



## Taking cloud networking & security to unprecedented levels

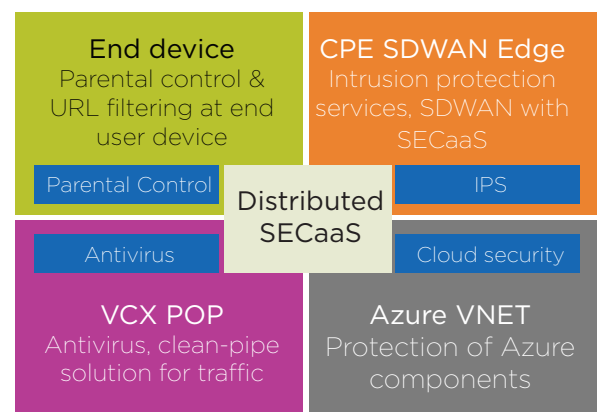
In today's business world, hybrid and pure cloud hosting scenarios are becoming increasingly common. By 2025, about 80% of enterprises will have moved their data centres off-premises, according to a recent forecast report by Gartner. With the number of IoT devices predicted at 64 billion by 2025, enterprises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

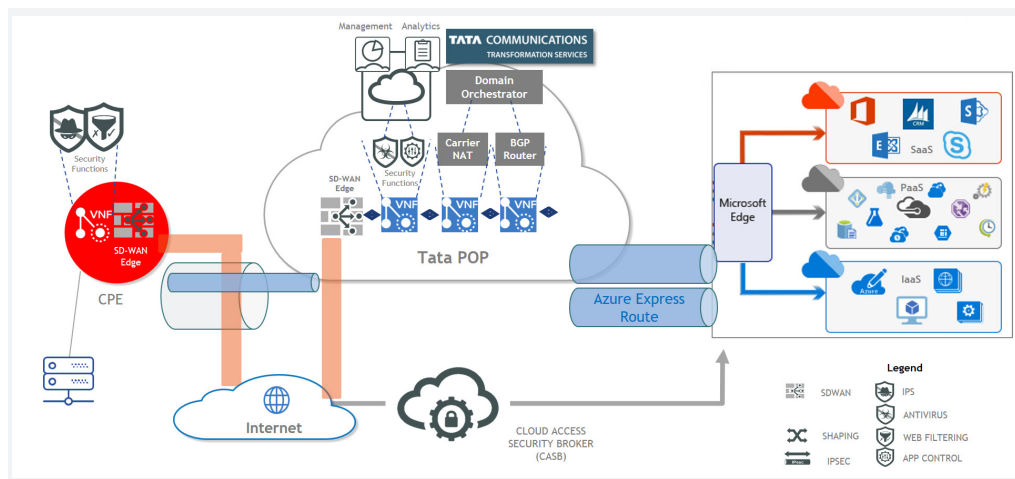
- Cloud networking as a service
- Contextual and distributed security
  - User equipment protection in customer network
  - Parental control with web filtering
  - Intrusion protection services
  - Secure SDWAN to POP
  - Data decryption and forwarding to dedicated cloud connectivity
  - Clean pipe with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



## Advantages

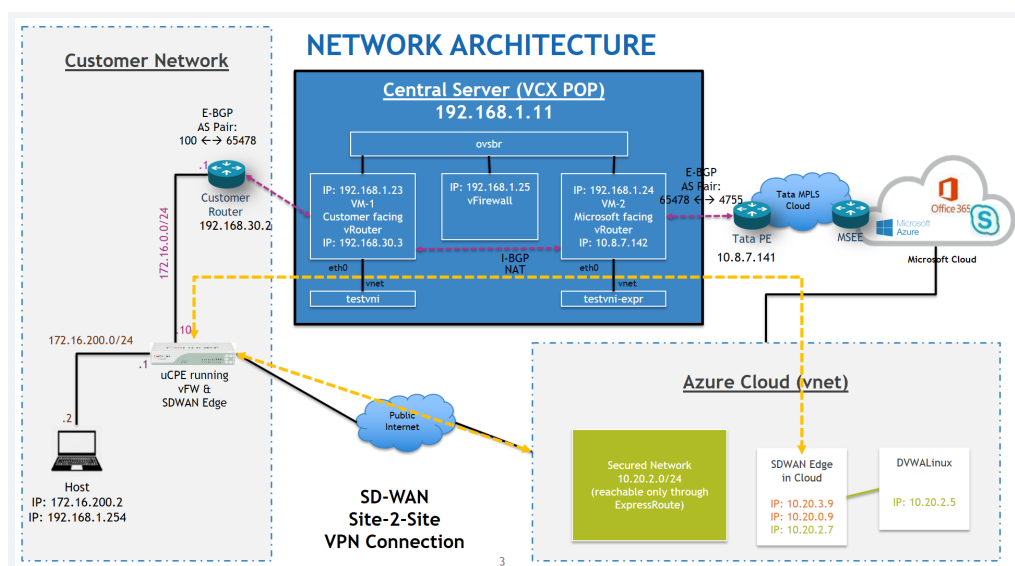
- Advanced multi-layer, multi-platform security with contextual and distributed capabilities
- Even if a CSP has little or no SDN/NFV background, they can still avail the synergistic SDN/ NFV solution, which can in-turn facilitate the TCTS SECaaS offering.
- The enterprise user is ensured secure connections 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.

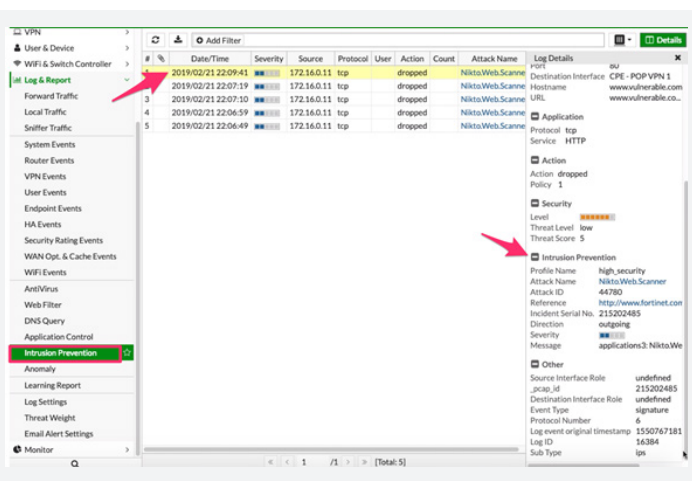


## Results and performance metrics

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

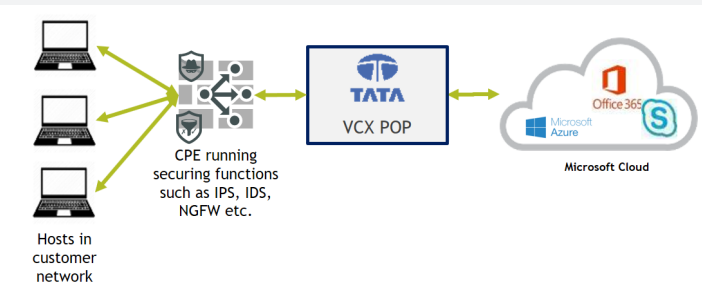
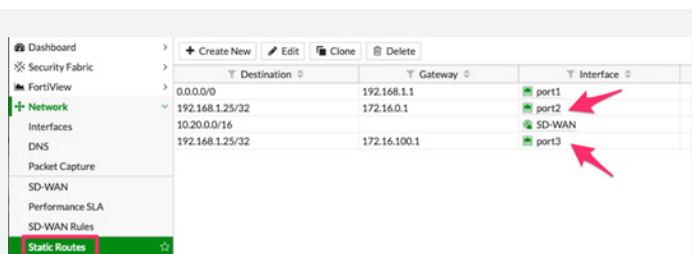
1. Parental control at hosts level in customer LAN
2. IPS/IDS at customer CPE

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:

PHP Version 5.6.40-1+ubuntu16.04.1+deb.sury.org-1	
System	Linux DVWA:Linux 4.15.0-1007-azure #39~16.04.1-Ubuntu SMP Tue Jan 15 17:20:47 UTC 2019 x86_64
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/5.6/apache2
Loaded Configuration File	/etc/php/5.6/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/5.6/apache2/conf.d
Additional .ini files parsed	/etc/php/5.6/apache2/conf.d/10-mysqlnd.ini, /etc/php/5.6/apache2/conf.d/10-opcache.ini, /etc/php/5.6/apache2/conf.d/10-pdo.ini, /etc/php/5.6/apache2/conf.d/15-xml.ini, /etc/php/5.6/apache2/conf.d/20-calendar.ini, /etc/php/5.6/apache2/conf.d/20-curl.ini, /etc/php/5.6/apache2/conf.d/20-dom.ini, /etc/php/5.6/apache2/conf.d/20-exif.ini, /etc/php/5.6/apache2/conf.d/20-ftp.ini, /etc/php/5.6/apache2/conf.d/20-gd.ini, /etc/php/5.6/apache2/conf.d/20-gettext.ini, /etc/php/5.6/apache2/conf.d/20-iconv.ini, /etc/php/5.6/apache2/conf.d/20-ldap.ini, /etc/php/5.6/apache2/conf.d/20-mcrypt.ini, /etc/php/5.6/apache2/conf.d/20-mysql.ini, /etc/php/5.6/apache2/conf.d/20-pdo_mysql.ini, /etc/php/5.6/apache2/conf.d/20-pdo_pgsql.ini, /etc/php/5.6/apache2/conf.d/20-pdo_sqlite.ini, /etc/php/5.6/apache2/conf.d/20-readline.ini, /etc/php/5.6/apache2/conf.d/20-shmop.ini, /etc/php/5.6/apache2/conf.d/20-simplexml.ini, /etc/php/5.6/apache2/conf.d/20-sockets.ini, /etc/php/5.6/apache2/conf.d/20-sysmsg.ini, /etc/php/5.6/apache2/conf.d/20-sysvshm.ini, /etc/php/5.6/apache2/conf.d/20-tokenizer.ini, /etc/php/5.6/apache2/conf.d/20-wddx.ini, /etc/php/5.6/apache2/conf.d/20-xdebug.ini, /etc/php/5.6/apache2/conf.d/20-xsl.ini
PHP API	20131106
PHP Extension	20131226
Zend Extension	220131226
Zend Extension Build	AP220131226.NTS
PHP Extension Build	AP220131226.NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	enabled
Registered PHP Streams	https, ftps, compress.zlib, file, glob, data, http, ftp, ghar
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, sslv2, tls, tlsv1.0, tlsv1.1, tlsv1.2

**Web Page Blocked!**

The page cannot be displayed. Please contact the administrator for additional information.

URL: [www.protected.com/DVWA/phpinfo.php](http://www.protected.com/DVWA/phpinfo.php)

Client IP: 85.62.6.19  
Attack ID: 20000008  
Message ID: 000000041727

This image shows a red circular icon with a white 'X' inside, indicating an error. Below the icon, the text 'Web Page Blocked!' is displayed in a large, bold, black font. Underneath this, a smaller black font message states: 'The page cannot be displayed. Please contact the administrator for additional information.' Further down, the URL 'URL: www.protected.com/DVWA/phpinfo.php' is shown. At the bottom, three lines of technical data are listed: 'Client IP: 85.62.6.19', 'Attack ID: 20000008', and 'Message ID: 000000041727'.

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:

**System**

**FortiView**

**User**

**Policy**

**Server Objects**

**Application Delivery**

**Web Protection**

**DoS Protection**

**IP Protection**

**Tracking**

**Machine Learning**

**AutoLearn**

**Web Vulnerability Scan**

**Log & Report**

**Log Access**

**Attack**

**Event**

**Traffic**

**Download**

**Report**

**Log Policy**

**Log Config**

**Monitor**

Severity Level: Informative
Add Filter

#	Date/Time	Policy	Source	Destination	Threat Level	Action	HTTP Host
1	04:28:45	TCTS_DVWA_Policy	85.103.182.67	10.20.2.5	High	Alert_Deny	www.protected.com
2	02:54:23	TCTS_DVWA_Policy	85.103.182.67	10.20.2.5	High	Erase	13.71.83.128:80
3	02:18:11	TCTS_DVWA_Policy	154.8.226.134	10.20.2.5	High	Erase	13.71.83.128
4	02:17:21	TCTS_DVWA_Policy	154.8.226.134	10.20.2.5	High	Alert_Deny	13.71.83.128
5	02:17:21	TCTS_DVWA_Policy	154.8.226.134	10.20.2.5	High	Alert_Deny	13.71.83.128
6	02:17:21	TCTS_DVWA_Policy	154.8.226.134	10.20.2.5	High	Alert_Deny	13.71.83.128
7	02:17:20	TCTS_DVWA_Policy	154.8.226.134	10.20.2.5	High	Alert_Deny	13.71.83.128
8	02:17:13	TCTS_DVWA_Policy	154.8.226.134	10.20.2.5	High	Alert_Deny	localhost
9	02:17:13	TCTS_DVWA_Policy	154.8.226.134	10.20.2.5	High	Alert	localhost
10	02:23:58	TCTS_DVWA_Policy	46.565.27.51	10.20.2.5	High	Alert_Deny	none
11	02:23:58	TCTS_DVWA_Policy	46.565.27.51	10.20.2.5	High	Alert_Deny	none
12	02:23:59	TCTS_DVWA_Policy	197.232.29.67	10.20.2.5	High	Erase	13.71.83.128:80
13	02:23:59	TCTS_DVWA_Policy	197.232.29.67	10.20.2.5	High	Erase	13.71.83.128:80
14	02:23:22	TCTS_DVWA_Policy	189.79.45.14	10.20.2.5	High	Erase	13.71.83.128:80
15	02:23:22	TCTS_DVWA_Policy	303.123.561.138	10.20.2.5	High	Erase	13.71.83.128
16	02:23:22	TCTS_DVWA_Policy	303.123.561.138	10.20.2.5	High	Alert_Deny	13.71.83.128
17	02:23:22	TCTS_DVWA_Policy	303.123.561.138	10.20.2.5	High	Alert_Deny	13.71.83.128
18	02:23:22	TCTS_DVWA_Policy	303.123.561.138	10.20.2.5	High	Alert_Deny	13.71.83.128
19	02:23:22	TCTS_DVWA_Policy	303.123.561.138	10.20.2.5	High	Alert_Deny	localhost
20	02:23:22	TCTS_DVWA_Policy	303.123.561.138	10.20.2.5	High	Alert	localhost
21	02:23:19	TCTS_DVWA_Policy	190.32.506.242	10.20.2.5	High	Erase	13.71.83.128:80
22	02:23:18	TCTS_DVWA_Policy	188.8.147.183	10.20.2.5	High	Erase	13.71.83.128:80
23	02:23:17	TCTS_DVWA_Policy	302.565.48.12	10.20.2.5	High	Erase	13.71.83.128
24	02:23:17	TCTS_DVWA_Policy	309.585.173.21	10.20.2.5	High	Erase	13.71.83.128:80
25	02:23:16	TCTS_DVWA_Policy	96.9.69.222	10.20.2.5	High	Erase	13.71.83.128:80
26	02:23:13	TCTS_DVWA_Policy	200.71.90.93	10.20.2.5	High	Erase	13.71.83.128:80
27	02:23:10	TCTS_DVWA_Policy	14.184.7.190	10.20.2.5	High	Erase	none
28	02:23:10	TCTS_DVWA_Policy	195.17.51.48	10.20.2.5	High	Erase	13.71.83.128:80
29	02:23:10	TCTS_DVWA_Policy	136.304.163.210	10.20.2.5	High	Erase	none

**Detailed Information**

Date: 2019-02-24

Time: 04:28:45

Log ID: 20000008

MSG ID: 000000041727

Type: attack

FortiWeb Device ID: FWM040000379772

Time Zone: GMT-8:00(Pacific Time[US&Canada])

Protocol: tcp

Service: http

Cipher Suite: none

HTTP Version: 1.x

Action: Alert\_Deny

Policy: TCTS\_DVWA\_Policy

Method: get

URL: /DVWA/phpinfo.php

HTTP Host: www.protected.com

FortiWeb Session ID: 4A05823BNA3V3PSVKV25KIUAM5U XNF76

Severity Level: High

Signature Subclass Type: PHP Injection

Signature ID: 050080035

CVE ID: N/A

OWASP Top10: A1-2017-Injection

Source Country: Spain

HTTP Content Routing: none

Server Pool: DVWA-Ubuntu

Username: Unknown

Monitor Mode: Disabled

HTTP Referrer: http://www.protected.com/DVWA/securify.php

Client Device ID: none

Main Type: Signature Detection

Sub Type: Generic Attacks

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.