TLS 1.3 Impact on Network Based Security Solutions

Flemming Andreasen, Nancy Cam-Winget, Eric Wang

July 23, 2019

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
- TLS 1.3 introduces some changes in the handshake protocol that affect these solutions

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

Scenarios and impacts document

- https://tools.ietf.org/html/draft-camwinget-tls-use-cases-04
  - Informational draft to describe scenarios and impact of deploying TLS 1.3
  - Draft has been stable since IETF 104

- Ask: publish draft as RFC as Informational Draft

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	Protecting 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 method and identity credential use

Inbound Use Cases as addressed today

Use Case	Summary
Data Center Protection	Protection of data resources from illicit transactions
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.