TLS 1.3 Implications to Network Security Solutions: Use Cases

[draft-camwinget-tls-use-cases-01]

Flemming Andreasen, Nancy Cam-Winget, Eric Wang

March 2018

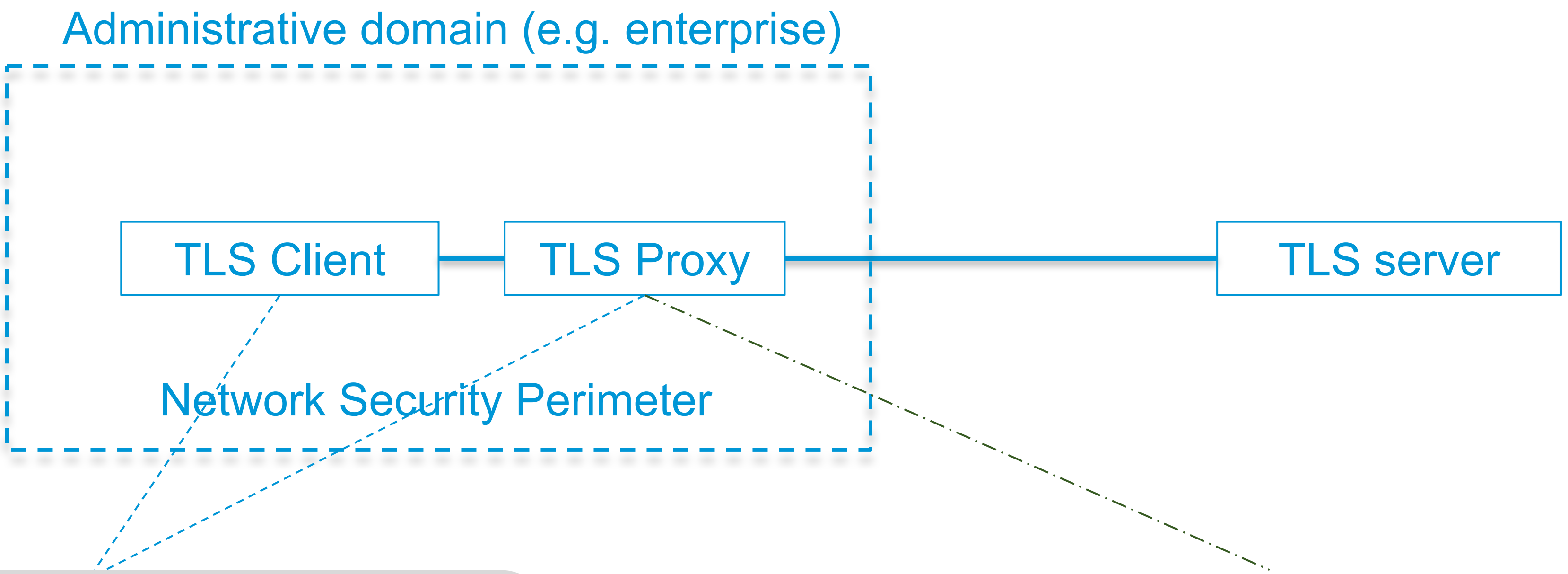
The image part with relationship ID rId34 was not found in the file.

Network Security solutions today

- Network Security Solutions provide access and security controls, auditing, compliance, vulnerability and threat detection
- Network Security Solutions today :
  - Observe TLS metadata to enable policy compliance and access control
  - Provide monitoring, audit and security control functions by *sometimes* inserting a *Middlebox* that acts as the *proxy*-TLS server to the originating client and as the *proxy-Client* to the TLS server

The image part with relationship ID rId34 was not found in the file.

Outbound Scenario



Administrative domain (e.g. enterprise)

TLS Client

TLS Proxy

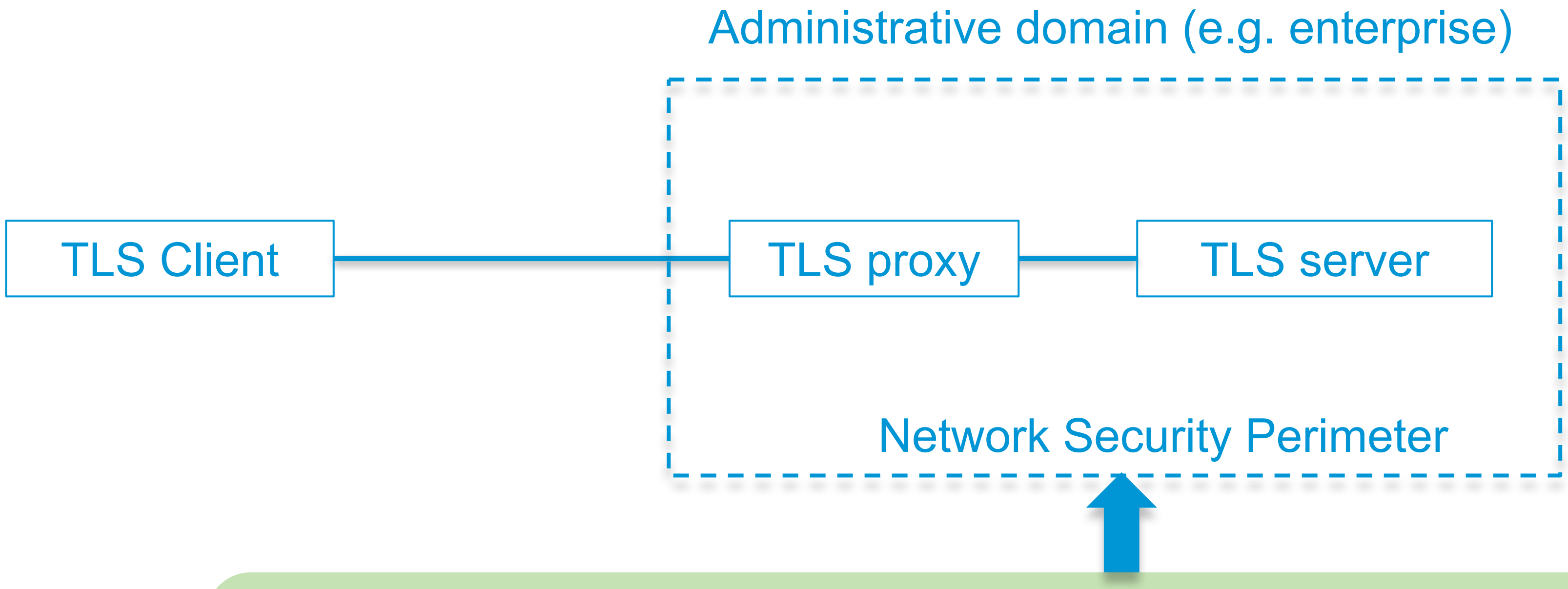
TLS server

Network Security Perimeter

TLS Client: Local Root cert installed Middelbox: Local cert (per TLS server – cached or generated on-the-fly)

When Policy is enforced → TLS Proxy changes TLS Server cert with Server-specific Local Cert signed with Local Root cert

Inbound Scenario


Administrative domain (e.g. enterprise)
TLS Client
TLS proxy
TLS server
Network Security Perimeter

When Policy is enforced →

- TLS Proxy has access to TLS Server’s cert and pub/priv keys (static keys)
- TLS Proxy determines TLS Server and its cert when Client initiates session

Outbound Use Cases as addressed today

Use Case	Summary
Acceptable Use Policy	Access control to application/websites: requiring DNS & HTTPs (URL) granular control
Malware and Threat Protection	Allowing the network to scan and protect from malware and known vulnerability attacks
IoT Endpoints	Enabling devices with weaker security posture
Unpatched Endpoints	Assess and protect unpatched endpoints from known vulnerabilities
Rapid Containment of New Vulnerability and Campaigns	Assess and protect vulnerable endpoints and general infrastructure
End of Life Endpoint	Legacy (unpatched) endpoint visibility to mitigate them as targets
Compliance	Continuous posture assessment for network-related compliance and endpoints without agents.
Crypto Security audit	Inspection of proper ciphers, authentication and identity credential use

The image

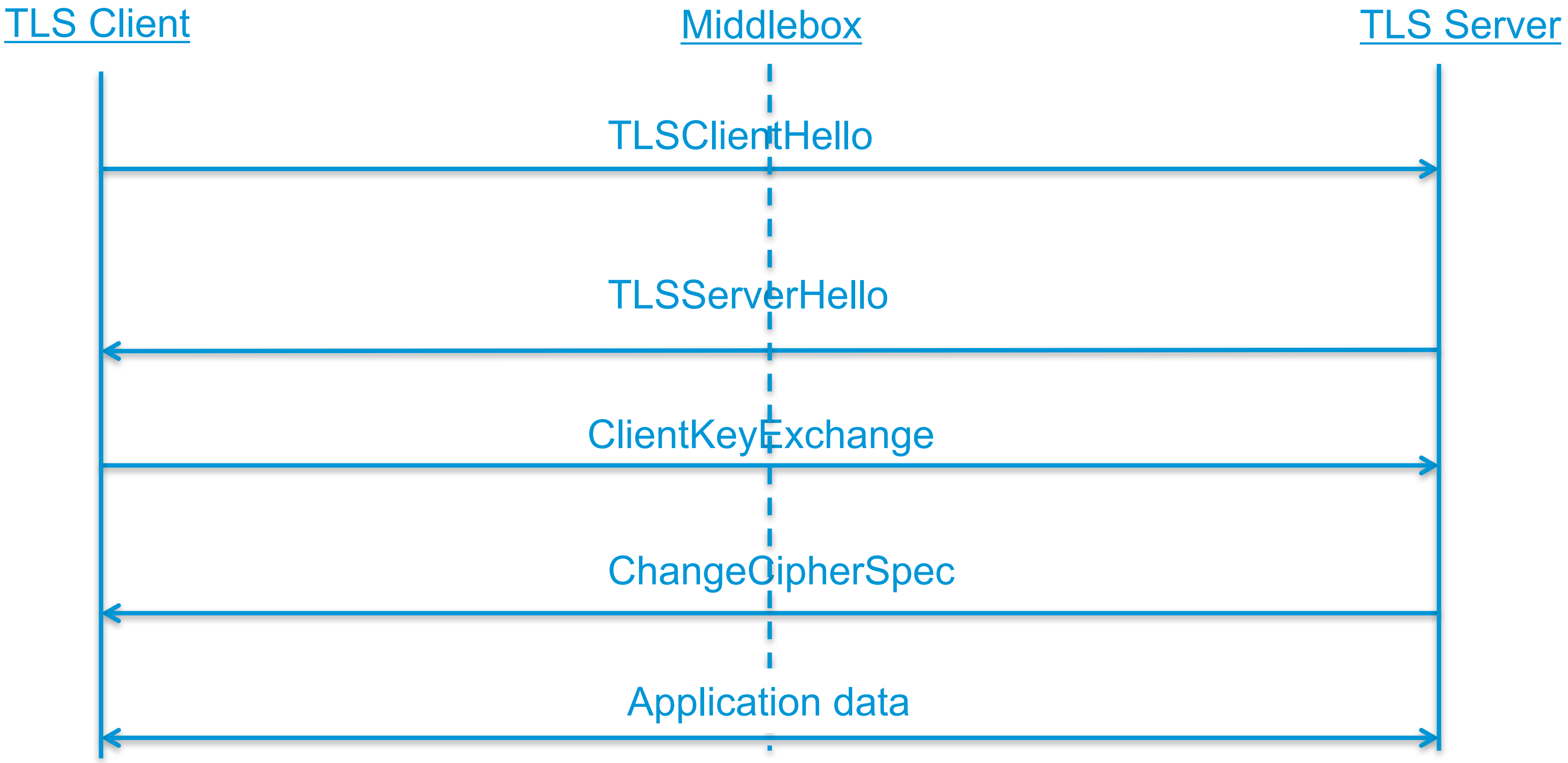
Inbound Use Cases as addressed today

Use Case	Summary
Data Center Protection	Protection of data resources from illicit transations
Application Operation over NAT	Passive application monitoring by NAT devices
Compliance	Continuous posture assessment
Crypto Security audit	Inspection of proper ciphers, authentication and identity credential use

The image part with relationship ID rId34 was not found in the file.

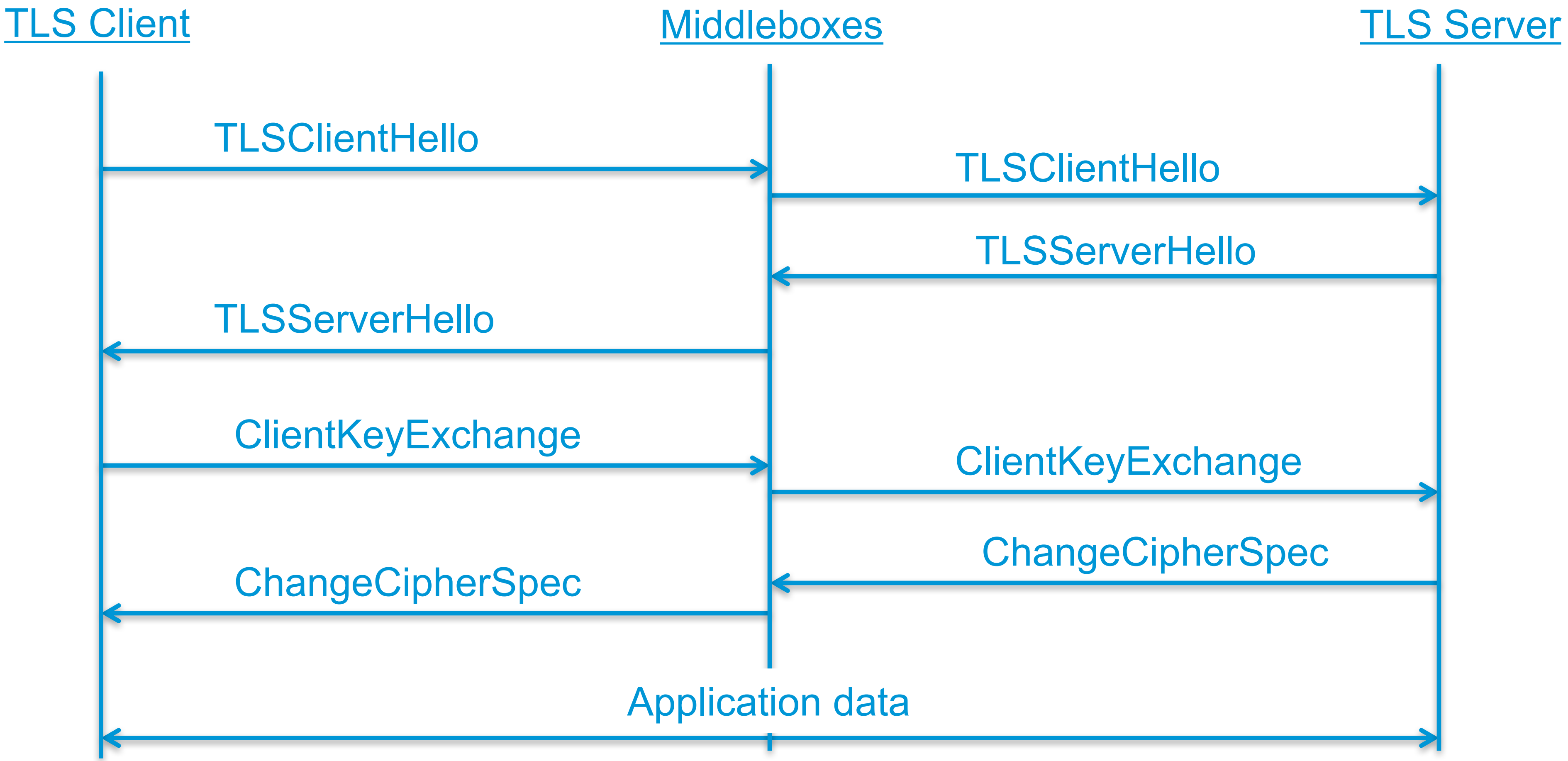
TLS 1.0-1.2 pass-through Proxies

Inspects metadata only



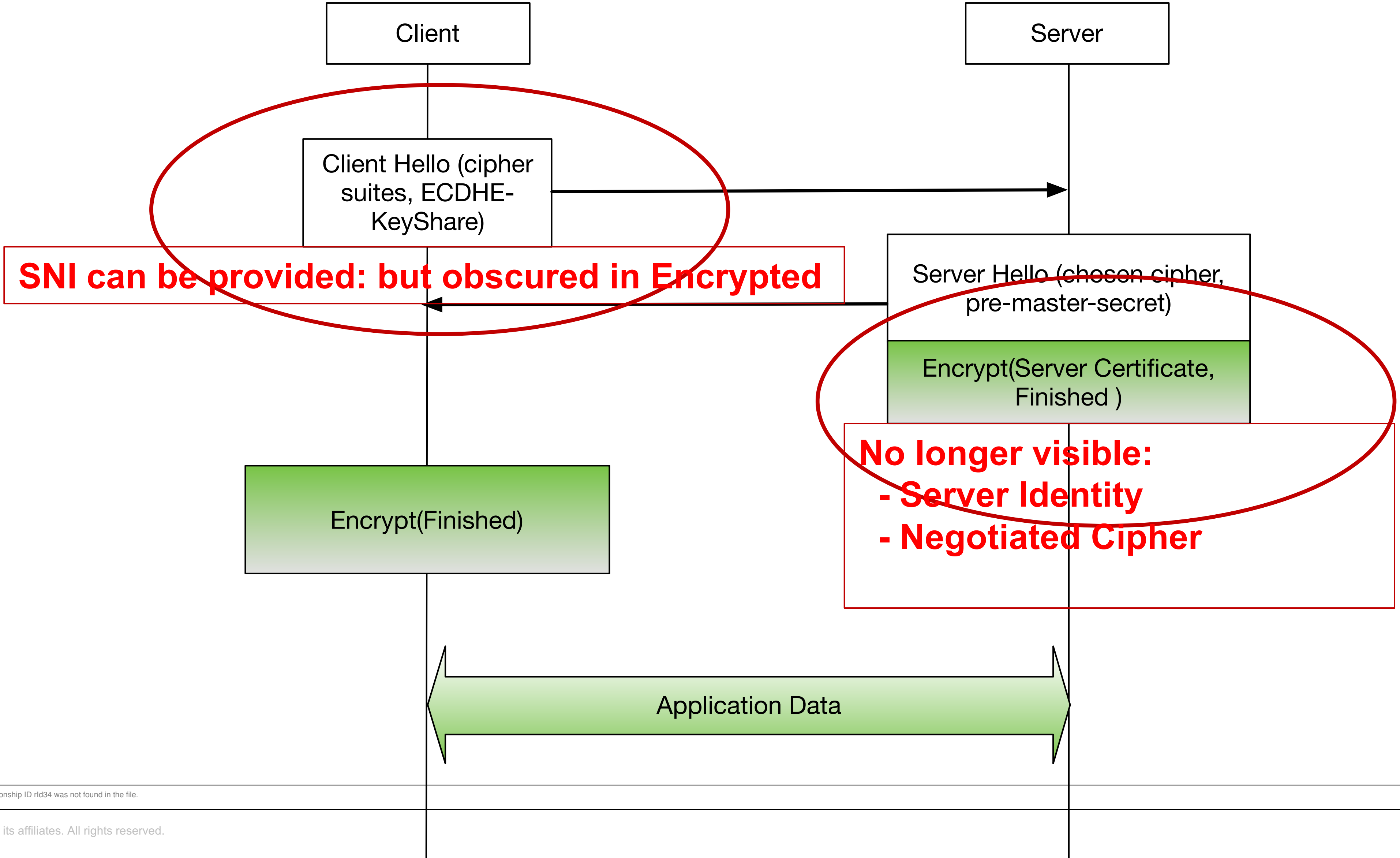
The image part with relationship ID rId34 was not found in the file.

TLS 1.0-1.2 *proxy-function* Middleboxes



The image part with relationship ID rId34 was not found in the file.

TLS 1.3 initial Handshake


Client
Server
Client Hello (cipher suites, ECDHE-KeyShare)
Server Hello (chosen cipher, pre-master-secret)
Encrypt(Server Certificate, Finished)
Encrypt(Finished)
Application Data

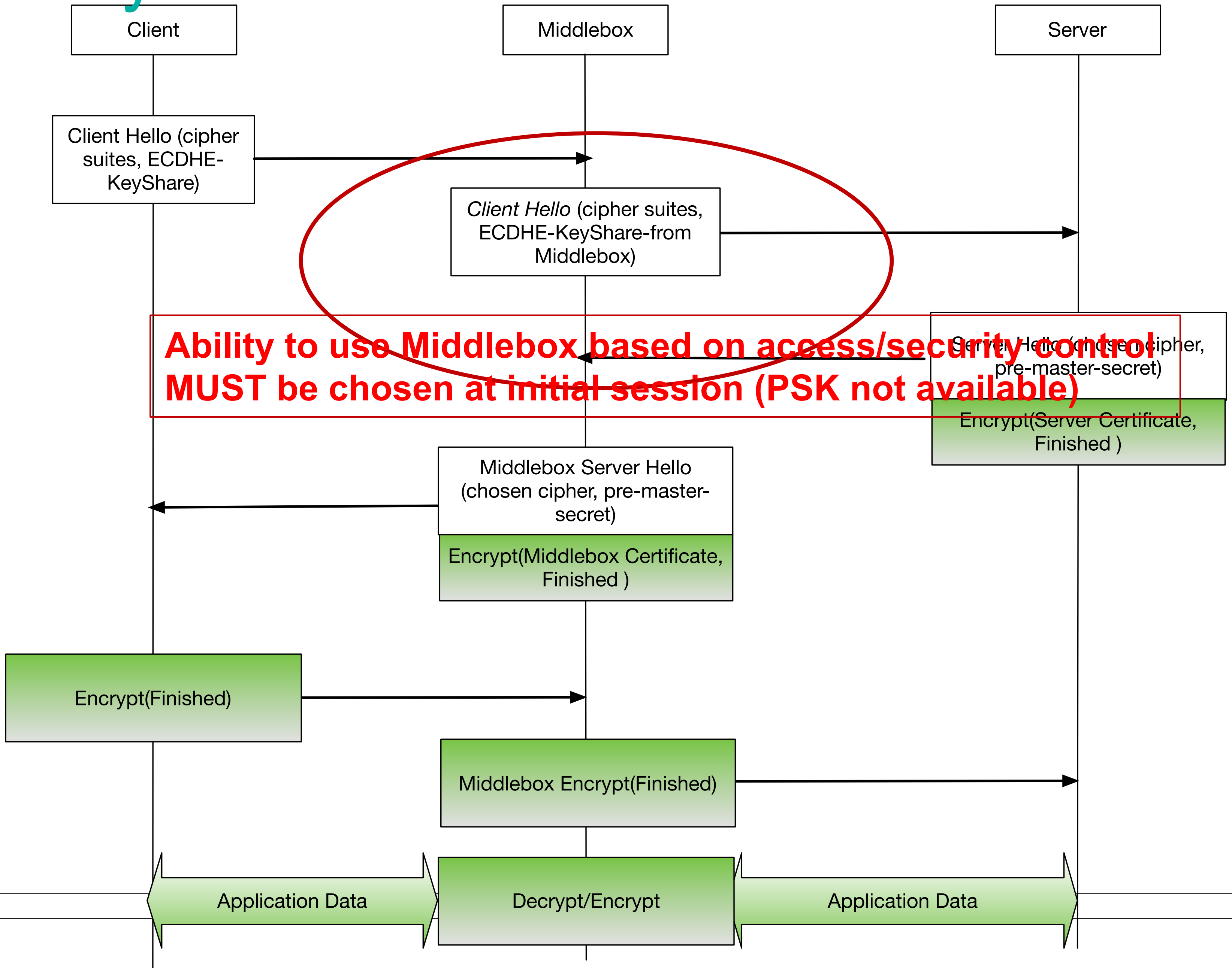
SNI can be provided: but obscured in Encrypted

No longer visible:

- Server Identity
- Negotiated Cipher

The image part with relationship ID rId34 was not found in the file.

TLS 1.3 Proxy-Function Middlebox


Client
Middlebox
Server
Client Hello (cipher suites, ECDHE-KeyShare)
Client Hello (cipher suites, ECDHE-KeyShare-from Middlebox)
Server Hello (chosen cipher, pre-master-secret)
Encrypt(Server Certificate, Finished)
Middlebox Server Hello (chosen cipher, pre-master-secret)
Encrypt(Middlebox Certificate, Finished)
Encrypt(Finished)
Middlebox Encrypt(Finished)
Application Data
Decrypt/Encrypt
Application Data

Ability to use Middlebox based on access/security control MUST be chosen at initial session (PSK not available)

The image part with relationship ID rId34 was not found in the file.

TLS 1.3 Impact on Outbound Use Cases

Use Case	Summary
Encrypted Server Certificate	ServerHello and Certificate messages are encrypted obscuring CN and impacting access and security control functions such as selective proxying, white- or black-lists, regulatory and audit functions.
Resumption and PSK	When inspection is enforced, TLS-proxy will not know PSK during resumption prohibiting access and security control functions. Fallback to full handshake is not an absolute TLS requirement; in practice, implementations are expected to support it though
Version negotiation and Downgrade Protection	Ensure TLS 1.3 Client and TLS 1.3 server will negotiate TLS 1.3. Results in the TLS Proxy having to always be an active man-in-the-middle from the start of the session. A TLS 1.2 Proxy will thus downgrade all proxied connections and cannot disengage subsequently.
Encrypted SNI in ClientHello	SNI in ClientHello can help with selective access and security controls but these functions are obviated if SNI is encrypted in all messages (since the server certificate is also encrypted).

The image part with relationship ID rId34 was not found in the file.

TLS 1.3 Impact on Inbound Use Cases

Use Case	Summary
Removal of Static RSA and DH Ciphers	TLS-proxy no longer gains access to TLS session data as TLS Server can no longer pre-share keys with Middlebox apriori. Impacts a number of Data Center scenarios such as • Threat Detection (e.g. IDS) • Monitoring (e.g. packet capture) • Compliance • Troubleshooting
Crypto Security audit	Final negotiation of cipher selection is no longer visible by TLS-proxy

Summary

- Network Security Solutions will evolve and adapt to support TLS 1.3
- Transition is causing some lack of functionality for now – endpoint cooperation and full proxying can help close these gaps.
- TLS 1.3 extensions may be defined to address endpoint opt-in, auditing functions, etc.