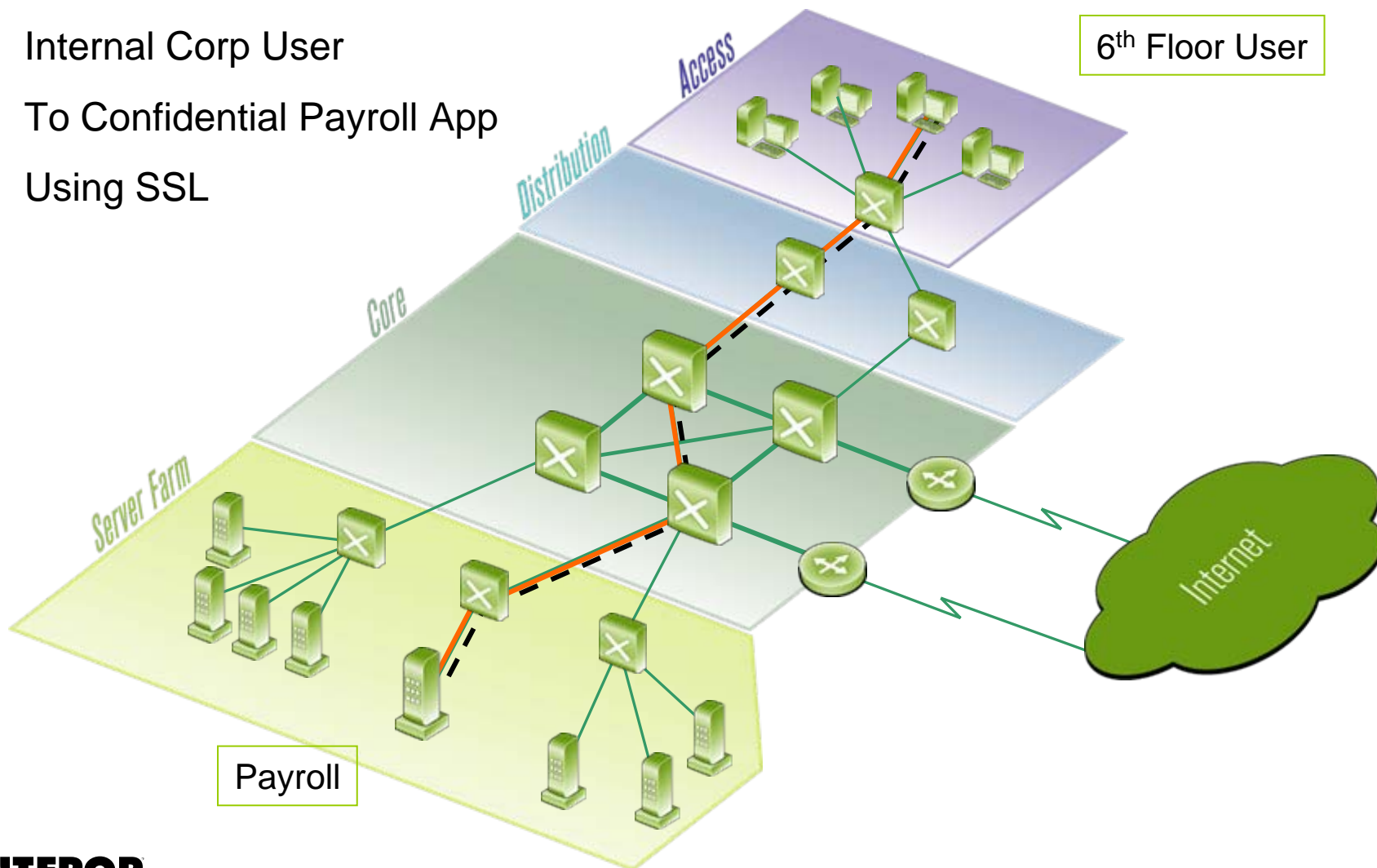
Hotel / Home User
w/ Multiple App Access
Using SSL



SSL Deployment Scenario #3

Internal Corp User
To Confidential Payroll App
Using SSL

6th Floor User



Encrypt at the Edges

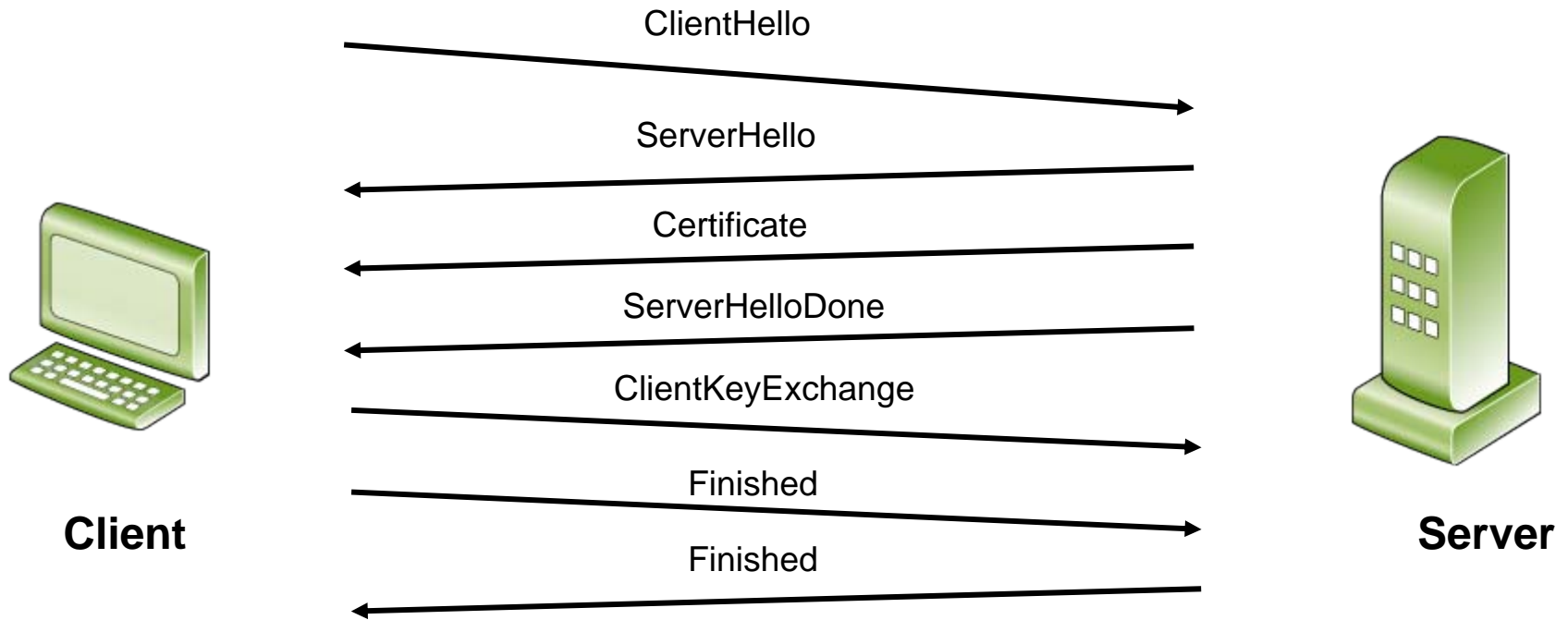
- You can reduce the amount of encryption in the LAN by putting SSL VPN gateways as far out on the “edge” as you can
- The main tradeoff is whether or not you feel you need to encrypt within your LAN, such as for regulatory/compliance needs
- If needed, many SSL gateways can do SSL within the LAN, so you can have both cleartext and encrypted text coming from the gateway

Design Decisions

- In many organizations, it is far from clear where the edge is, so deciding where to put SSL gateways needs to be done with your network architects
- Putting the gateway too far in keeps the traffic encrypted longer, but...
- Putting the gateway too far out keeps the traffic in the clear longer

SSL Cryptography

- It all begins with a simple handshake...



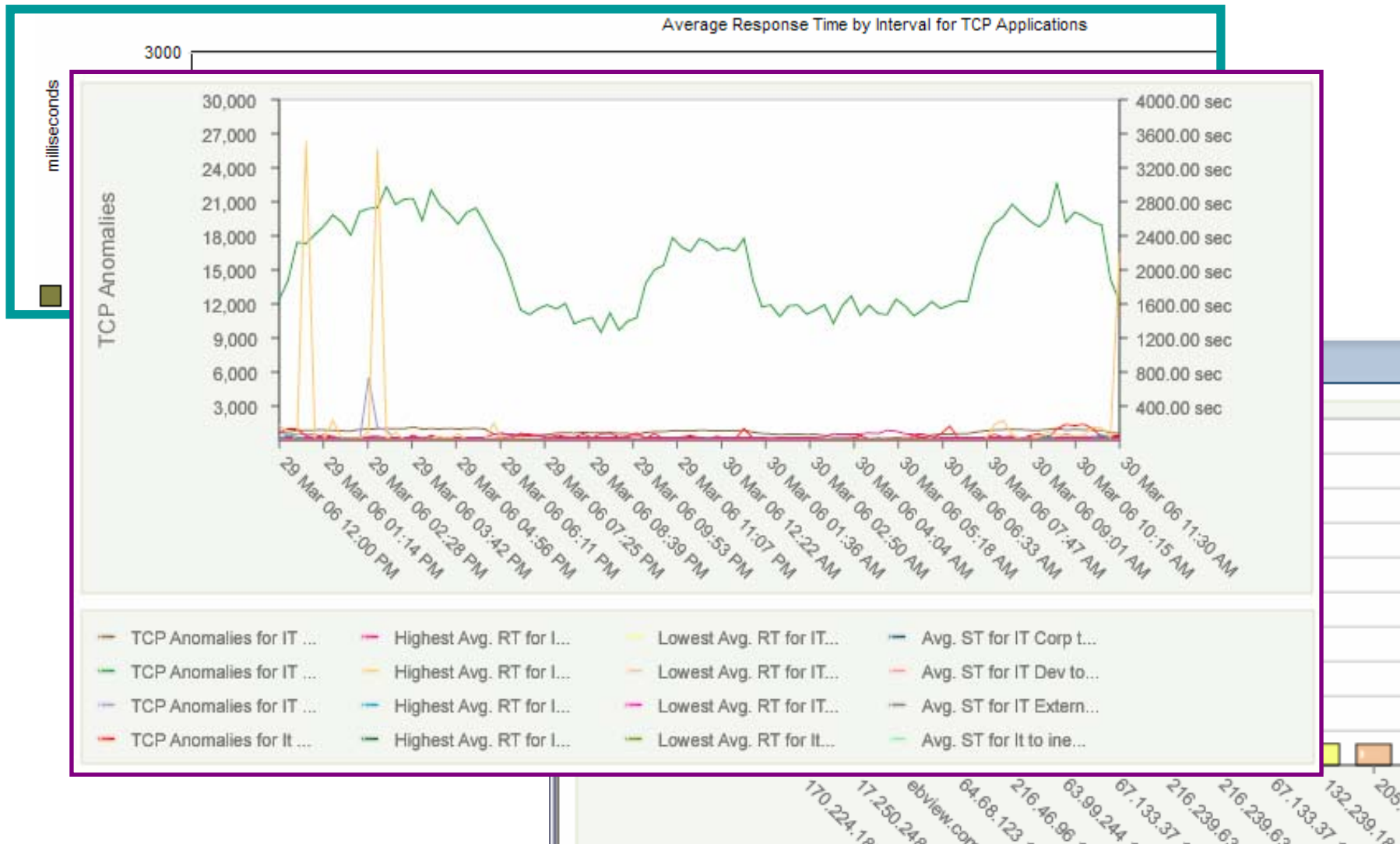
SSL Packet Analysis

Packet Decode

Packet 76, file 'Https.cap'

- DLC: ----- DLC Header -----
 - DLC:
 - DLC: Packet 76; packet size is 119 (0077 hex) bytes.
 - DLC: Destination = Station 1120E29EBF
 - DLC: Source = Station Supermicro 28EDE0
 - DLC: Ethertype = 0800 (IP)
 - DLC:
- IP: ----- IP Header -----
 - IP:
 - IP: Version = 4, header length = 20 bytes
 - IP: DiffServ Field = 00
 - IP: 0000 00.. = DSCP - 0 , Best Effort
 - IP:00 = ECT - Transport protocol will not participate in ECN
 - IP: Total length = 101 bytes
 - IP: Identification = 58074
 - IP: Flags = 0X
 - IP: .0.. = may fragment
 - IP: ..0. = last fragment
 - IP: Fragment offset = 0 bytes
 - IP: Time to live = 128 seconds/hops
 - IP: Protocol = 6 (TCP)
 - IP: Header checksum = 0x6F3A (correct)
 - IP: Source address = [172.21.72.163]
 - IP: Destination address = [172.21.71.176]
 - IP: No options
 - IP:
- TCP: ----- TCP header -----
- SSL: ----- Record Layer -----
 - SSL:
 - SSL: Content Type = Handshake (22)
 - SSL: Version = SSLv3 (3.0)
 - SSL: Payload Length = 56
 - SSL: -- Handshake Message --
 - SSL: Encrypted/Compressed or Unknown Handshake Type
 - SSL:
- DLC: Packet padding= 4 bytes

HTTPS Statistical Data – Easily Done



SSL Decryption Methods

- The master secret key is required to properly decrypt a given packet within a session
- If the entire packet stream is available, knowing the server private key is often enough to decrypt in post-capture
 - Ssldump is open source
- Key management is important
 - Must work with security team and auditors
 - Some products work within a vaulted environment
 - Need to decide if key transport is over secure link or disk

SSL Decryption Methods

SFA_SSL_trace.cap: Decode, 52/251 Ethernet Frames

No.	Status	Source Address	Dest Address	Summary	Len (Byte)	Rel. Time
51		[172.21.72.193]	data.msg.yahoo2.ak	HTTP: C Port=3020 GET /siv/v4/2.html?pc=&.a=0&.ta=cgnone.ccn	542	0:00:01
52		[172.21.72.193]	[172.21.72.201]	SSLv3: Application Data	420	0:00:01
53		[172.21.72.193]	[172.21.72.201]	TCP: D=443 S=3021 SYN ACK=0 SEQ=565132542 LEN=0 WIN=65535	62	0:00:01

IP: Identification = 24032
IP: Flags = 4X
IP: .1.. = don't fragment

```
00000000: 00 30 48 2d b2 64 00 03 47 6d f2 d8 08 00 45 00 .OH-²d..Gmò@..E.  
00000010: 01 96 5d e0 40 00 80 06 b1 cc ac 15 48 c1 ac 15 .]ä@...î-.HÁ-.  
00000020: 48 c9 0b ca 01 bb 21 ad ac a2 9a 16 cd c0 50 18 HE.E.»!-~c|.IÂP.  
00000030: fb 4a ae 9d 00 00 17 03 00 01 69 67 41 3d 90 ee úJ@...ligA=.i  
00000040: 7a 91 b3 69 e6 a3 43 32 99 fa e0 21 02 bd 13 e7 z'³iæfC2.úà!.%ç  
00000050: b9 f6 d6 2c 61 bc b0 fd 6f 9f 82 a0 6a 49 7d 2b 'dÖ,a4'yo|| jI}+  
00000060: 73 73 1d 5e 19 26 40 38 66 48 4d 0a 84 75 65 fa ss.^.&@8fHM.¡ueú  
00000070: 6c e2 3f 49 65 f0 95 97 c9 e5 f4 ae 07 e7 58 b2 lá?Ieö||Éäó.çX²  
00000080: 26 fb 7a 8b bf 72 02 59 e1 05 36 08 26 f4 e1 e7 &úz|çr.Yá.6.&óâç  
00000090: de c4 f6 24 d4 fd d0 5b 49 a9 cd ec 5e d6 26 f9 bÄñSÖwPIT@fi^Ö&ð
```

Before

SFA_SSL_trace_new.cap: Decode, 18/70 Ethernet Frames

No.	Status	Source Address	Dest Address	Summary	Len (Bytes)	Rel. Time
17		[172.21.72.193]	data.msg.yahoo2.ak	HTTP: C Port=3020 GET /siv/v4/2.html?pc=&.a=0&.ta=cgnone.ccn	542	0:00:00
18		[172.21.72.193]	[172.21.72.201]	HTTP: C Port=3018 GET /ResourceManager/css/ng_style.css HTTP/	399	0:00:00
19		[172.21.72.201]	[172.21.72.193]	HTTP: P Ports=3018 HTTP/1.1 Status=200	9054	0:00:00

IP: Identification = 24032
IP: Flags = 4X
IP: .1.. = don't fragment
IP: ..0..... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 128 seconds/hours

```
00000000: 00 30 48 2d b2 64 00 03 47 6d f2 d8 08 00 45 00 .OH-²d..Gmò@..E.  
00000010: 01 96 5d e0 40 00 80 06 b1 cc ac 15 48 c1 ac 15 .]ä@...î-.HÁ-.  
00000020: 48 c9 0b ca 00 50 21 ad ac a2 9a 16 cd c0 50 18 HE.E.P!-~c|.IÂP.  
00000030: fb 4a ae 9d 00 00 47 45 54 20 2f 52 65 73 6f 75 úJ@...GET /Resou  
00000040: 72 63 65 4d 61 6e 61 67 65 72 2f 63 73 73 2f 6e rceManager/css/n  
00000050: 67 5f 73 74 79 6c 65 2e 63 73 73 20 48 54 54 50 g_style.css HTTP  
00000060: 2f 31 2e 31 0d 0a 41 63 63 65 70 74 3a 20 2a 2f /1.1..Accept: */
```

After

Best Practices Summary

- Plan ahead
- Design your SSL deployment with a good balance of security and analysis capabilities
- Limit your SSL footprint to increase your troubleshooting options
- Troubleshoot data from clear locations when possible
- Monitor / analyze HTTPS with statistical data
- When required, decrypt the SSL packets

Q & A Session

psd@cisco.com
michael.valladao@networkgeneral.com