





# SANGFOR SSL VPN Solution

By using the exclusive acceleration technology of SANGFOR SSL VPN, enterprises are able to provide users with a satisfied and efficient remote access experience, which improves the work productivity of remote workforces.



## Rapid

### Less Bandwidth Required

Compression is commonly used in other solutions but not enough to offer a high-speed SSL VPN connection. SANGFOR SSL VPN innovates by adopting the Byte Cache technology into SSL VPN sessions, which effectively eliminates 30-90% of redundant traffics on SSL VPN links and improves the access speed of remote users.

### Smooth Performance under Harsh Network Environments

Under harsh network environments such as cross-border and cross-operator with high packet loss rate or high latency, the access speed would be significantly lower than one had expected.

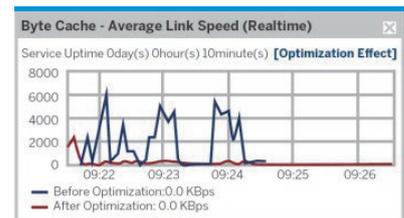
SANGFOR SSL VPN employs HTP (High-speed Transfer Protocol) to smooth the transfer environment and minimize the negative impact of packet loss and latency. End users are able to consistently enjoy a favorable access experience.

### Access Optimization on Tablets and Mobile Devices

In order to solve the display and slow connection problems that tablets and mobile devices users might encounter when accessing browser-based applications, SANGFOR SSL VPN not only optimizes the page display and mobile access, but also provides various image optimization policies such as image filtering and compression to prevent the problems mentioned above.

### Full Utilization of Resources

Considering real-life deployment, SANGFOR SSL VPN is also equipped with Intelligent Link Selector. The Intelligent Link Selector can automatically select the optimal link for remote access when there are multiple links.




**Never Been So Fast !**  
SANGFOR SSL VPN provides remote user with extraordinary access performance and experience by embedding acceleration technologies without additional license fee !



## Secure

### Identity Authentication

#### Authentication

- Support up to 8 types of authentication methods.
- User name/password, LDAP, RADIUS, CA (Certification Authority).
- Certificate/USB key based authentication, Dynamic token, Hardware ID, SMS.

#### Host Checker

- Endpoint detection and scanning of operating system, registry files, personal firewall, anti-virus files, user- customized security rules and other security policies prior to user login as well as during SSL VPN session.

#### Account Binding

- Binds SSL VPN user accounts to authorized applications accounts for account compliance and management.

### Transmission Security

#### Tunnel Encryption

- SSL session encryption.

#### Dedicated SSL VPN Tunnel

- Provides the flexibility of disconnecting all other Internet connections but SSL VPN session to prevent intrusions and attacks from Internet.

#### Man-in-the-middle Attack Detection

- Detects and alerts if the endpoint is suffering from Man- in-the-middle" Attack before it is connected to the Intranet.

#### Cache Cleanup

- Wipes off any cached data when the SSL VPN session terminates, which avoids data leakage if any remote users are accessing SSL VPN with a public endpoint.

### Resources Authorization Policy

#### "User-Role-Resource"Assignment

- Accurately and meticulously assigns resources to specifically defined users or roles, which avoids unauthorized usage of published applications.

*SANGFOR SSL VPN has built-in all-round security protection polices including identity authentication, endpoint security, transmitting security and resources authorization polices to achieve a secure remote connection.*



## Simple

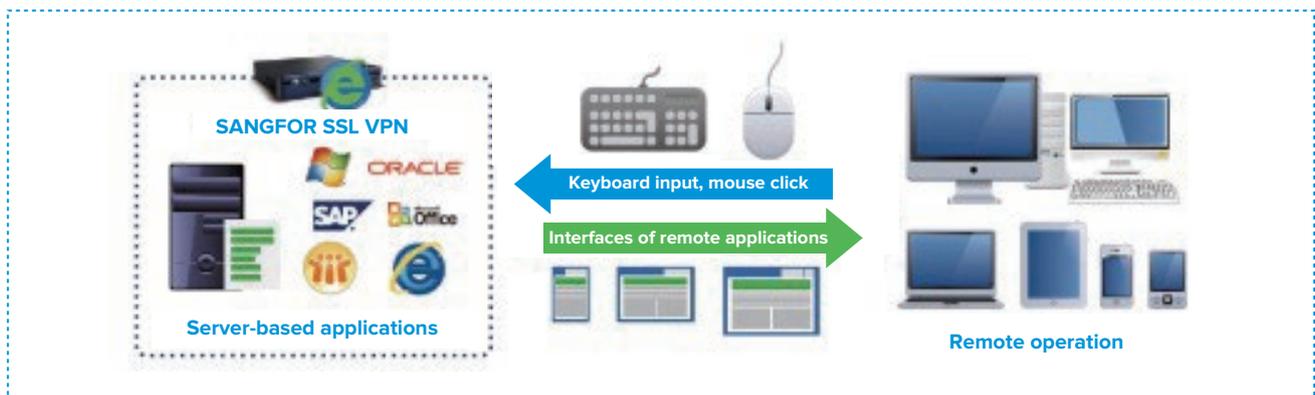
SANGFOR SSL VPN simplifies the account/authentication by allowing administrators to do seamless combination with the LDAP/RADIUS servers and supporting SSO (single-sign-on) with published applications.

### Application Virtualization Delivers Applications as On-demand Service

With new diversity of endpoints and business applications, IT managers have always been looking for a better remote access solution. This way business applications can be securely delivered to remote workforces as an on-demand service via a browser, with no limitation to remote workspaces, application types or available endpoints. SANGFOR SSL VPN Remote Application is the solution.

### SANGFOR Remote Application for Application Virtualization

- Interfaces of published applications are pushed to endpoints screens as virtual access windows, so end users are able to remotely access the applications through a browser.
- Operation and control on applications occur in the server end, no business data will be stored locally.



With SANGFOR Remote Application, business applications are virtualized, centralized and managed in the datacenter and instantly delivered as a service to those users in need. Since everything occurs within the virtual application servers, users are virtually operating in the enterprise network, which prevents any possibility of data leakage.

### Smooth Access from Tablets and Smart Phones

As business applications are delivered to remote workforce as on-demand service, remote workforces can now access any published applications freely from any endpoints with a browser including mobile devices, no matter the applications are based on Windows or in the form of B/S and C/S.

### Flexible Deployment

Various deployment features are offered for consolidating it into the existing IT infrastructure with typical functions such as the asymmetrical cluster and cloud cluster. Asymmetrical cluster supports robust clustering of different hardware models for scalability. Cloud cluster assigns SSL VPN requests to the fastest and most healthy appliance when SSL VPNs are deployed in multiple data centers that are located in different places.



# EasyConnect Remote Access and Mobile Office for Enterprises

*With Sangfor EasyConnect APP, you are able to access any business applications (Lotus notes, Exchange, OA, SAP, ERP, CRM, etc.) remotely from your smartphones and tablets!*

Remote and mobile connectivity has always been of value to enterprises. With the increasing popularity of smartphones and tablets, there is an ever increasing demand for a convenient and secure approach for remote access to corporate data to perform business activities. However, as the enterprises are expanding the network infrastructure to the remote workforce, IT managers can find it extremely difficult to provide full application availability for tablets and smartphones due to resource compatibility, OS support and security concerns.

## Sangfor EasyConnect

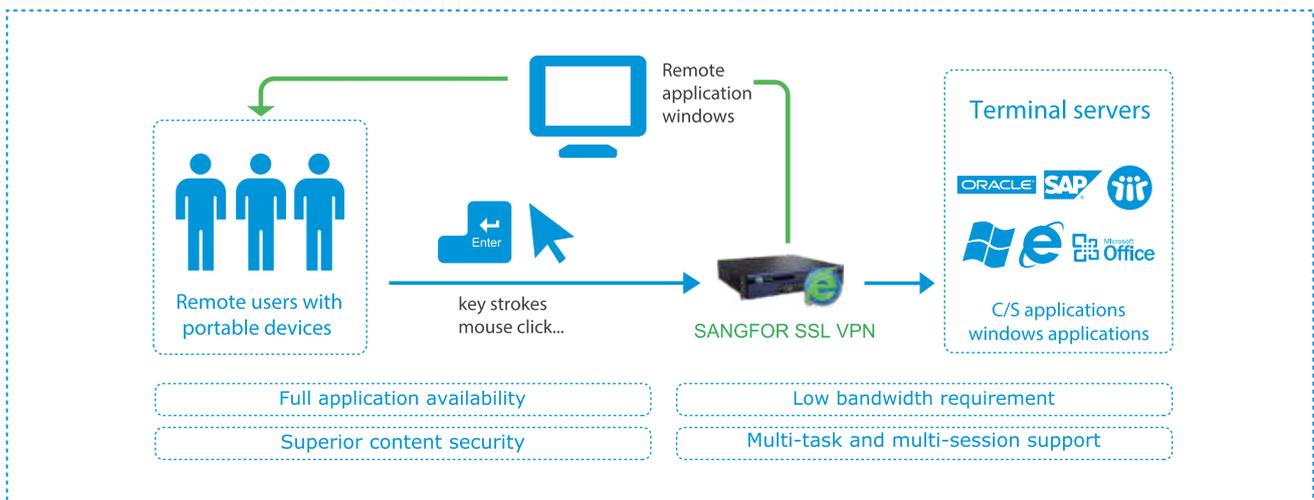
Sangfor EasyConnect, is the tailor-made APP for remote users to access business applications with mobile devices anytime and anywhere, as long as there is a network connection. Remote users are now able to work anywhere!

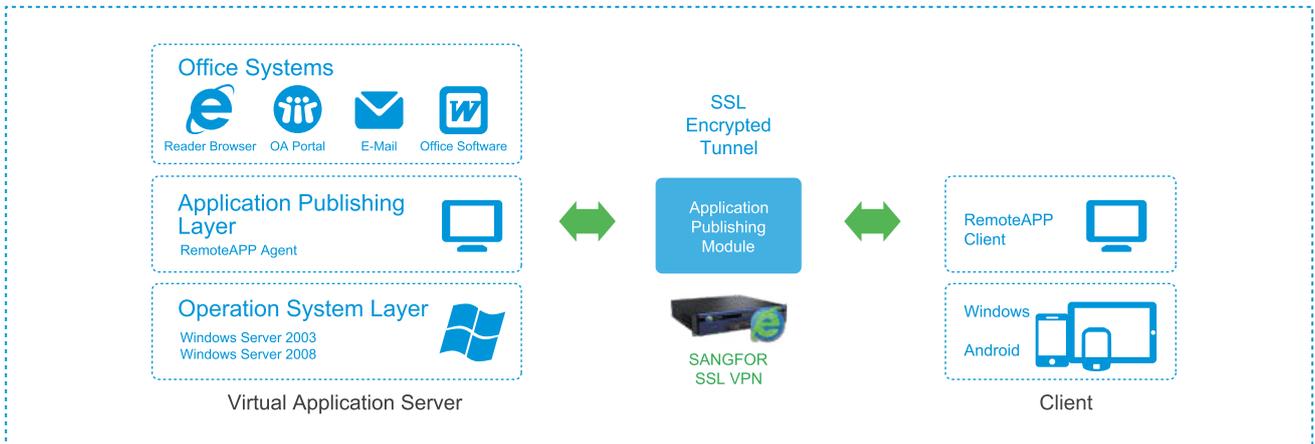


## How does it work ?

EasyConnect is the perfect mobile office solution for business organizations, especially for those that require superior connectivity for remote branches and business travelers. The APP leverage Sangfor's unique remote application technology to simplify mobile and remote access.

To work properly, remote application service needs the following components:





With the remote application enabled, published application interfaces are available on the mobile screens. Thus, users will operate on the virtualized graphical interfaces.

Furthermore, since all processes are conducted in the virtual application servers, by all means users are virtually operating within the corporate network only, avoiding any possibility of information leakage.

#### Remote Application Module

The core of remote application service that is embedded in SSL VPN device, in charge of identity authentication, obtaining resource information from remote servers, data processing and so on.

#### RemoteApp Agent

One ActiveX control that should be installed on remote application server and plays the role of providing remote application service and monitoring server status. By default, auto-start is enabled.

#### Application Client Program

Application client should be installed on the remote application server before publishing the application (such as MS Office, WordPad).

#### RemoteApp Client

A SSL VPN client that should be installed on client end and provides service of connecting to remote server.

### Benefits

- [Workforce Mobility Drives Business Productivity and Continuity](#)

Business travelers are now able to access the business application systems, to work effectively without limitation of location, time or available endpoints, boosting mobile workforce productivity while guarding the business continuity.

- [Full Application Availability to Smart Devices](#)
- [Secure Mobile Office without Leakage Risk](#)
- [Higher IT Productivity by Maximizing Value of IT Resource](#)



# SSL VPN Datasheet



## SANGFOR SSL VPN Rapid, Secure, Simple

SANGFOR SSL VPN solution can be a convenient and effective way of landing a large number of security mechanisms and end-user groups in achieving safe and efficient remote access to enterprise applications, ensuring application system availability for remote workforce while preventing business data exposed to direct risks of internet attacks.

### Product Family

Model	M5100-S-I	M5400-S-I	M5600-S-I
Profile	1U	1U	2U
RAM	1G	2G	4G
HD Capacity	500G	500G	500G
Concurrent Users	300	1200	3800

### Network Interfaces

Model	M5100-S-I	M5400-S-I	M5600-S-I
10/100/1000 Base-T (WAN)	2	4	2
10/100/1000 Base-T (LAN)	1	1	1
10/100/1000 Base-T (DMZ)	1	1	1
SFP	N/A	N/A	4

### Power and Physical Specifications

Model	M5100-S-I	M5400-S-I	M5600-S-I
Dual Power Supplies	N/A	N/A	Y
Power [Watt] (Typical)	40W	180W	212W
Temperature	-10~50°C	-10~50°C	-10~50°C
Relative Humidity	5%~95% non-condensing	5%~95% non-condensing	5%~95% non-condensing
System Dimensions (W×L×H×mm <sup>3</sup> )	430×300×44.5	430×430×44.5	440×500×89
System Weight	4.0 Kg	6.65 Kg	15.3 Kg

### Compliance and Certifications

Model	M5100-S-I	M5400-S-I	M5600-S-I
Compliance	CE, FCC	CE, FCC	CE, FCC

All performance values are "up to" and vary depending on the system configuration.



# SANGFOR SSL VPN: Product Features

## User Authentication

Authentication	Support authentication with combination of AD, local password, LDAP/RADIUS, Certificate/USB key, dynamic token, hardware ID and SMS.
Import of User Accounts	- Import user accounts information using CSV file, LDAP Server. - Synchronize user with LDAP, Database and H3C CAMS Server.
Import of SSL Accounts	Support import of user accounts via CSV file.
CA Authentication	Allow import of local/external CA authenticated certificate.
Account Attribution Options	- Private account for single user. - Public account that allow access for multiple users.
Account Security Enhancement Policies	On-screen keyboard, CAPTCHA, password security options, etc.

## Security Protection

Host Checker	Endpoint detection and scanning of operating system, registry files, personal firewall, anti-virus files, user- customized security rules and other security policies prior to user login, and during the SSL VPN session.
Man-in-the-Middle Attack Detection	Detects if the endpoint is suffering from a Man-in-the- middle attack before it is connected to the internal network and send out alert if any attack is detected.
Dedicated SSL VPN Tunnel	Possibility to disconnect other internet connections when the SSL VPN tunnel is created.
Virtual Secure Portal	Support for creating up to 253 independent secure portals, by which different user groups are able to enjoy different SSL VPN access addresses, authentication methods, application resource, administrators, etc.
Resource Path Hiding	Support for hiding, masquerading of SSL VPN resource path to protect resource security.
Cache Cleanup	Secure and safe deletion of sensitive data after session termination.
Account Binding	Bind user's application account and his/her SSL VPN account together for unified authorization and simplified account administration.
SMS Password Reset	Sangfor SSL VPN supports password retrieval via SMS.

## Rapidity and Access Performance

Byte Cache	Cache data at byte level to ensure the SSL VPN data traffic is de-duplicated, greatly reduces the demanded bandwidth of remote access.
Streaming Compression	Conduct LZO, GZIP/ZLIB compression to TCP and Web applications to decrease the data transmission volume.
Web Cache	Especially optimize accesses to web resource by adopting web cache.
High-speed Transfer Protocol (HTP)	Streamline data packets under high packet loss and network latency network environment such as wireless and cross- border.
Webpage Access Optimization	Dynamic reduction of web pages and images sizes displayed on mobile devices resulting in faster performance and better user experience.
Intelligent Link Selection	Automatically choose the healthy and quickest link for remote access when a network has multiple operators lines.

Application Virtualization	
Remote application (application virtualization)	Delivers the virtual graphical interface of applications to remote users so that users can operate on the applications simply via a browser, while all the calculations/operations take place in server end.
Remote application features	<ul style="list-style-type: none"> <li>- Enable BYOD: Smart phone and tablet users can access all kinds of applications freely. PC users do not need to pre-install application clients before accessing C/S based applications.</li> <li>*BYOD : Bring Your Own Device</li> <li>- Options to enable/disable network drivers, clipboard, printers of endpoints.</li> </ul>
Remote application features	<ul style="list-style-type: none"> <li>- Support virtual printer mapping.</li> <li>- Support local resource invocation.</li> <li>- Various operation optimization policies to mobile devices including local input methods mapping, virtual mouse, magnifier, scrolling tool, tab card, etc.</li> <li>- Support access private resources and public resource on storage servers.</li> <li>- Built-in load balancer for remote application servers on basis of number of sessions , CPU, memory , I / O, integrated performance, etc. Provides secure virtual desktop workspace where all data and I/O traffic are encrypted, monitored and controlled. Under secure desktop environment, applications, data and peripherals activities are restricted according to security policies.</li> <li>- Controlled activities include USB key, printer, file save, file copy, file share, etc.</li> </ul>
Endpoint Usability	
SSL VPN System Tray	Allow personal SSL VPN setups and activities history check through the system tray.
Single-Sign-On	Allow user to access the SSL VPN resource without entering in the username(s)/password(s) when the user get authenticated by SSL VPN.
Appliance management	
Cross Platform Support	<ul style="list-style-type: none"> <li>- Windows, Linux, Mac OS, iOS, and Android OS.</li> <li>- IE, Opera, Firefox, Safari, Google Chrome and other browsers that support https.</li> </ul>
Resource Compatibility	Web app, TCP app, L3VPN, Full support to all kinds of B/S, C/S applications.
Sign-in Page Customization	Fully customizable sign-in page.
Bandwidth Control	<ul style="list-style-type: none"> <li>- Support for setting TCP session limitation based on user.</li> <li>- Support for setting inbound and outbound bandwidth limitation based on user.</li> </ul>
Logging & Reporting	<ul style="list-style-type: none"> <li>- Display real-time status including CPU, link traffic, network throughput, concurrent sessions, byte cache status, etc. connected SSL VPN users.</li> <li>- Online user information: access time, authentication methods, concurrent sessions, traffic flow, IP address, etc.</li> <li>- Alarm, error, debugging, system management logs, back up logs can dump and save externally.</li> <li>- Syslog support.</li> </ul>
Stability	
Web Browser & OS Compatibility	<ul style="list-style-type: none"> <li>- EasyConnect client supports Windows browsers and mobile OS such as Android and iOS.</li> <li>- Comprehensive web browsers support in primary OS.</li> </ul>
Link Stability	Enable tunnel auto switch when used with multiple Internet link deployments.
Asymmetrical Cluster	Supports robust clustering of different hardware models with the capability of up to 20 nodes.
Cluster Cloud	Enabling of multiple Sangfor SSL VPN devices clustered in cloud or multi-datacenter environment.
HA Deployment	Support HA and the session synchronization.
Bypass	Hardware bypass.

Please do not hesitate to contact us by email or by phone if you need more information about our SSL VPN features.



# COMPANY PROFILE



Sangfor Technologies is a leading global vendor of IT infrastructure solutions, specializing in Cloud Computing & Network Security with a wide range of products including: Hyper-Converged Infrastructure, Virtual Desktop Infrastructure, Next Generation Firewall, Internet Access Management, WAN Optimization, SD-WAN and many others.

Sangfor takes customers' business needs and user experience seriously, placing them at the heart of our corporate strategy. Constant innovation and commitment to creating value for our customers helps them achieve sustainable growth. Established in 2000, Sangfor currently has 5,000 + employees with more than 60 branch offices globally in exciting locations like Hong Kong, Malaysia, Thailand, Indonesia, Singapore, Philippines, Vietnam, Myanmar, Pakistan, UAE, Italy and the USA.

# CONTINUOUS INNOVATION & EXCELLENT SERVICE

Sangfor invests at least 20% of its yearly revenue in R&D, improving current products and developing new solutions in their four R&D centers in the USA & China. So far, Sangfor has applied for more than 940+ patents with more patent applications scheduled for 2019. This dedication to innovation enables Sangfor to release new and updated versions of products every quarter and launch new products yearly or bi-yearly.

Sangfor also emphasizes excellent service. With three Customer Service Centers in Malaysia & China, Sangfor's total customer service capacity exceeds 250 technicians and providers.

With thousands of certified engineers and 24/7 online support 365 days a year, Sangfor customers enjoy fast and personalized on-site service support.

At present, Sangfor has more than 60,000 customers worldwide, many of them Fortune 500 companies, governmental institutions, universities and schools.



# AWARDS & ACHIEVEMENTS



- "Technology Fast 500 Asia Pacific Region" Award for 8 consecutive years from 2005 to 2012 by Deloitte
- Sangfor SSL VPN no. 1 in Network Security market in China, Hong Kong & Taiwan according to F&S
- No. 1 for Secure Content Management Hardware and VPN Hardware segment in China according to IDC
- Sangfor IAM listed in the Gartner MQ for Secure Web Gateways (2011-2018)
- Sangfor WANO listed for 3 consecutive years in the Gartner MQ for WAN Optimization (2013-2016)
- Sangfor NGAF listed in the Gartner MQ for Enterprise Network Firewalls (2015-2018)
- Sangfor NGAF WAF recommended by NSS labs (2014)
- Sangfor HCI listed in the Gartner MQ for x86 Server Virtualization Infrastructure MQ (2016)
- ICSA Labs certification for SANGFOR Next Generation Firewall (2018)
- "Most Promising Network Security Solution" in June 2016 by Singapore NetworkWorld Asia
- "Readers Choice Awards for Enterprise Security" in October 2016 by Computerworld Malaysia
- Member of various technology alliances including VirusTotal

# Sangfor SSL VPN

---

## SANGFOR SINGAPORE

8 Burn Road # 04-09, Trivex,  
Singapore (369977)  
Tel: (+65) 6276 9133

## SANGFOR HONG KONG

Unit 04, 6/F, Greenfield Tower, Concordia Plaza,  
No.1 Science Museum Road, Tsim Sha Tsui East,  
Kowloon, Hong Kong  
Tel: (+852) 3427 9160  
Fax: (+852) 3427 9910

## SANGFOR INDONESIA

MD Place 3rd Floor, Jl Setiabudi No.7, Jakarta Selatan  
12910, Indonesia  
Tel: (+62) 21 2933 2643  
Fax: (+62) 21 2933 2643

## SANGFOR MALAYSIA

No. 47-10 The Boulevard Offices, Mid Valley City, Lingkaran  
Syed Putra, 59200 Kuala Lumpur, Malaysia  
Tel: (+60) 3 2201 0192  
Fax: (+60) 3 2282 1206

## SANGFOR THAILAND

6th Floor, 518/5 Maneeya Center Building, Ploenchit Road,  
Lumpini, Patumwan, Bangkok, 10330 Thailand  
Tel: (+66) 22517700  
Fax: (+66) 22517700

## SANGFOR USA

2901 Tasman Drive, Suite 107, Santa Clara, California, USA  
Tel: (+1) 408 520 7898  
Fax: (+1) 408 520 7898

## SANGFOR EMEA

C-80 (C-Wing), Dubai Silicon Oasis HQ Building, Dubai, UAE  
Tel: +971-52-9606471

## SANGFOR Pakistan

D203, Navy Housing Scheme, ZamZamma, Karachi, Pakistan  
Tel: +92 3142288929

## SANGFOR ITALY

Sede Legale ed Operativa via E. Berlinguer, 9 20834 Nova  
Milanese MB Italia  
Tel: +393400616767

## SANGFOR USA

2901 Tasman Drive, Suite 107, Santa Clara, California, USA  
Tel: (+1) 408 520 7898  
Fax: (+1) 408 520 7898

## AVAILABLE SOLUTIONS

- IAM** Simplify User & Network Management
- NGAF** Smarter Security Powered By AI
- SD-WAN** Boost Your Branch Business With Sangfor
- WANO** Enjoy a LAN Speed on your WAN
- HCI** Driving Hyperconvergence to Fully Converged
- aCLOUD** Enterprise Cloud Built on HCI
- VDI** Ultimate User Experience that Beats PC
- aBOS** The World First NFV Converged Gateway
- BBC** Centralized Management Platform



[www.sangfor.com](http://www.sangfor.com)

Sales : [sales@sangfor.com](mailto:sales@sangfor.com)

Marketing : [marketing@sangfor.com](mailto:marketing@sangfor.com)

Global Service Center : +60 12711 7129 (or 7511)

Our Social Networks :



<https://twitter.com/SANGFOR>



<https://www.linkedin.com/company/sangfor-technologies>



<https://www.facebook.com/Sangfor>



<https://plus.google.com/+SangforTechnologies>



<http://www.youtube.com/user/SangforTechnologies>