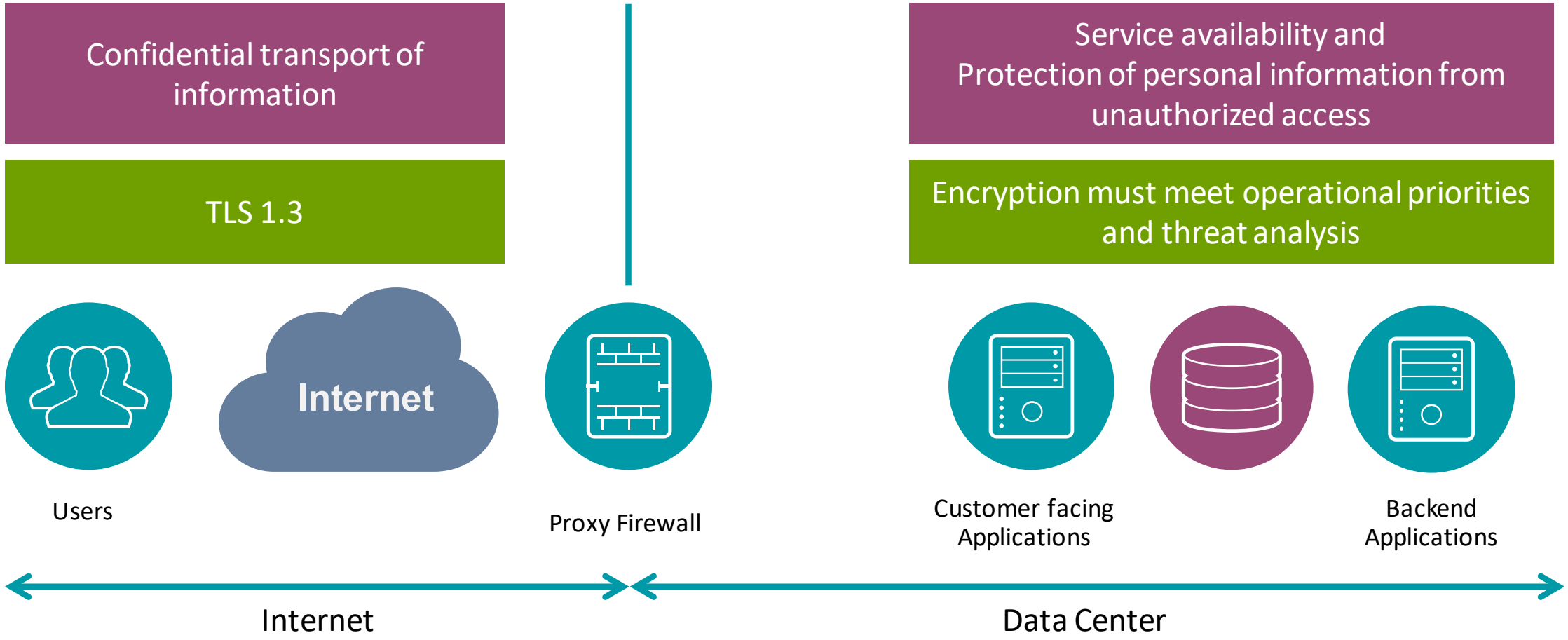
Managed Diffie-Hellman

Paul Barrett
CTO, Enterprise
NETSCOUT SYSTEMS

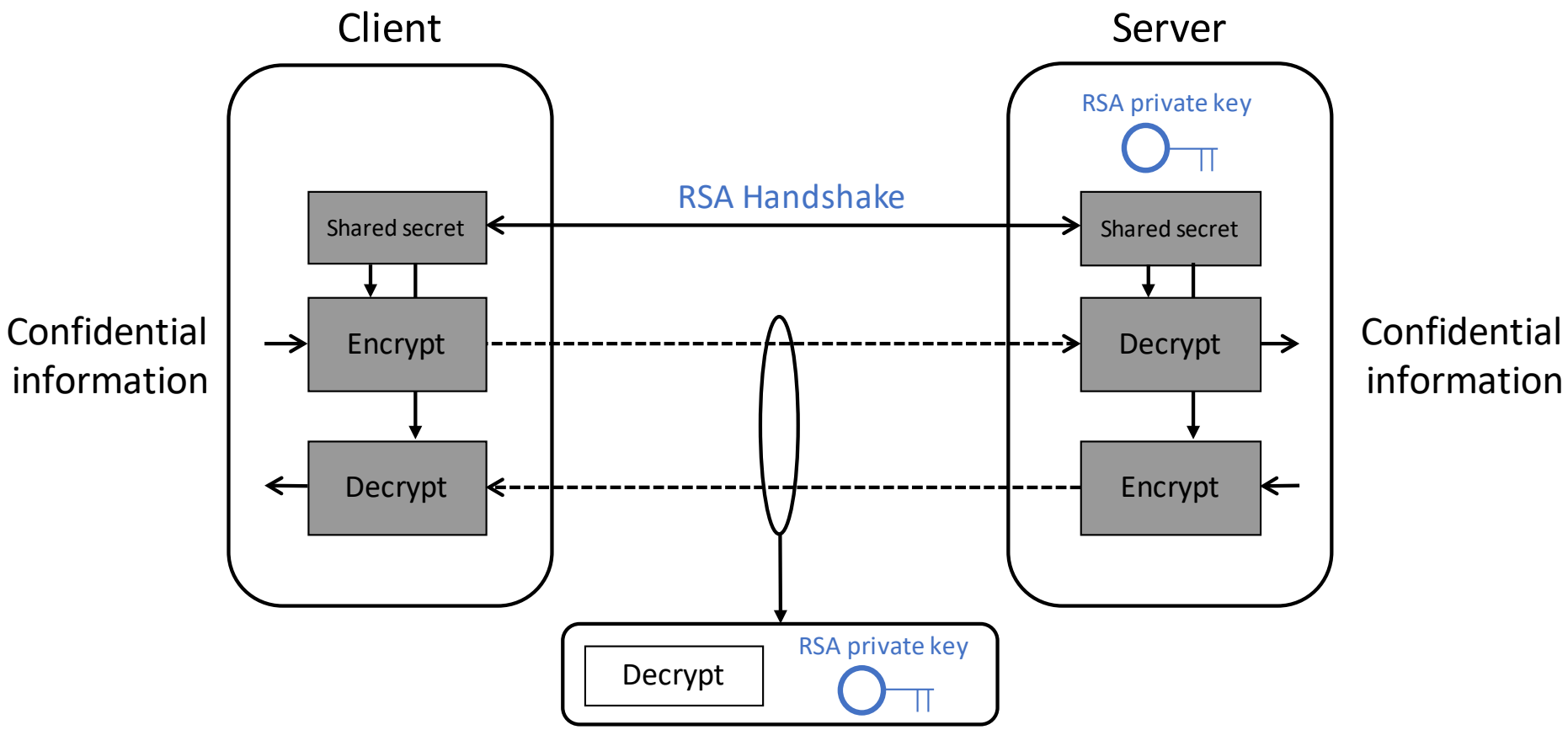
NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Encryption in the Data Center

Encryption considerations for the Internet are different from the Data Center

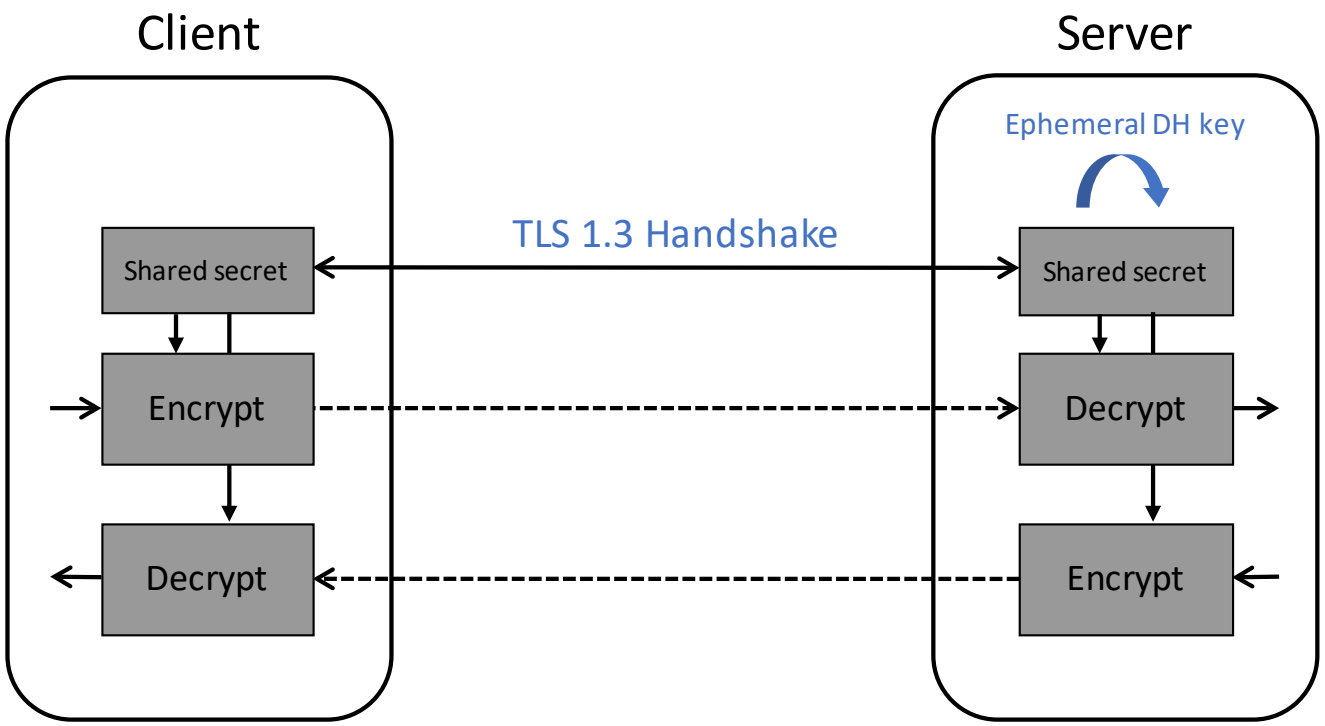


Decrypting traffic with RSA

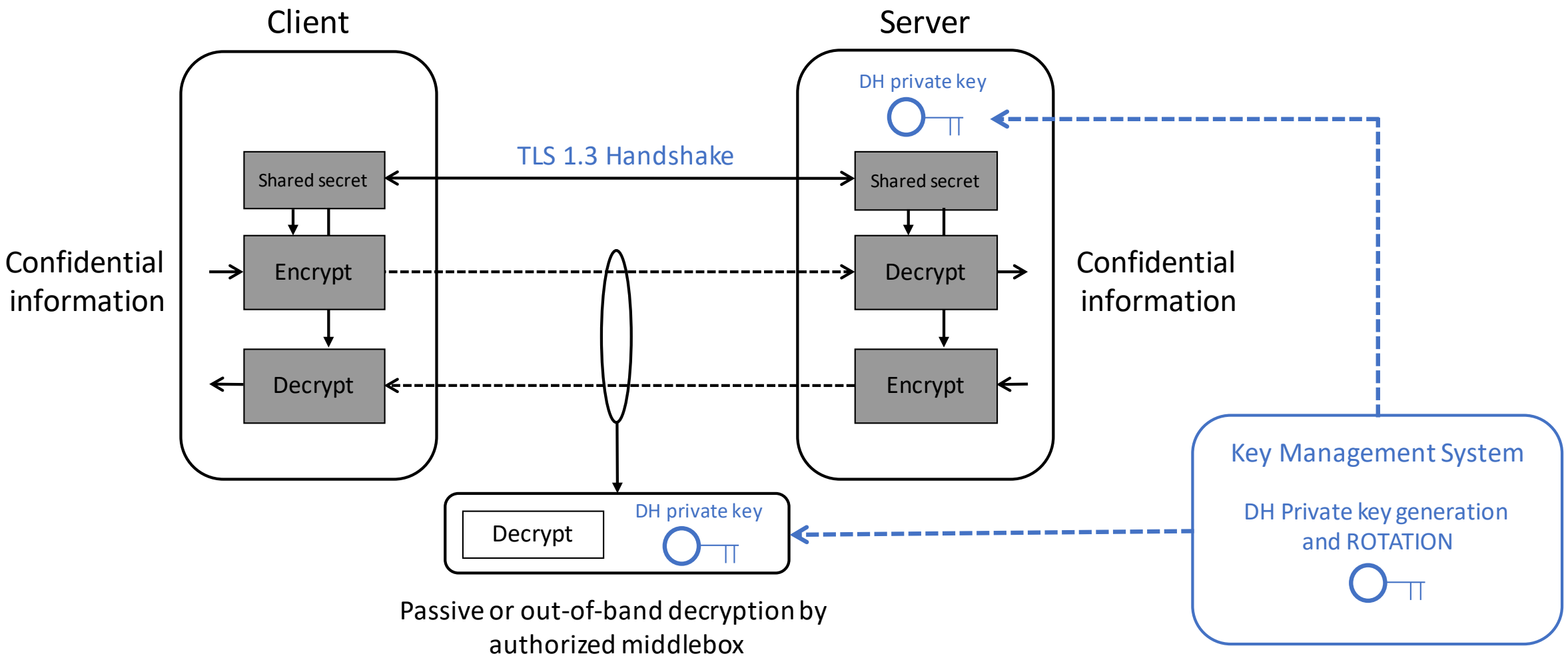


Passive or out-of-band decryption by authorized middlebox

TLS 1.3 and Ephemeral DH



Managed Diffie-Hellman



TLS 1.3 and Managed DH

Features	TLS 1.3	Managed DH
Compatible with all TLS 1.3 clients	✓	✓
Diffie-Hellman Handshake	✓	✓
Fast session re-establishment	✓	✓
Encrypted certificate information	✓	✓
Immune to masquerading	✓	✓
Per-session forward secrecy	✓	
Forward secrecy through key rotation		✓

FAQ

- Does this work with standard TLS implementations?
  - Works with all TLS 1.3 clients
  - Requires TLS server stack that supports TLS 1.3 with an externally provided Private DH key
- What is the exposure from key retention?
  - Devices performing real-time decryption only need current key and next key
  - Keys for post-capture decryption can be securely stored centrally
- Isn't searching for the correct key slow?
  - No: the Client Hello Random can be used an index into a hash table
- What is the correct key rotation period?
  - That is for the data center operator to decide
- When is true Forward Secrecy achieved?
  - When all copies of the private DH key are deleted
  - However, key rotation is far more robust than static keys with lifetimes of months or years

Status

- Managed Diffie-Hellman
  - Requires TLS 1.3 server stack with support for externally provided Diffie-Hellman keys
  - OpenSSL fork available on ETSI git repository with required functionality
- Proof of Concepts using ETSI implementation include
  - Use of ETSI TLS stack to provide web pages over TLS 1.3 to a commercially available browser
  - Secure key distribution of rotating Diffie-Hellman private keys to web server using Venafi Trust Protection Platform
  - Post Capture decryption of web pages using rotating Diffie-Hellman private keys in NETSCOUT nGeniusONE Service Assurance Platform

Packet decode in nGeniusONE

nGeniusONE | All Modules | Data Mining | Device Configuration | ADMINISTRATOR

Packet Decode

Filter - 1 | 11:29:59.207 AM - 11:29:59.337 AM BST | Filtered Packets : 17 | Processed Packets: 358 | Filter Complete

Packet	Absolute Time	Delta Time	Length	Source	Destination	Interpretation	Status
114	11:29:59.207.674.503 AM BST	0.009.965.147	74	10.20.53.134			
116	11:29:59.207.951.268 AM BST	0.000.230.913	74	10.20.53.136			
117	11:29:59.208.010.035 AM BST	0.000.058.767	66	10.20.53.134			

```
PACKET: #126 2020/10/16 10:29:59.329.854.672(UTC); Length=321 byt
ETHERNET: S=[00-50-56-97-56-C4], D=[00-50-56-97-01-2C], EtherType
IP:  S=10.20.53.136 D=10.20.53.134 LEN=287,  ID=38190, Offset=0,
TCP: S=443 D=42086 LEN=255  SEQ=382833516 ACK=2336210776 WIN<<7=3
SSL: v=1.3 Application Data #1
  Record Layer :Application Data
    Content Type = 23 (Application Data)
    Version = 0x303 (TLS1.2)
    Content Length = 250
    Encrypted Application Data Message[250 data bytes]
```

Interpretation	Status
TCP: S=42086 D=443 LEN=0 SYN SEQ=2336210541 WIN=29200	SYN
TCP: S=443 D=42086 LEN=0 SYN SEQ=382831312 ACK=2336210542 WIN=28960	ACK/SYN
TCP: S=42086 D=443 LEN=0 SEQ=2336210542 ACK=382831313 WIN<<7=29312	ACK
SSL: v=1.3 Client Hello	ACK/PSH
TCP: S=443 D=42086 LEN=0 SEQ=382831313 ACK=2336210718 WIN<<7=30080	ACK
SSL: v=1.3 Server Hello, Change Cipher Spec, Application Data #4	ACK/PSH
TCP: S=42086 D=443 LEN=0 SEQ=2336210718 ACK=382833516 WIN<<7=33664	ACK
SSL: v=1.3 Application Data #1	ACK/PSH
SSL: v=1.3 Application Data #1	ACK/PSH
SSL: v=1.3 Application Data #1	ACK/PSH
SSL: v=1.3 Application Data #1	ACK/PSH
SSL: v=1.3 Application Data #1	ACK/PSH
TCP: S=42086 D=443 LEN=0 SEQ=2336210874 ACK=382839121 WIN<<7=49664	ACK
SSL: v=1.3 Application Data #1	ACK/PSH
TCP: S=42086 D=443 LEN=0 FIN SEQ=2336210898 ACK=382839121 WIN<<7=49664	ACK/FIN
TCP: S=443 D=42086 LEN=0 FIN SEQ=382839121 ACK=2336210899 WIN<<7=30080	ACK/FIN
TCP: S=42086 D=443 LEN=0 SEQ=2336210899 ACK=382839122 WIN<<7=49664	ACK

Packet 126 of 17

```
PACKET: #126 2020/10/16 10:29:59.329.854.672(UTC); Length=321 bytes; Captured=321 bytes
ETHERNET: S=[00-50-56-97-56-C4], D=[00-50-56-97-01-2C], EtherType=0x0800
IP:  S=10.20.53.136 D=10.20.53.134 LEN=287,  ID=38190, Offset=0, Proto=TCP;
TCP: S=443 D=42086 LEN=255  SEQ=382833516 ACK=2336210776 WIN<<7=30080
SSL: v=1.3 Application Data #1
  Record Layer :Application Data
    Content Type = 23 (Application Data)
    Version = 0x303 (TLS1.2)
    Content Length = 250
    Encrypted Application Data Message[250 data bytes]
```

EBCDIC

Decryption in nGeniusONE

nGeniusONE | All Modules | Data Mining | Device Configuration | ADMINISTRATOR

Packet Decode

Filter - 1 | 11:29:59.207 AM - 11:29:59.337 AM BST | Filtered Packets : 17 | Processed Packets: 358 | Filter Complete

Packet	Absolute Time	Delta Time	Length	Source	Destination	Interpretation	Status
114	11:29:59.207.674.503 AM BST	0.009.965.147	74	10.20.53.134			
116	11:29:59.207.951.268 AM BST	0.000.230.913	74	10.20.53.136			
117	11:29:59.208.010.035 AM BST	0.000.058.767	66	10.20.53.134			
120	11:29:59.312.555.878 AM BST	0.015.797.120	242	10.20.53.134			
121	11:29:59.312.793.487 AM BST	0.000.237.609	66	10.20.53.136			

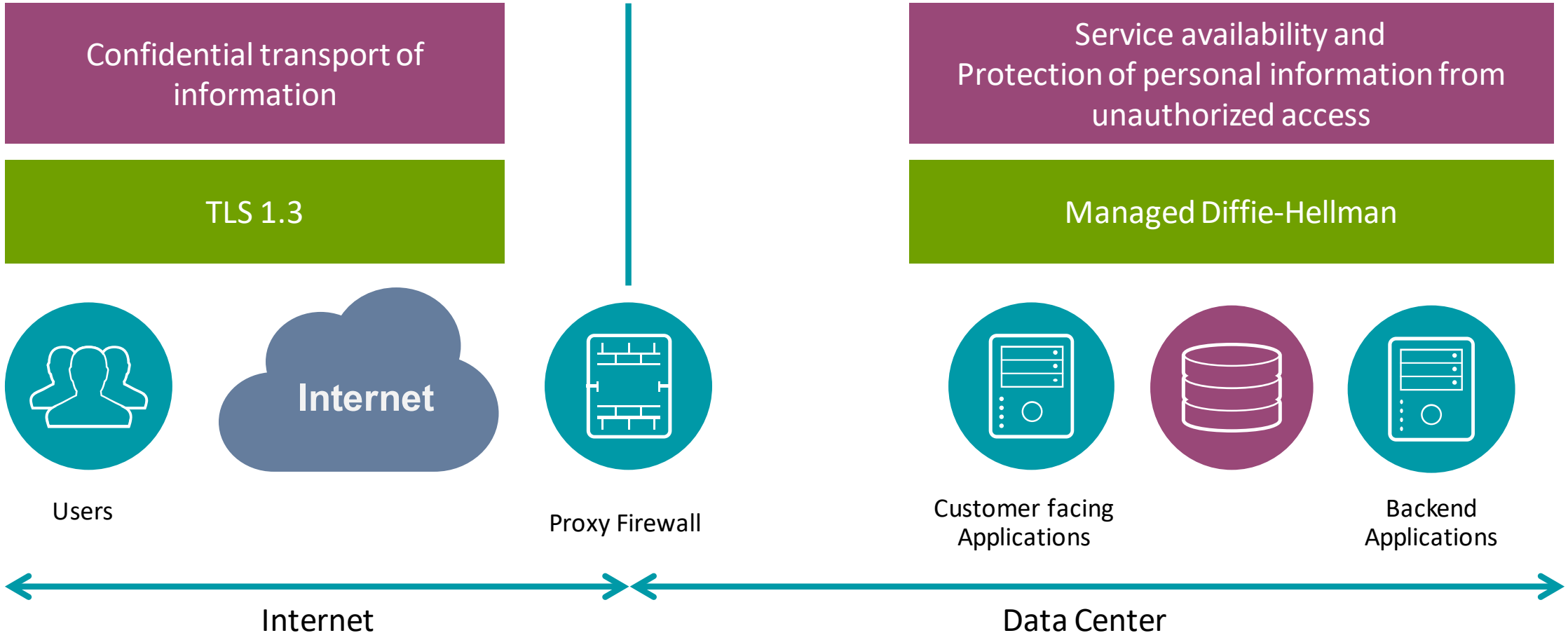
```
PACKET: #129 2020/10/16 10:29:59.330.373.210(UTC); Length=5161 bytes; Ca
ETHERNET: S=[00-50-56-97-56-C4], D=[00-50-56-97-01-2C], Type=802.3
IP:  S=10.20.53.136 D=10.20.53.134 LEN=5105,  ID=5424, Offset=0, Proto=T
TCP: S=80 D=42086 LEN=5073  SEQ=382834026 ACK=2336210852 WIN=235
HTTP: R  HTTP/1.1 Status=OK; 4833 bytes of content
HTML: [HTTP]   R  HTTP/1.1 Status=OK; 4833 bytes of content; !DOCTYPE, h
  DOCTYPE
    HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
    html
      head
        title = Welcome to CentOS
      style
        rel="stylesheet"
        type="text/css"
        style = html {background-image:url(img/html-background.png
      body
        div
```

Interpretation	Status
TCP: S=42086 D=443 LEN=0 SYN SEQ=2336210541 WIN=29200	SYN
TCP: S=443 D=42086 LEN=0 SYN SEQ=382831312 ACK=2336210542 WIN=28960	ACK/SYN
TCP: S=42086 D=443 LEN=0 SEQ=2336210542 ACK=382831313 WIN<<7=29312	ACK
SSL: v=1.3 Client Hello	ACK/PSH
TCP: S=443 D=42086 LEN=0 SEQ=382831313 ACK=2336210718 WIN<<7=30080	ACK
SSL: v=1.3 Server Hello, Change Cipher Spec, Application Data #4	ACK/PSH
TCP: S=42086 D=443 LEN=0 SEQ=2336210718 ACK=382833516 WIN<<7=33664	ACK
SSL: v=1.3 Finished	ACK/PSH
SSL: v=1.3 New Session Ticket	ACK/PSH
SSL: v=1.3 New Session Ticket	ACK/PSH
HTTP: C GET / HTTP/1.1	ACK/PSH
HTML: [HTTP] R HTTP/1.1 Status=OK; 4833 bytes of content; !DOCTYPE, html	ACK/PSH
TCP: S=42086 D=80 LEN=0 SEQ=2336210852 ACK=382839099 WIN=388	ACK
SSL: v=1.3 Alert (Encrypted)	ACK/PSH
TCP: S=42086 D=443 LEN=0 FIN SEQ=2336210898 ACK=382839121 WIN<<7=49664	ACK/FIN
TCP: S=443 D=42086 LEN=0 FIN SEQ=382839121 ACK=2336210899 WIN<<7=30080	ACK/FIN
TCP: S=42086 D=443 LEN=0 SEQ=2336210899 ACK=382839122 WIN<<7=49664	ACK

```
rel="stylesheet"
type="text/css"
style = html {background-image:url(img/html-background.png);background-color: white;font-family: "DejaVu Sans", "Liberation Sans", sans-serif;font-size: 0.85em;line-height: 1.25em;margin: 0 4% 0 4%;}body {border: 10px solid #fff;margin:0;paddin
body
div
```

Encryption in the Data Center

Encryption considerations for the Internet are different from those in the Data Center



Thank you