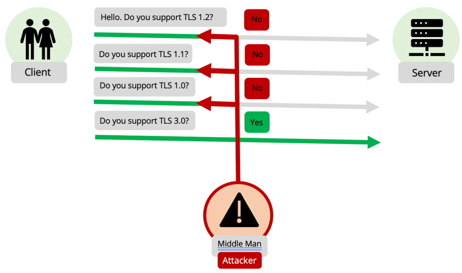
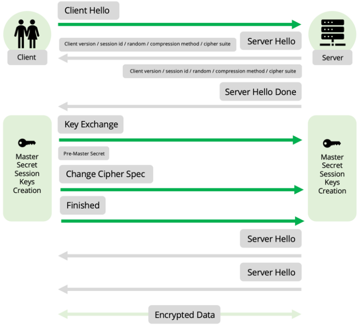
CN Anti-Exfiltration solution
Cisco HCI -> Cohesity AWS Anti-Ransomware Backup PoC

The Challenge

Cisco HCI Server to Secure AWS Cloud Backup over the Internet – The Backup application currently protects Data in Transit via TLS. TLS is initiated via a handshake protocol which is where most of its vulnerabilities occur. TLS has known vulnerabilities that include malware injection and 'Man in the Middle' data exfiltration attacks. Once compromised the Anti-Ransomware backup is no longer secure. How can you protect the data itself from the Man in the Middle data exfiltration?

Padding Oracle on Downgraded Legacy Encryption (POODLE) Attack



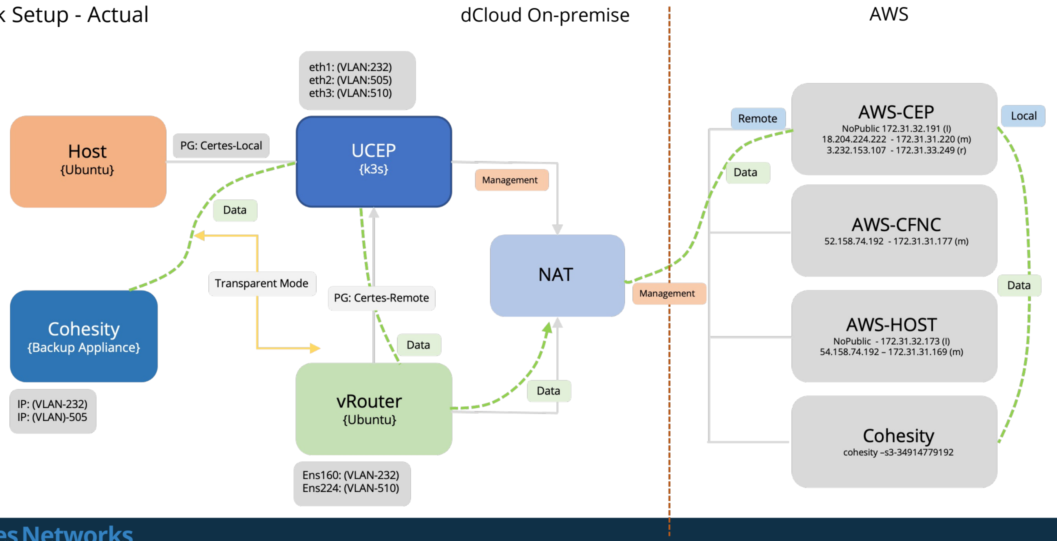

Client Hello
Client
Server
Server Hello
Client version / session id / random / compression method / cipher suite
Client version / session id / random / compression method / cipher suite
Server Hello Done
Key Exchange
Master Secret Session Keys Creation
Pre-Master Secret
Change Cipher Spec
Master Secret Session Keys Creation
Finished
Server Hello
Server Hello
Encrypted Data

This is where TLS can fall down – Hacker can force negotiation down to lower level of TLS and open vulnerabilities.

The Solution

- Certes Patented technology focuses on encrypting the data payload at layer 4 – all other aspects of the IP packet are left unchanged, any application treats the IP packet as unchanged.
- Certes can protect individual application flows by defining policies – each flow has its own Quantum encryption keys and each is individually rotated every hour.
- Certes CEP's (enforcement points) do not build any tunnels and do not suffer from the same vulnerabilities of the TLS handshake.
- Certes CEP's placed in-line (acting as a network Bridge) at the source and Destination will protect the data payload and prevent anyone other than the intended recipient from being able to read the data.
- Traffic can be protected via Policies as to what can and cannot be viewed and 100% under customer control
- Data leaving via a CEP will be encrypted by policy – any 'Man in the Middle Attack' or Attempted Exfiltration of data will get worthless encrypted data. A TLS Man in the Middle attack will fail as a result.
- At the HCI side the Certes devices are deployed in their containerised format where they act as a bridge between two virtual switches monitoring traffic and matching by policy at which point the data payload will be encrypted and the packet sent on its way.
- At the AWS side Certes is deployed in its Cloud Native form within the Cohestiy AWS Cohesity S3 Storage.

Certes Network Setup - Actual



Contact Certes Networks

300 Corporate Center Drive,
Suite 140 Pittsburgh, PA 15108
www.certesnetworks.com

CERTES NETWORKS

Tel: 1 (888) 833-1142
Fax: 1 (412) 262-2574
sales@certesnetworks.com
info@certesnetworks.com