Software Defined WAN (SD-WAN) - Security Implications and Design Solutions

Ken Kaminski
Technical Solutions Architect – Global Enterprise Segment
Cisco Systems
CISSP, GAWN, GPEN, GCIA, GCFA, GMOB, GPYC
June 2017
Agenda

- SD-WAN – What is it?
- Tunnel Transport – Centralized Security Model
- Direct Internet Access
SD-WAN – What is it?

Gartner predicted in 2015 that by the end of 2019 30% of enterprises will deploy SD-WAN technology in their branches.
Enterprise WAN - What’s Going on?

- WAN bandwidth needs are growing!
  - Cloud, BYOD/IOE and Video making it worse
- IT budgets flat or declining
  - Transport/bandwidth costs are majority of WAN budget
- These factors are driving WAN modernization
  - Lower cost transports – Internet, LTE, Carrier Ethernet,
  - Cloud application performance monitoring and optimization
  - Security – strong encryption and threat protection

Cloud

50% of CIOs Expect to Operate via the Cloud by 2015

Mobility

6X More Mobile Data Traffic by 2015

Fat Apps

2/3 of Mobile Traffic Will Be Video
Why is the Internet viable now?

46% of Organizations Are Planning to Transition to Internet Connections

Internet Pricing vs. Reliability, 1998-2012

1Internet Transit Pricing based on surveys and informal data collection primarily from Internet Operations Forums—‘street pricing’ estimates
2Packet delivery based on 15 years of ping data from PingER for WORLD (global server sample) from EDU.STANFORD.SLAC in California

Source: William Norton (DrPeering.net); Stanford ping end-to-end reporting (PingER)
### SD-WAN Solution Components

**Control & Management with Automation**

**Transport Independent**
- Consistent operational model
- Simple provider migrations
- Scalable and modular design
- IPsec routing overlay design

**Intelligent Path Control**
- Dynamic Application best path based on policy
- Load balancing for full utilization of bandwidth
- Improved availability

**Application Optimization**
- Application visibility with performance monitoring
- Application acceleration and bandwidth optimization

**Secure Connectivity**
- Certified strong encryption
- Cloud Managed Security for secure direct Internet access
- Comprehensive threat defense

---

<table>
<thead>
<tr>
<th>AVC</th>
<th>MPLS</th>
<th>3G/4G-LTE</th>
</tr>
</thead>
<tbody>
<tr>
<td>WAAS</td>
<td>Internet</td>
<td>Public Cloud</td>
</tr>
<tr>
<td>Perf Routing</td>
<td>Private Cloud</td>
<td>Private Cloud</td>
</tr>
</tbody>
</table>

---

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential
Hybrid WAN Designs
Traditional and IWAN

Active/Standby
WAN Paths
Primary With Backup

Two IPsec Technologies
GETVPN/MPLS
DMVPN/Internet

Two WAN Routing Domains
MPLS: eBGP or Static
Internet: iBGP, EIGRP or OSPF
Route Redistribution
Route Filtering Loop Prevention

Active/Active
WAN Paths

One IPsec Overlay

One WAN Routing Domain
iBGP, EIGRP, or OSPF
Minimal route filtering
SD-WAN Deployment Models

**Dual MPLS**
- Highest SLA guarantees
- Tightly coupled to SP
- Expensive

**Public Internet**

**Branch**

**MPLS**

**Hybrid**
- More BW for key applications
- Balanced SLA guarantees
- Moderately priced

**Public Internet**

**Enterprise**

**MPLS+**

**Branch**

**Consistent VPN Overlay Enables Security Across Transition**

**Dual Internet**
- Best price/performance
- Most SP flexibility
- Enterprise responsible for SLAs

**Public Internet**

**Enterprise**

**Branch**
SD-WAN: Leveraging the Internet
Secure WAN Transport and Internet Access

1. Secure transport for private and virtual private cloud access

2. Leverage local Internet path for public cloud and Internet access

- Increase WAN transport capacity and app performance cost effectively!
- Improve application performance (right flows to right places)
Dell’Oro SD WAN Market Size

- Forecast base is Access Routers and vCPE
- Estimate the number of CPE devices managed by the SD-WAN controller.
- CPE can be access router or vCPE
- “Control plane sw” includes controller plus VNFs
- Forecast includes both Ent and SP use cases
- Approx. 80% is HW

### SD-WAN Manufacturers Revenue

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>SD-WAN Control Plane Software</td>
<td>$5.7</td>
<td>$13.1</td>
<td>$29.4</td>
<td>$76.0</td>
<td>$106.1</td>
<td>$137.1</td>
<td>$178.2</td>
<td>$211.8</td>
</tr>
<tr>
<td>SD-WAN CPE</td>
<td>$12.5</td>
<td>$29.4</td>
<td>$76.8</td>
<td>$228.1</td>
<td>$368.3</td>
<td>$520.3</td>
<td>$729.2</td>
<td>$900.2</td>
</tr>
<tr>
<td>Total</td>
<td>$18.2</td>
<td>$42.5</td>
<td>$106.2</td>
<td>$304.1</td>
<td>$474.5</td>
<td>$657.4</td>
<td>$907.4</td>
<td>$1,112.0</td>
</tr>
</tbody>
</table>

### Market Share

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Aryaka</td>
<td>130%</td>
<td>124%</td>
<td>159%</td>
<td>40%</td>
<td>29%</td>
<td>30%</td>
<td>19%</td>
<td></td>
</tr>
<tr>
<td>BigLeaf</td>
<td>135%</td>
<td>161%</td>
<td>197%</td>
<td>62%</td>
<td>41%</td>
<td>40%</td>
<td>23%</td>
<td></td>
</tr>
<tr>
<td>Certes</td>
<td>134%</td>
<td>150%</td>
<td>186%</td>
<td>56%</td>
<td>39%</td>
<td>38%</td>
<td>23%</td>
<td></td>
</tr>
<tr>
<td>Citrix</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CloudGenix</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cradlepoint</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ecessa</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Elfiq</td>
<td>31%</td>
<td>31%</td>
<td>28%</td>
<td>25%</td>
<td>22%</td>
<td>21%</td>
<td>20%</td>
<td>19%</td>
</tr>
<tr>
<td>Fatpipe</td>
<td>69%</td>
<td>69%</td>
<td>72%</td>
<td>75%</td>
<td>78%</td>
<td>79%</td>
<td>80%</td>
<td>81%</td>
</tr>
<tr>
<td>Glue Networks</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
</tr>
<tr>
<td>Juniper</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mushroom Networks</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nginx/Nuage</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Riverbed</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SilverPeak</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sonus</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tami</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TELoP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Teridion</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VeloCloud</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Versa Networks</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Viptela</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Source: Dell’Oro NFV Forecast, October 2016
Tunnel Transport – Centralized Security Model
Central versus Direct Internet Access

Central Internet Access

- Sub-optimal access to cloud based resources
- All traffic traverses the WAN

Direct Internet Access

- Optimal access to cloud based resources
- Only Internal traffic traverses the WAN
### SD-WAN Tunnel Transport

#### Secure VPN

<table>
<thead>
<tr>
<th><strong>VPN</strong></th>
<th><strong>IPsec overlay</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Secure transport independent overlay</td>
</tr>
<tr>
<td></td>
<td>• IPsec VPN over public and private WANs</td>
</tr>
<tr>
<td></td>
<td>• Ensures confidentiality, eliminates eavesdropping and man-in-the-middle</td>
</tr>
<tr>
<td></td>
<td>• Strong Cryptography: IKEv2 + AES-GCM 256</td>
</tr>
</tbody>
</table>

| **Device Authentication** | **Certificate based mutual authentication (PKI)** |

| **Network Segmentation** | • Logical (VRF) isolation of provider networks  |
|                         | • Firewall or ACLs blocks all unauthorized traffic  |
Protecting Public facing SD-WAN Interfaces

- Use ACLs or internal or external firewall to block all traffic except the VPN tunnel traffic to routers
- Full Firewall at the branch if there are plans for direct Internet access
- Typical ACL for protecting the Internet interface

```plaintext
interface GigabitEthernet0/0
bandwidth 10000
ip vrf forwarding INET-PUBLIC
ip address dhcp
ip access-group ACL-INET-PUBLIC in
duplex auto
!
ip access-list extended ACL-INET-PUBLIC
permit udp any any eq non500-isakmp
permit udp any any eq isakmp
permit esp any any
permit udp any any eq bootpc
permit icmp any any echo
permit icmp any any echo-reply
permit icmp any any ttl-exceeded
permit icmp any any port-unreachable
!
```
Security challenges with simplified deployment solutions

Security complicates auto-provisioning over the WAN

• Where did this platform arrive from and can you trust it?
  • Directly from the manufacturer
  • From a reseller
  • Out of stock/spare platform

• Can I trust the providers WAN the device is joining from?
  • Private Networks: MPLS L3VPN, Carrier Ethernet L2VPN, Satellite, LTE?
  • Public Networks: Internet, LTE, …?
How do we verify the hardware, software and identity?

Trust Anchor Module (TAM)

<table>
<thead>
<tr>
<th>TAM Enables</th>
<th>TAM Provides</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Authenticity – hardware, software</td>
<td>• Anti-Theft &amp; Anti-Tamper Chip Design</td>
</tr>
<tr>
<td>• Provides Verifiable Identity</td>
<td>• Immutable Identity</td>
</tr>
<tr>
<td>• Secure Crypto assist</td>
<td>• Standard Identity- IEEE 802.1AR (SUDI- X.509 cert)</td>
</tr>
<tr>
<td>• License Check</td>
<td>• Secure Storage of Credentials</td>
</tr>
<tr>
<td></td>
<td>• Certifiable Entropy for Random Number Generation</td>
</tr>
<tr>
<td></td>
<td>• Secure Storage (Keys &amp; Objects)</td>
</tr>
</tbody>
</table>
Verification: Secure Boot
Ensuring the authenticity of software and hardware

• Ensures that the platform has authentic vendor hardware and software
• Software image is signed and verified at boot time
• As the software boots, the system checks to ensure the installed digital certificate is valid
• Subsequent hash checks provides continuous monitoring with runtime integrity

Verifies the software has not been altered or tampered since it was signed
SD-WAN Provisioning: Automated Secure Lifecycle

- **Embedded Trust Devices**
- **Secure Boot – hw/sw Validation**
- **Secure ZTD Boot Strap**
- **Automatic Configuration and Trust Establishment**
- **Dynamic IPsec Crypto/Session Key Management**
- **Automatic Session Key Refresh/Rollover (IKEv2)**
- **Trust Revocation**

- **Campus**
- **Metro-E**
- **Large Site**
- **Branch**
- **Intelligent Branch**
- **4G**
- **MPLS**
- **ISP**
- **Resilient WAN POP**

- **Software Controller**
- **Configuration Orchestration**
- **Key and Certificate Controller**
- **Optional External Certificate Authority**

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential 18
Router Security Certifications

Standards Based with Peer review
Strong Encryption
Branch to HQ Suite-B Support

Threat Landscape Is Changing

- Communications and IT infrastructures must be defended against cyber attacks and exploitation
- Attackers are persistent and well funded
- Computing advances are driving a move to higher cryptographic strengths – NSA 80 bits today, 100 bits 2030
- Future-ready Devices: Meets security and scalability requirements for many years
- Efficiency and scale: Hardware crypto acceleration
- FIPS-140-2 Level 2 and Common Criteria EAL4

<table>
<thead>
<tr>
<th>Legacy Encryption</th>
<th>Hazards</th>
<th>Cisco Suite-B</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES, 3DES</td>
<td>1GB Encryption Limit</td>
<td>✓ AEAD: AES-128-GCM</td>
</tr>
<tr>
<td>HMAC-MD5 - Authc</td>
<td>Theoretical Weakness</td>
<td>✓ HMAC-SHA-256 (not need w/AEAD)</td>
</tr>
<tr>
<td>DH, RSA</td>
<td>Significant Risk-1024</td>
<td>✓ ECC - ECDH</td>
</tr>
<tr>
<td>RSA Dig Sigs</td>
<td>Significant Risk - 1024</td>
<td>✓ ECC - ECDSA</td>
</tr>
<tr>
<td>MD5, SHA1</td>
<td>Collision Attacks</td>
<td>✓ SHA-256</td>
</tr>
<tr>
<td>Entropy</td>
<td>Significant Risk</td>
<td></td>
</tr>
<tr>
<td>TLS1.0, IKEv1</td>
<td>Known Flaws, no Authentication</td>
<td>IKEv2</td>
</tr>
</tbody>
</table>
Direct Internet Access – Distributed Security Model
SD-WAN—Direct Internet Access

- Leverage **Local Internet path** for Public Cloud and Internet access
- Improve application performance (right flows to right places)

**Solutions**
- On Premise – Firewall
- Cloud Based – Cloud Web Proxy
SD-WAN Direct Internet Access

CIO & Network Team

CISO & Security Team
DIA Deployment Model Use Cases

- **Branch Direct Internet Access**
- **Corporate Network**
- **Virtual Private Cloud**
- **Public Cloud**
- **Cloud Security Services**

**Compliance**
- VPN
- Firewall
- Snort IPS

**Guest Access**
- VPN
- Firewall
- Snort IPS
- Cloud Security Services

**Direct Cloud Access**
- VPN
- Cloud Security Services
- Firewall
- NGIPS

**Direct Internet Access**
- VPN
- Cloud Security Services
- Firewall
- NGIPS
Guest Internet Access

- VLAN separation, guest devices are outside the branch corporate network
- FW blocks inter-VLAN traffic
- Cloud Web Security provides content filtering and policy enforcement
- Snort Powered IPS provides basic intrusion protection
- Corporate devices reach Internet via HQ

Examples:
Retail stores / Auto Dealerships
Hospitals / Pharmacies
Financials
Schools / Universities
Direct Cloud / Partner Access

- Domain Based Routing, routes only the cloud specific traffic directly
- FW provides pinholes for return traffic from cloud services
- Cloud Security services provide additional protection

Examples:
Retail stores accessing Supplier websites
Hospital / Pharmacy accessing Insurance websites
Cloud based enterprise service (webex, salesforce etc.)
Current problem: Cloud Security is based on whitelists and these are based on IP addresses with a limited number allowed. These define what is **not** sent to Internet and stays on corporate network. Requirement: Whitelist of apps to only send to the Internet and solve Office365 Problem of changing IP addresses and route on domains.

- Domain Based Routing, routes only the cloud specific traffic directly.
- Add metadata to DNS server of App-ID and port numbers to domain.
- Router looks at this and applies policy like Route to Internet.
- Link to Policy Based Routing and Performance Routing.
All Internet bound traffic is routed directly to Internet
Ideally the same level security as in Head Quarters
Depending on the value of the assets in the branch, security approach can differ
NGFW and NGIPS
Cloud Security Services – more extensive than Web Proxy
Centralized monitoring and threat analysis
## Snort vs NGIPS Threat Defense

<table>
<thead>
<tr>
<th></th>
<th>Threats</th>
<th>Application visibility and control</th>
<th>Contextual awareness</th>
<th>Impact assessment</th>
<th>Automated IPS tuning</th>
<th>User identities</th>
<th>Management Center</th>
</tr>
</thead>
<tbody>
<tr>
<td>Snort IPS</td>
<td>✔️</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NGIPS</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
</tbody>
</table>
How a SIG compares to a SWG

<table>
<thead>
<tr>
<th>Feature</th>
<th>SIG (Secure internet access, anywhere users go)</th>
<th>SWG (Granular web usage controls for compliance and protection)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open platform w/ bi-directional API integrations</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>SaaS discovery and control; works w/ CASB</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Internet traffic enforcement for all ports &amp; protocols</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Cloud-delivered security to cover on and off-network</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Web traffic enforcement for ports 80/443 and HTTP/S</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Web application visibility and control</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Web content filtering</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Web data loss prevention</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Web productivity and bandwidth control</td>
<td></td>
<td>✔</td>
</tr>
</tbody>
</table>

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential
SIG Compared to SWG

Problem:
Incomplete coverage of destinations and files

SWG

HTTP/S layer
AV

VENDOR FEEDS

REACTIVE FILE INTEL

SIG

DNS and IP layer

HTTP/S layer

Files + AV

VENDOR + CUSTOMER FEEDS

RETROSPECTIVE FILE INTEL
Cloud Security Services

Multiple Technologies Converging

- All Ports + Protocols
- Web proxy
- File inspection & AV
- Sandboxing
Basic Operation of the Machine Learning Software for Branches

1. Discovers traffic paths
2. Builds map of IP addresses to learn about its environment
3. Identifies applications DPI
4. Studies traffic movement, volumes, patterns, times of day
5. Learns to distinguish normal from anomalous
6. Precisely identifies anomaly; allows operator to take action to remediate
Network Function Virtualization (NFV)
Network services in minutes, on any platform

SDN Controllers

Virtual Router
Virtual Firewall
Virtual WAN Optimization
Virtual Wireless LAN Controller
3rd Party VNFs

Network Functions Virtualization Infrastructure Software

Vendor Routers
Servers
Specialized Hardware for Branches
Resources

- SD-WAN Wiki: https://en.wikipedia.org/wiki/SD-WAN
- Network World: SD-WAN: What it is and why you’ll use it one day
- SD-WAN Experts: Security a Driver to Use SD-WAN
- Network World: SD-WAN facilitates security on the WAN