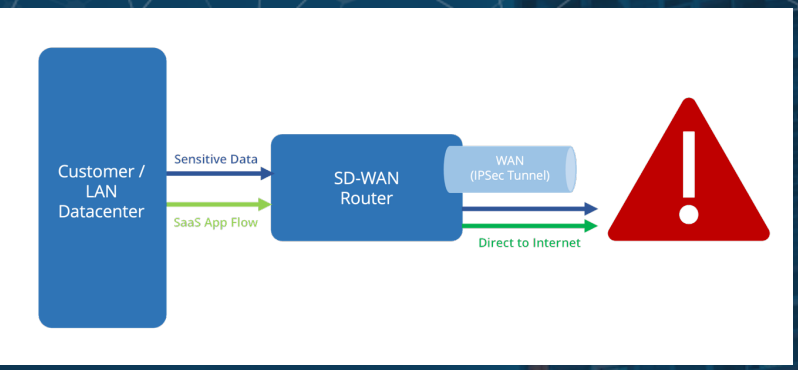
Risk Mitigation from a Data Breach for Cisco SDWAN

The Challenge

SDWAN is a technology that has rapidly become the "technology of choice" for protecting unsecure links such as the public Internet as well as automatically steering traffic by policy based on current latency / loss / jitter characteristics to provide great customer experience. However, SDWAN is focused on the link and its characteristics and not the business value of the Data flowing through it. As a tunnelled solution it protects the link between its two end points with traditional IPSec, but if that SDWAN fabric is compromised or a policy mistake sends sensitive data "direct to net" it can do little to protect the individual data flows. This could lead to Regulatory fines, Adverse Publicity and in some cases Criminal prosecutions for the customer and or Service Provider.

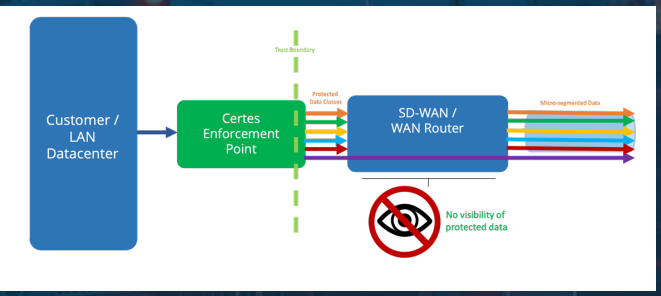


In this diagram we see Customer sensitive data being incorrectly steered direct to the Internet instead of going through the secure IPsec tunnel.

For the Network team this is a configuration problem that can easily be fixed once identified - for the Customer it is already too late, they are now required to inform the regulators of the breach, that process can lead to huge fines, reputational damage, class action lawsuits and potentially criminal proceedings for officers of the company / CISO etc.

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 a 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 as they and only they define and control the protection policies.
- 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.
- Certes separates the management of the security from the management of the infrastructure – the customer is 100% in control of the security and not the network team or service provider.



By adding a Certes Enforcement Point in-line we can mitigate the impact of this misconfiguration by protecting the sensitive data based on business risk before it gets to the SDWAN or WAN edge. This means that even if an SDWAN policy is incorrectly defined to send sensitive data "direct to net" there will be no business impact as the data will be fully protected and not visible to anyone other than the intended recipient.

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

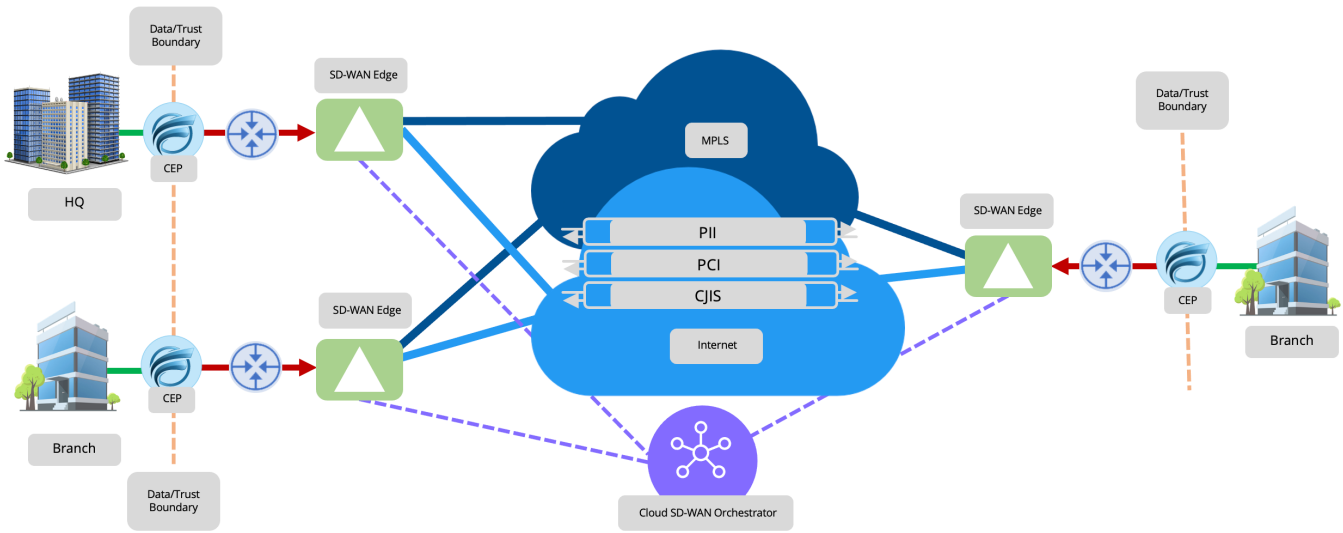
Risk Mitigation from a Data Breach for Cisco SDWAN

Misconfiguration is just one example, the Certes data protection solution can protect against data sovereignty breaches and data exfiltration resulting from a ransomware attack. It can do this because it is focused on protecting the data no matter where it travels irrespective of who owns or controls the network infrastructure.

The Certes solution is completely transparent to the Cisco SDWAN solution(s)

- No configuration changes required on the SDWAN
- No impact to the security monitoring and reporting tools such as Talos or ThousandEyes
- No performance impact
- Protects against data sovereignty breaches when no network breach occurs (such as the META / Facebook Data Sovereignty Schrems II judgement of GDPR = 4% Global Group Revenue fine of $1.3Bn)
- Helps mitigate the Business Risk of a Data Breach by ensuring the data itself is protected. The regulators main concern will be “was any data exposed to those that should not be able see it” with Certes complimenting the SDWAN the response will be – “No, the data at all times was protected”.

Deployment:
The Certes enforcement points come in VM (ESXi and KVM) , physical (FIPS 140-2 Certified, CC EAL4+) and containerised formats that can be deployed on-prem or in the cloud, they are totally transparent to any other network device or service. The only part of the IP packet affected is the payload which will be protected according to customer defined policy. The enforcement points act as a network bridge, they protect the Customers valuable data and mitigate the risk from fines and potential criminal prosecution resulting from a data or sovereignty breach.



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