TATA COMMUNICATIONS
TRANSFORMATION SERVICES

Taking cloud networking & security to unprecedented levels

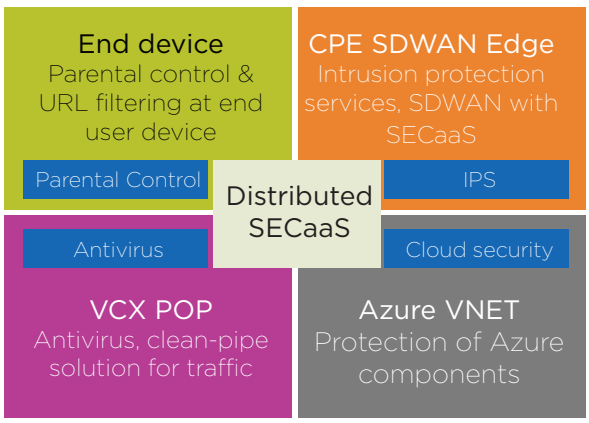
In today's business world, hybrid and pure cloud hosting scenarios are becoming increasingly common. By 2025, about 80% of enterprises will have moved their data centres off-premises, according to a recent forecast report by Gartner. With the number of IoT devices predicted at 64 billion by 2025, enterprises are accelerating investment in IoT solutions.

Tata Communications Transformation Services' (TCTS) Security as a Service (SECaaS) offering, along with the Virtual Cloud Exchange (VCX) platform, addresses the security and connectivity challenges faced by enterprises across public clouds, private data centres and other interconnected ecosystems, bringing the benefits of automation, accessibility, security and improved synergies. SECaaS is a fully software-defined platform running on a generic Network Function Virtualisation (NFV) infrastructure and hosting multiple Virtual Network Functions (VNFs) to protect enterprise networks against external threats, attacks and data loss. This platform is an innovative take on an in-depth, multi-layer defence strategy for enhanced cybersecurity and connectivity.

Built on generic NFV infrastructure, the TCTS' SECaaS cloud offering consists of virtual Firewall (vFW), universal CPE (uCPEs) and SDN access boxes. Users can manage the solution through the zero-touch automation portal orchestrated by a Lifecycle Service Orchestrator (LSO). The solution works cohesively with SDWAN, creating a powerful combo of SDWAN, security and cloud access. It coexists with the TCTS Virtual Cloud Exchange (VCX) solution that CSPs use to connect seamlessly with major public cloud providers.

Salient features

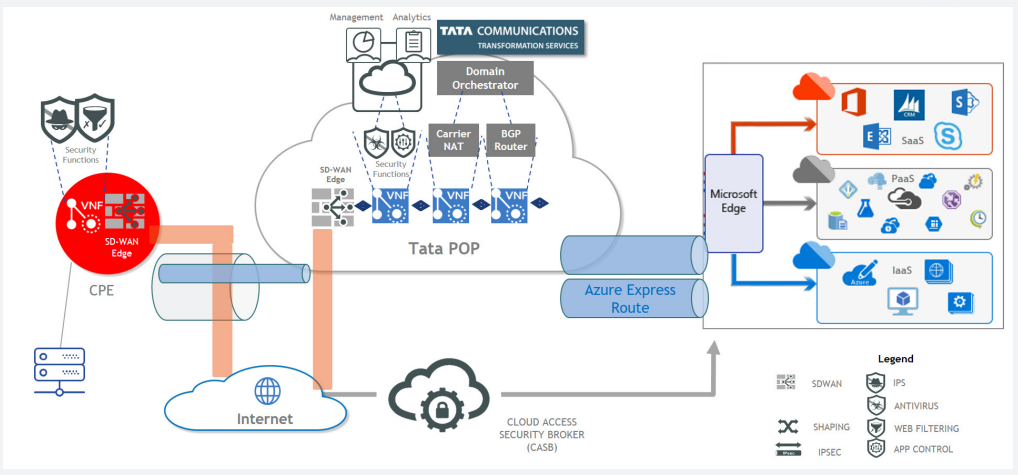
- Cloud networking as a service
- Contextual and distributed security
  - User equipment protection in customer network
  - Parental control with web filtering
  - Intrusion protection services
  - Secure SDWAN to POP
  - Data decryption and forwarding to dedicated cloud connectivity
  - Clean pipe with gateway-level antivirus
  - Protection at cloud level
- Traffic failover and routing management



Advantages

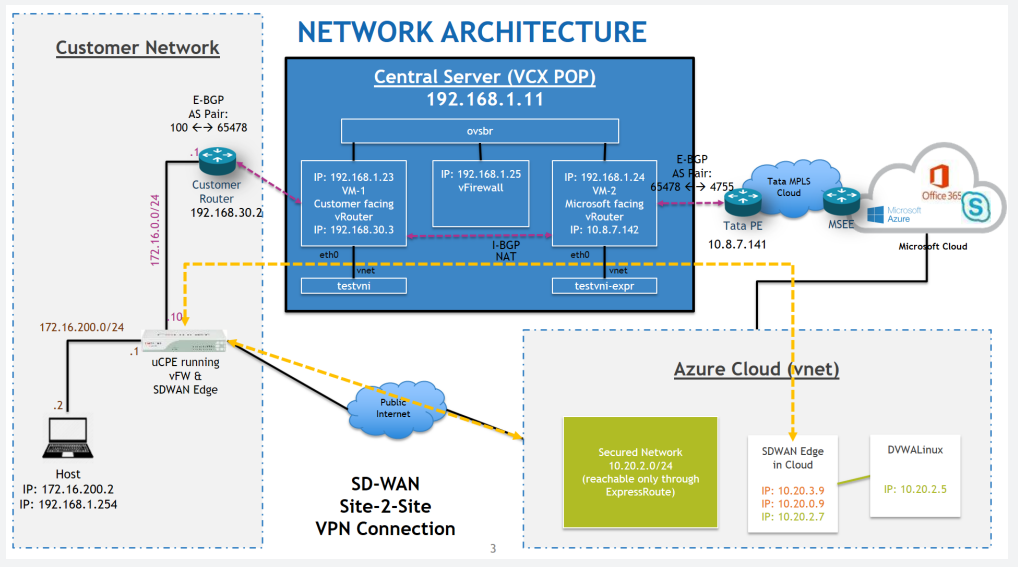
- Advanced multi-layer, multi-platform security with contextual and distributed capabilities
- Even if a CSP has little or no SDN/NFV background, they can still avail the synergistic SDN/NFV solution, which can in-turn facilitate the TCTS SECaaS offering.
- The enterprise user is ensured secure connections across any hybrid network environment.
- Additional security functionality can be added on-demand based on user requirement.
- One of the simplest solutions to providing seamless connectivity to public clouds in an SDWAN environment with enhanced security at each level. (Based on customer feedback)
- Single self-service portal powered by LSO results in increased multi-vendor synergies and elimination of user silos

SDWAN Usecase



Proof of concept demonstration of SDWAN, TCTS VCX and SECaaS

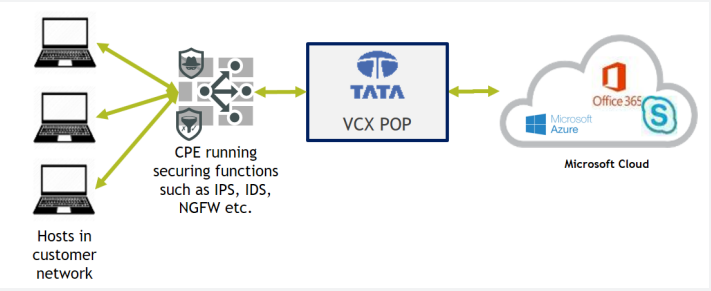
Jointly, the offering works to provide enterprise customers secure and managed connectivity with public cloud providers. Overlay tunnels are created between Universal Customer Premises Equipment (uCPE) at the customer-edge and the CPE instance running in the public cloud environment, by utilising a public internet link as well as the dedicated ExpressRoute connectivity that is facilitated by TCTS VCX.



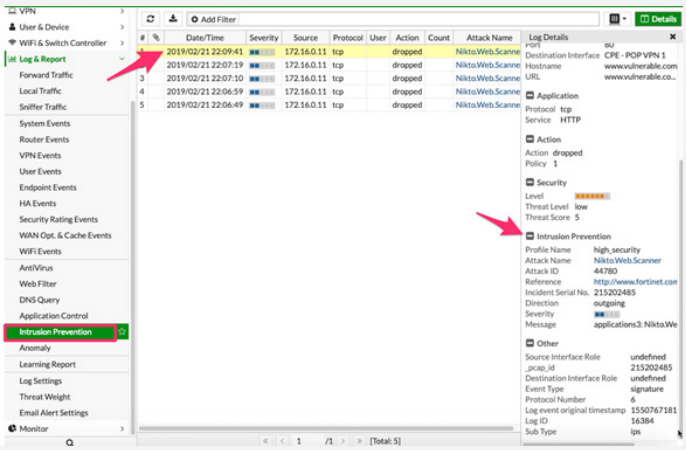
Results and performance metrics

As part of proof of concept, below use cases were identified, and results are validated against those use cases:

1. Parental control at hosts level in customer LAN
2. IPS/IDS at customer CPE

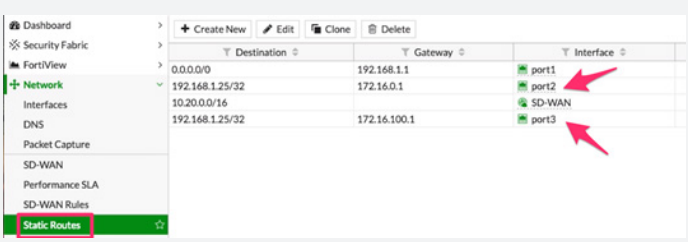


We set up multiple hosts in the customer environment, a few harmless Windows machines and evil Kali Linux loaded with various attacking tools including Nikto trying to probe against the vulnerable web application running in Azure environment. When Nikto tried to profile the destination server, IPS system at CPE categorised the traffic as intrusion and blocked the same.



3. SDWAN for redundant IPSEC VPN tunnels

Customer CPE & another instance in Azure are connected with IPSEC VPN. Instead of a single tunnel, we configured multiple tunnels with redundant WAN links; one through public internet and another through VCX setup with ExpressRoute connectivity. This configuration gives resiliency against VPN tunnel failures, latency and jitter. Tunnel traffic being continuously monitored and automatic fail-over to secondary tunnel if quality drops below a threshold level.



4. Anti-virus in VCX POP

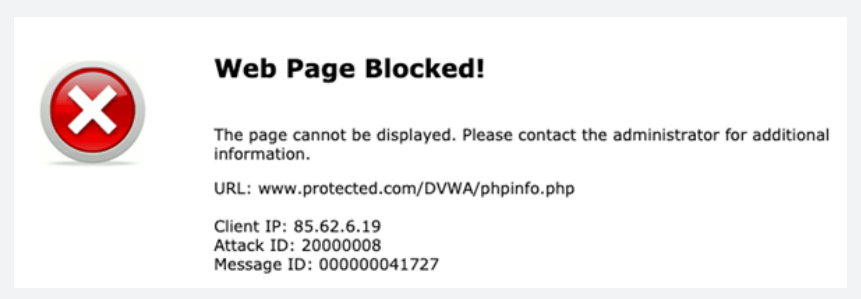
We set up a dummy virus and put in place anti-virus system at VCX POP to block access to the same.

5. Protection in the cloud

Damn Vulnerable Web Application (DVWA) was set up in Azure cloud, which would have been exposed for hackers to exploit if TCTS SECaaS service was not been in place. We demonstrated the same when coming through public internet exploiting the vulnerabilities and through another secured link powered by TCTS SECaaS & VCX solution.

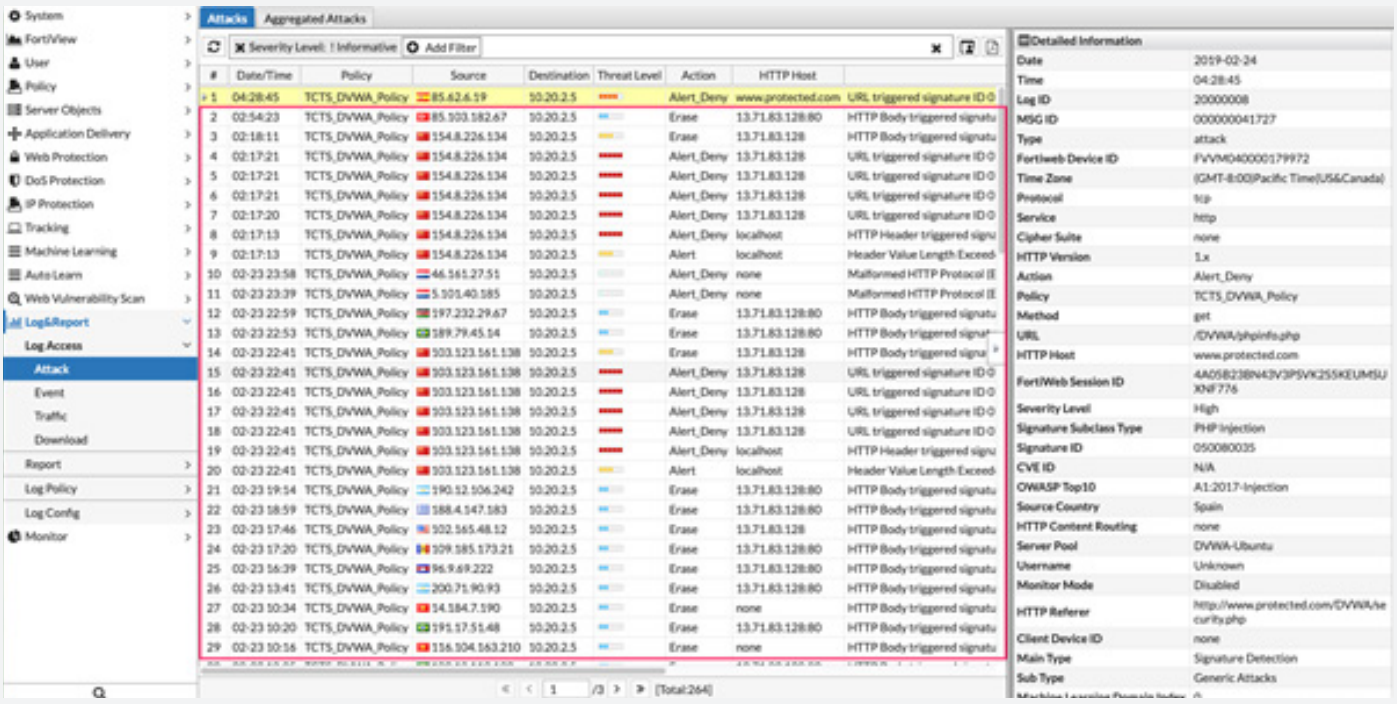
Application leaks sensitive information when coming through open unsecured link:

and same been protected through SECaaS + VCX solution:



6. Visualise real-time hackers trying to attack the systems

Hosting the workloads in public cloud doesn't mean that they are automatically protected. With the shared responsibility model, customers are required to provide adequate protection mechanism for various attacks. Since the DVWA application set-up for demo has public IP address, it attracts a lot of visitors from the public internet. Below are the list of attackers captured trying to access the vulnerable application on our SECaaS component:



ABOUT TATA COMMUNICATIONS TRANSFORMATION SERVICES

Tata Communications Transformation Services Limited (TCTS), a 100% subsidiary of Tata Communications Ltd, provides leading business transformation, managed network operations, network outsourcing and consultancy services to telecom companies around the world. TCTS delivers operational efficiency, cost transformation and revenue acceleration solutions for all the stages of the carrier process lifecycle, including but not limited to network engineering and design, implementation and operations.