SD-WAN INTERNET CENSUS

or
How to Find SD-WANs and not to Lose Yourself

ZERO NIGHTS 2018

Denis Kolegov
Oleg Broslavsky
Anton Nikolaev

A NEW
SDWANNEWHOPE

A LONG
TIME AGO
IN A GALAXY
FAR, FAR AWAY...

Wait, stop!

Not (really) so long time ago, we decide to start a big SD-WAN journey

SD-WAN / SILVER PEAK NEWS

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

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

Four Reasons Why SD-WAN Makes Sense

By Peter Scott, SD-WAN Contributor

2. Better Security

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

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

The Rise of the SD-WAN

August 2, 2017

By Tony Bardo

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

2^3 EDITION

The Security of SD-WAN

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

Email This Print Comment

Login

50% 50%

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

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

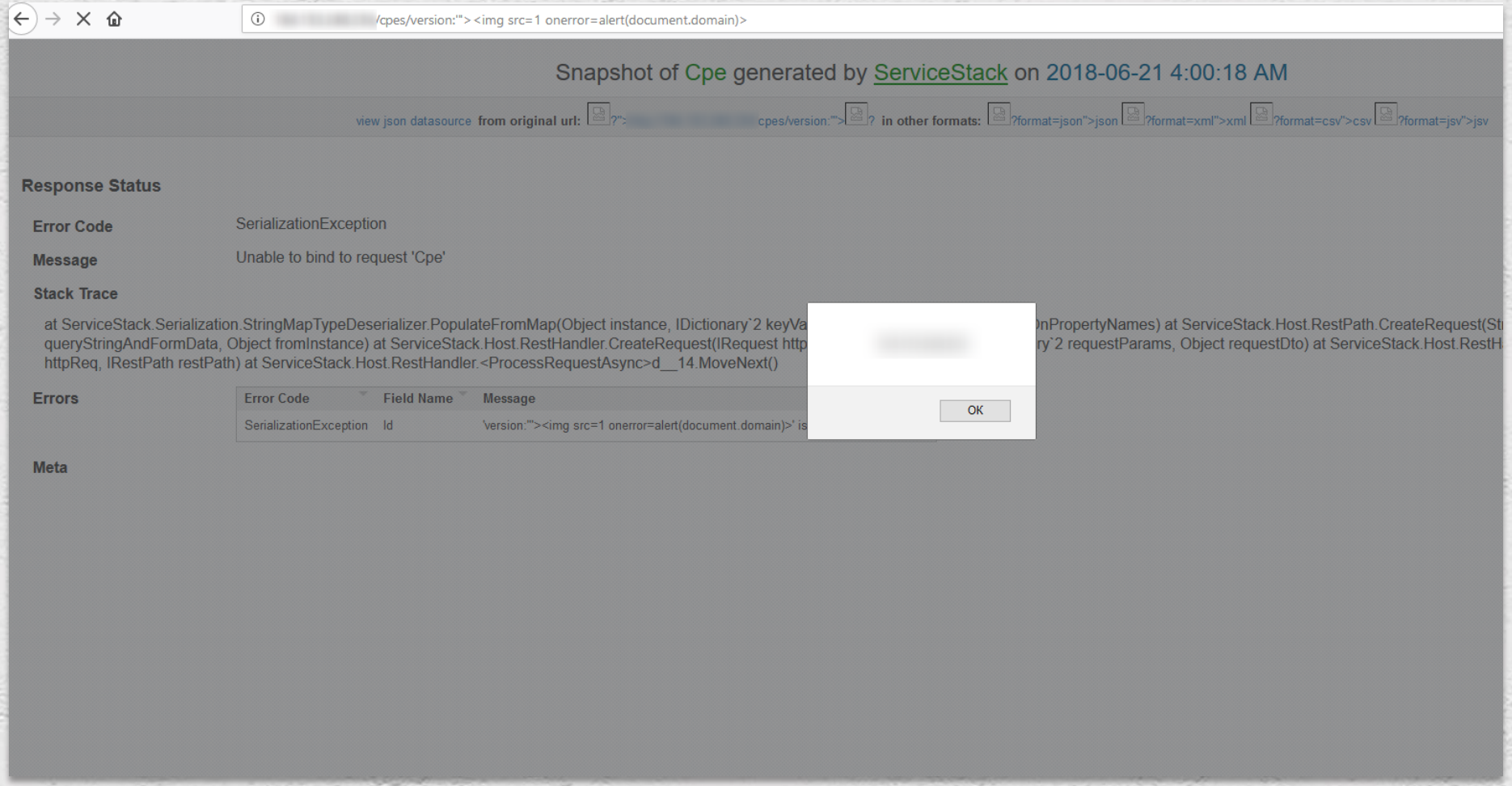
Perfectly safe?

Not exactly…


ZERO
NIGHTS
2018


2 3
EDITION

XSS


/cpes/version:""><img src=1 onerror=alert(document.domain)>
Snapshot of Cpe generated by ServiceStack on 2018-06-21 4:00:18 AM
view json datasource from original url: ?"> cpes/version:""> ? in other formats: ?format=json">json ?format=xml">xml ?format=csv">csv ?format=jsv">jsv
Response Status
Error Code SerializationException
Message Unable to bind to request 'Cpe'
Stack Trace
at ServiceStack.Serialization.StringMapTypeDeserializer.PopulateFromMap(Object instance, IDictionary`2 keyVa nPropertyNames) at ServiceStack.Host.RestPath.CreateRequest(St
queryStringAndFormData, Object fromInstance) at ServiceStack.Host.RestHandler.CreateRequest(IRequest http ry`2 requestParams, Object requestDto) at ServiceStack.Host.RestH
httpReq, IRestPath restPath) at ServiceStack.Host.RestHandler.<ProcessRequestAsync>d__14.MoveNext()
Errors
Error Code
Field Name
Message
SerializationException
Id
'version:""><img src=1 onerror=alert(document.domain)>' is
OK
Meta

EDITION 2^3

Client-side Authentication

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

        };

    }
```

?

!

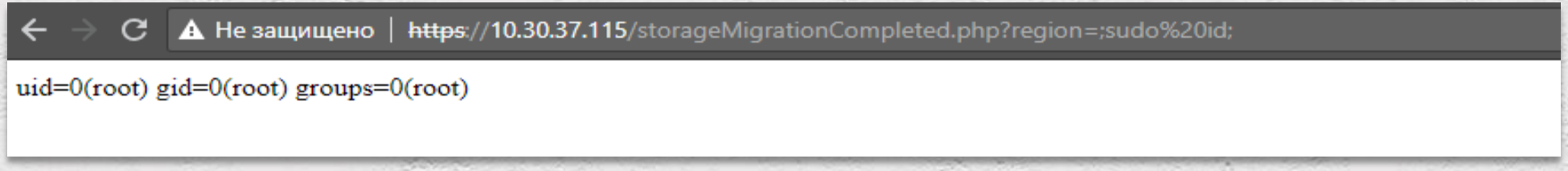
// TODO: fix in prod ?

OS Command Injection

```
$response = shell_exec(
        "cat /home/REDACTED/regions_by_name/"
        .$_GET["region"].
        "/maintenanceCurrentCompleted");
```

OS Command Injection

```
$response = shell_exec(
        "cat /home/REDACTED/regions_by_name/"
        .$_GET["region"].
        "/maintenanceCurrentCompleted");
```



2^3 EDITION

Unfortunately, this talk is not about sophisticated hacking techniques (cause you do not need them to hack SD-WAN)

This talk about how to find those low-hanging fruits on the Internet?

The Main Questions

- How many SD-WAN nodes on the Internet?
- Do we need new techniques to scan and fingerprint them?
- How to find vulnerable SD-WAN nodes?

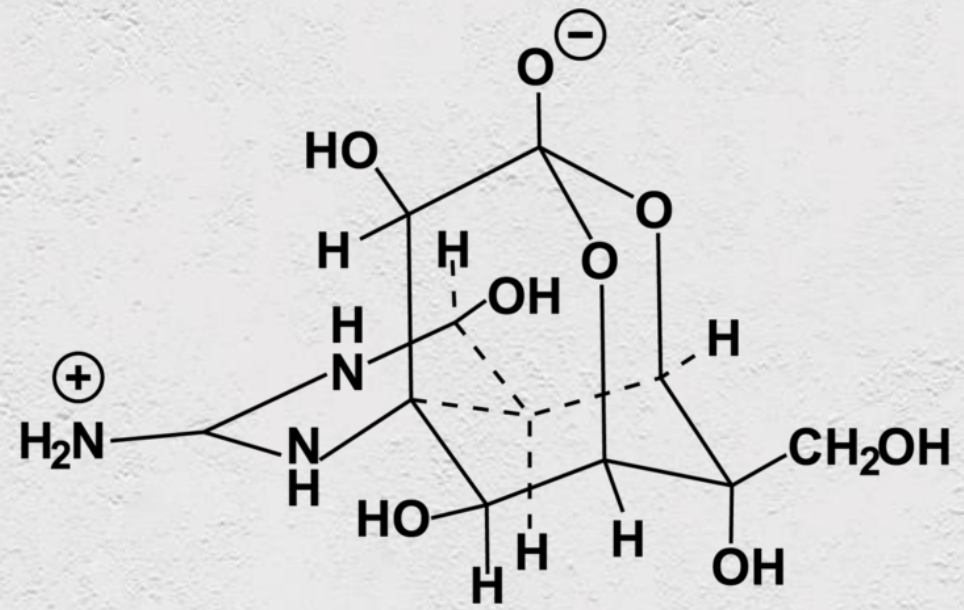
Approach

Best Effort

*When you have to underline the **best effort** approach but you don't know exactly how to*

2^3 EDITION

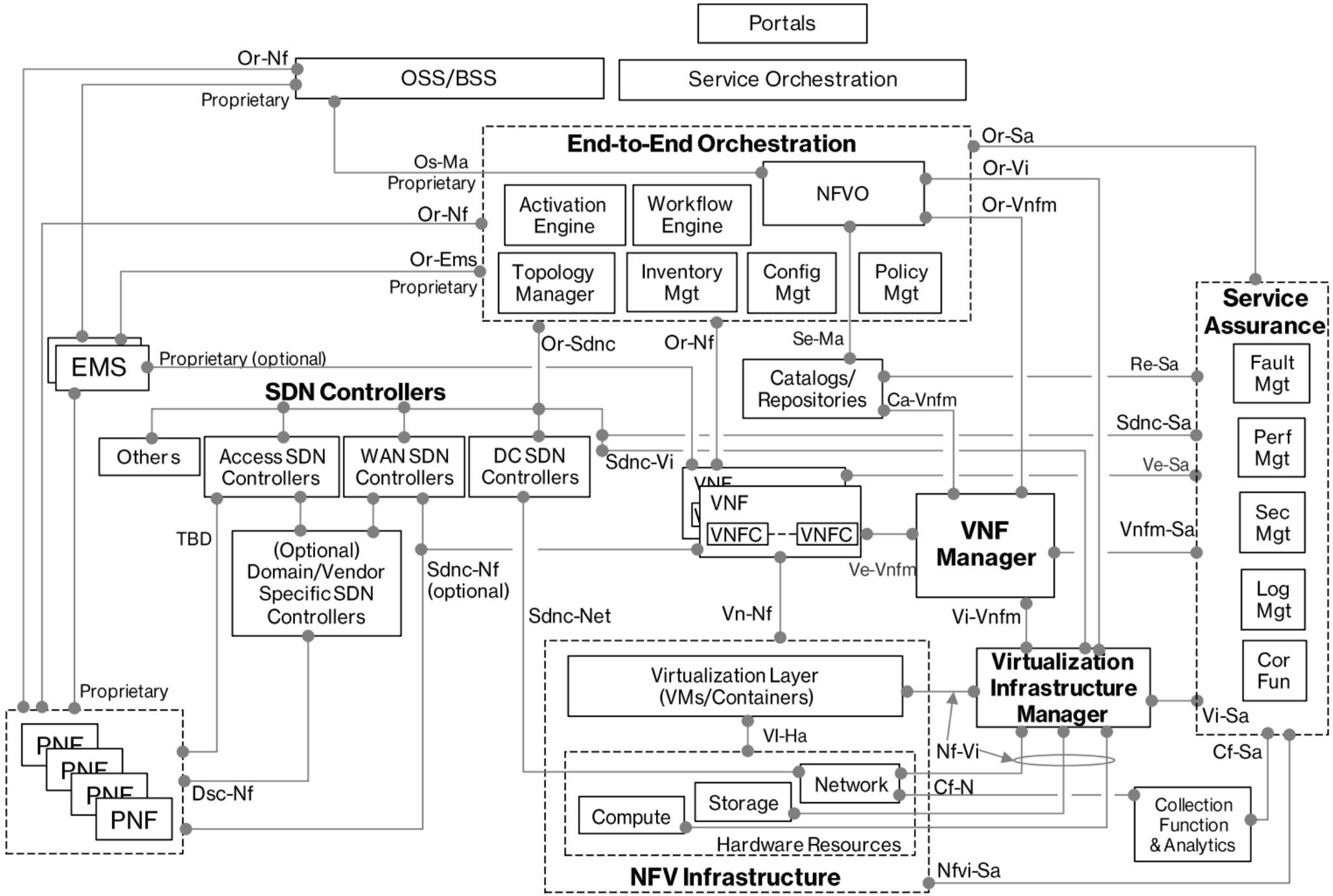
But nevertheless, let's start!



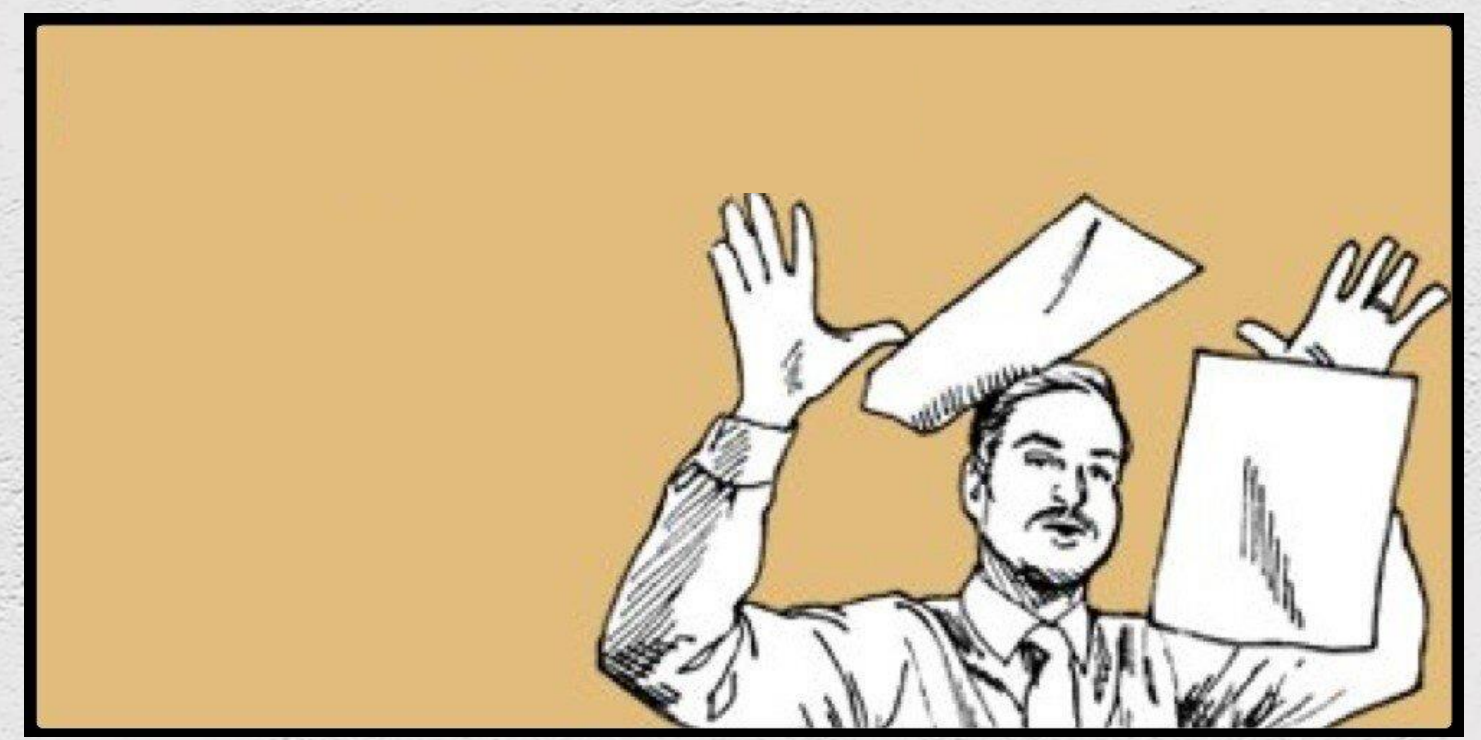
SD-WAN Essence

or

That Boring Part of Slides Again

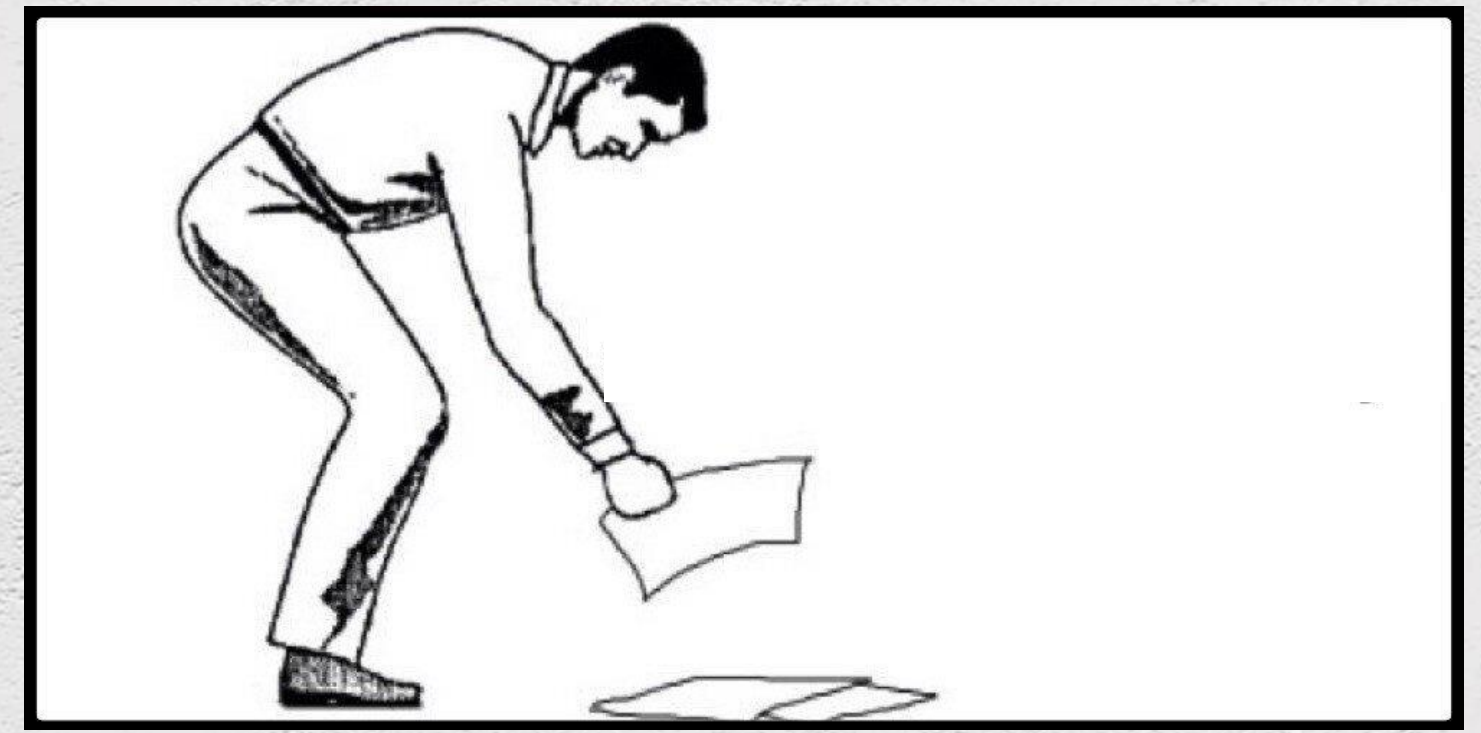

Portals
Or-Nf
Proprietary
OSS/BSS
Service Orchestration
End-to-End Orchestration
Os-Ma
Proprietary
Or-Nf
Or-Ems
Proprietary
Activation Engine
Workflow Engine
NFVO
Topology Manager
Inventory Mgt
Config Mgt
Policy Mgt
Or-Sa
Or-Vi
Or-Vnfm
Service Assurance
Fault Mgt
Perf Mgt
Sec Mgt
Log Mgt
Cor Fun
Re-Sa
Sdnc-Sa
Ve-Sa
Vnfm-Sa
Vi-Sa
Cf-Sa
EMS
Proprietary (optional)
Or-Sdnc
Or-Nf
Se-Ma
Catalogs/ Repositories
Ca-Vnfm
SDN Controllers
Others
Access SDN Controllers
WAN SDN Controllers
DC SDN Controllers
Sdnc-Vi
VNF
VNFC
VNFC
Ve-Vnfm
VNF Manager
Vi-Vnfm
TBD
(Optional) Domain/Vendor Specific SDN Controllers
Sdnc-Nf (optional)
Sdnc-Net
Vn-Nf
Virtualization Layer (VMs/Containers)
Virtualization Infrastructure Manager
Vl-Ha
Nf-Vi
Cf-N
Network
Compute
Storage
Hardware Resources
Collection Function & Analytics
NFV Infrastructure
Nfvi-Sa
Proprietary
PNF
PNF
PNF
PNF
Dsc-Nf

F*ck that shit! We are hackers!

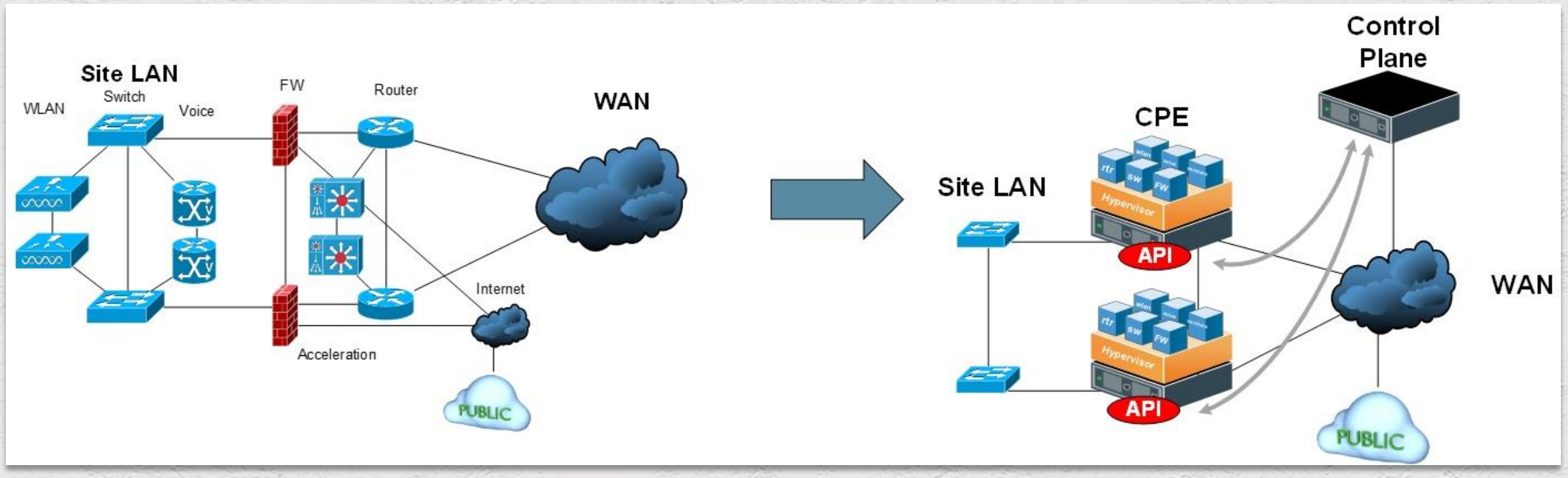


2^3 EDITION

Just kidding.
We need it for understanding.



Traditional WAN vs Software-defined WAN



ZERO NIGHTS 2018

2^3 EDITION

So, we are

Gotta catch 'em all!™

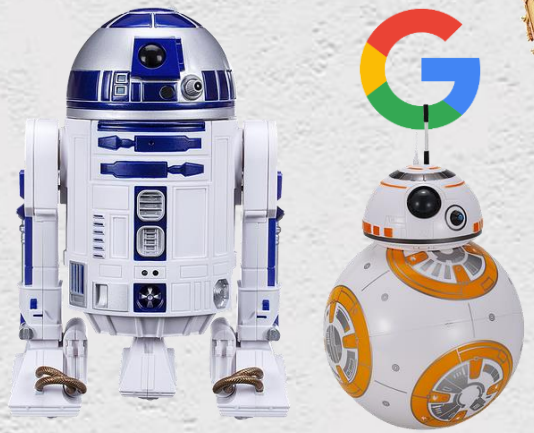
2018.ZERONIGHTS.ORG

2^3 EDITION

Search Engines

SHODAN

censys



Straightforward Examples

```
title:"Viptela vManage"
title:"Cisco vManage"
title:"Flex VNF Web-UI"
```

SHODAN


```
80.http.get.title: "Viptela vManage"
80.http.get.title: "Cisco vManage"
80.http.get.title: "Flex VNF Web-UI"
```

2³ EDITION

More Sophisticated Examples

```
http.favicon.hash:-1338133217
ssl:"Riverbed Apache"
```

SHODAN

censys

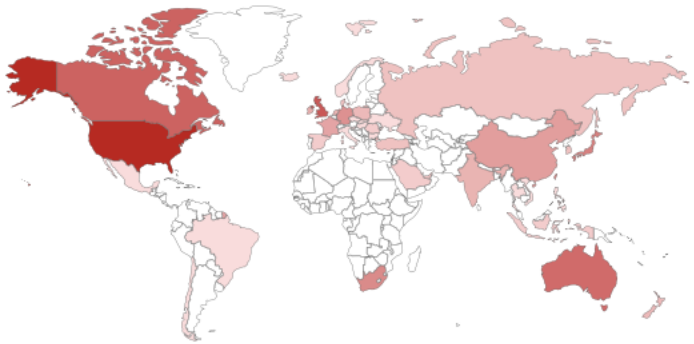
```
80.http.get.body_sha256:
                "867f6fead63c8809f2..."
```

Query Correction

TOTAL RESULTS

488

TOP COUNTRIES



```
html:Sonus
```

```
+ title:
  "SBC Management
   Application"
```

TOTAL RESULTS

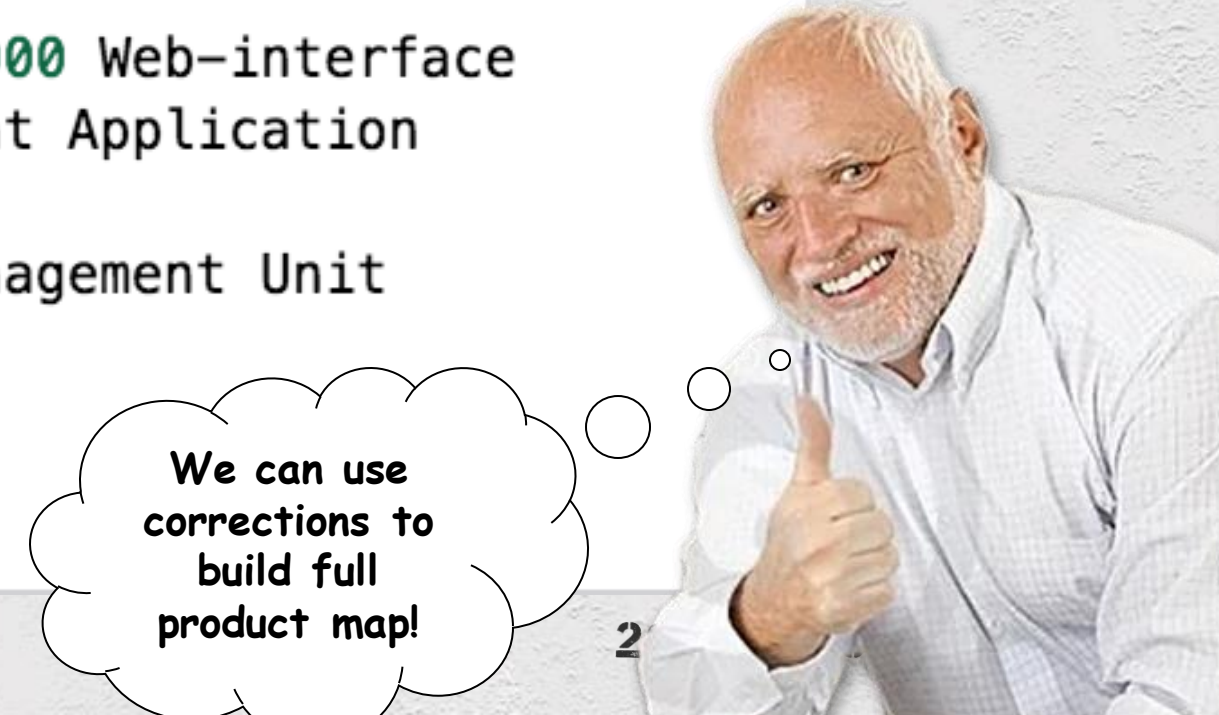
3

TOP COUNTRIES

More Query Correction!

https://github.com/sdnewhop/sdwannewhope/issues/7

```
All Sonus results = 408:
    - 349 - SBC:
        - 196 - SBC Edge
        - 150 - SBC 1000/2000 Web-interface
        - 3 - SBC Management Application
    - 5 - SecureLink
    - 5 - Configuration Management Unit
    - 4 - FTP Servers
    - 20 - Switches
    - 24 - Trash
```



2^3 EDITION

Query Confidence

Tentative Firm Certain


Bugbounter using SDNEWHOP queries
pikabu.ru

Version Leakage

2^3 EDITION

Version Leakage Patterns

```
yalegko:~ $ ssh admin@REDACTED
viptela 17.2.4
admin@REDACTED password:
```

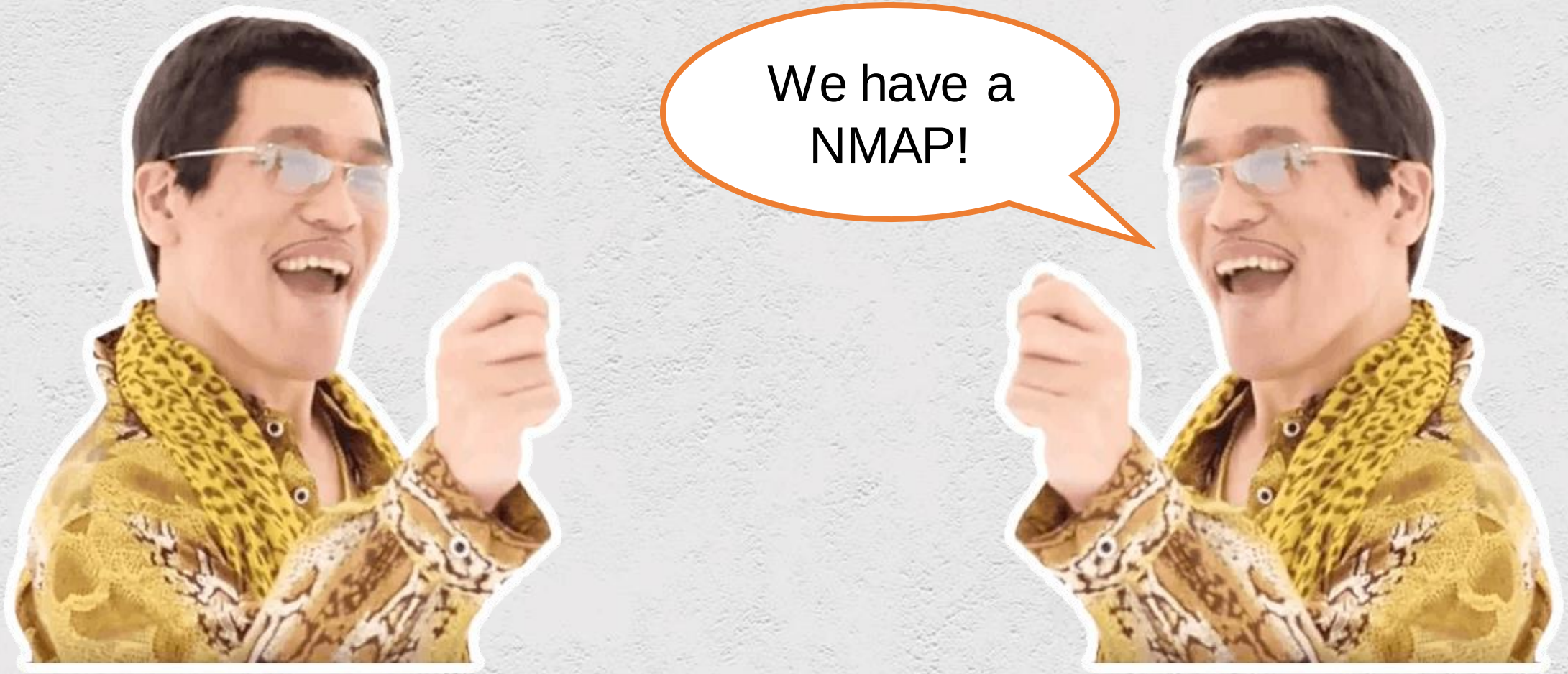
```
<h2 style="margin-top:5px;">FatPipe WARP</h2>
    <h5>9.1.2r142</h5>
```

```
<link href="/br_ui/rdx/core/css/rdx.css?v=9.3.1.35" rel="stylesheet" type="text/css"/>
<link href="/br_ui/app/css/br.css?v=9.3.1.35" rel="stylesheet" type="text/css"/>
```

How to Find Them All?

Let’s help Dora!

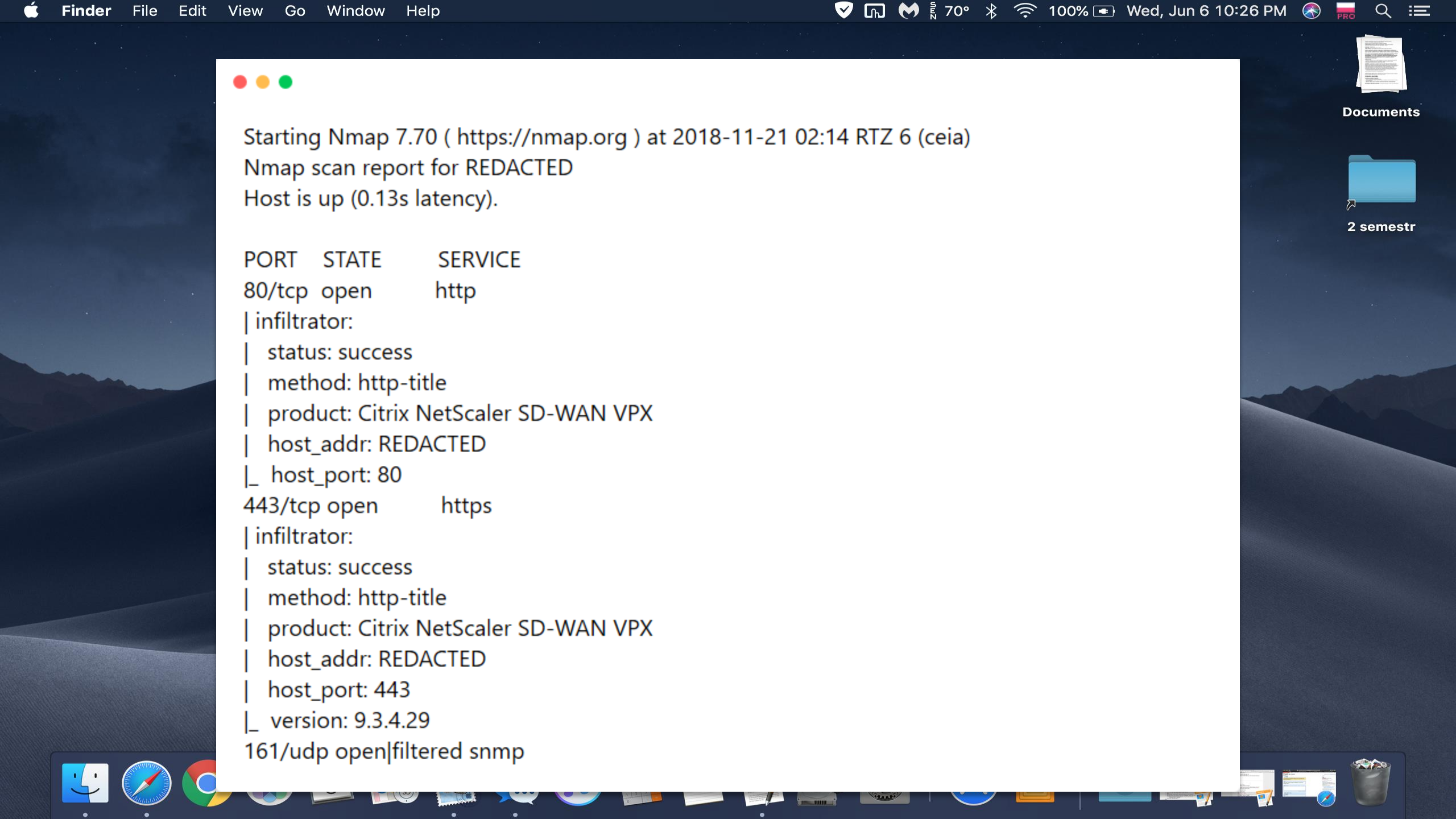

We have a leakage!


We have a
NMAP!


ZERO NIGHTS 2018
2^3 EDITION
Pen Pineapple Apple
SD-WAN
Infiltrator!
2018.ZERONIGHTS.ORG

2³ EDITION

SD-WAN Infiltrator


Finder File Edit View Go Window Help
70°
100%
Wed, Jun 6 10:26 PM
Documents
2 semestr
Starting Nmap 7.70 (https://nmap.org) at 2018-11-21 02:14 RTZ 6 (ceia)
Nmap scan report for REDACTED
Host is up (0.13s latency).
PORT STATE SERVICE
80/tcp open http
| infiltrator:
| status: success
| method: http-title
| product: Citrix NetScaler SD-WAN VPX
| host_addr: REDACTED
|_ host_port: 80
443/tcp open https
| infiltrator:
| status: success
| method: http-title
| product: Citrix NetScaler SD-WAN VPX
| host_addr: REDACTED
| host_port: 443
|_ version: 9.3.4.29
161/udp open|filtered snmp

What About Really Hard Cases?

Easy Peasy Lemon Squeezy?

Difficult Difficult Lemon Difficult!

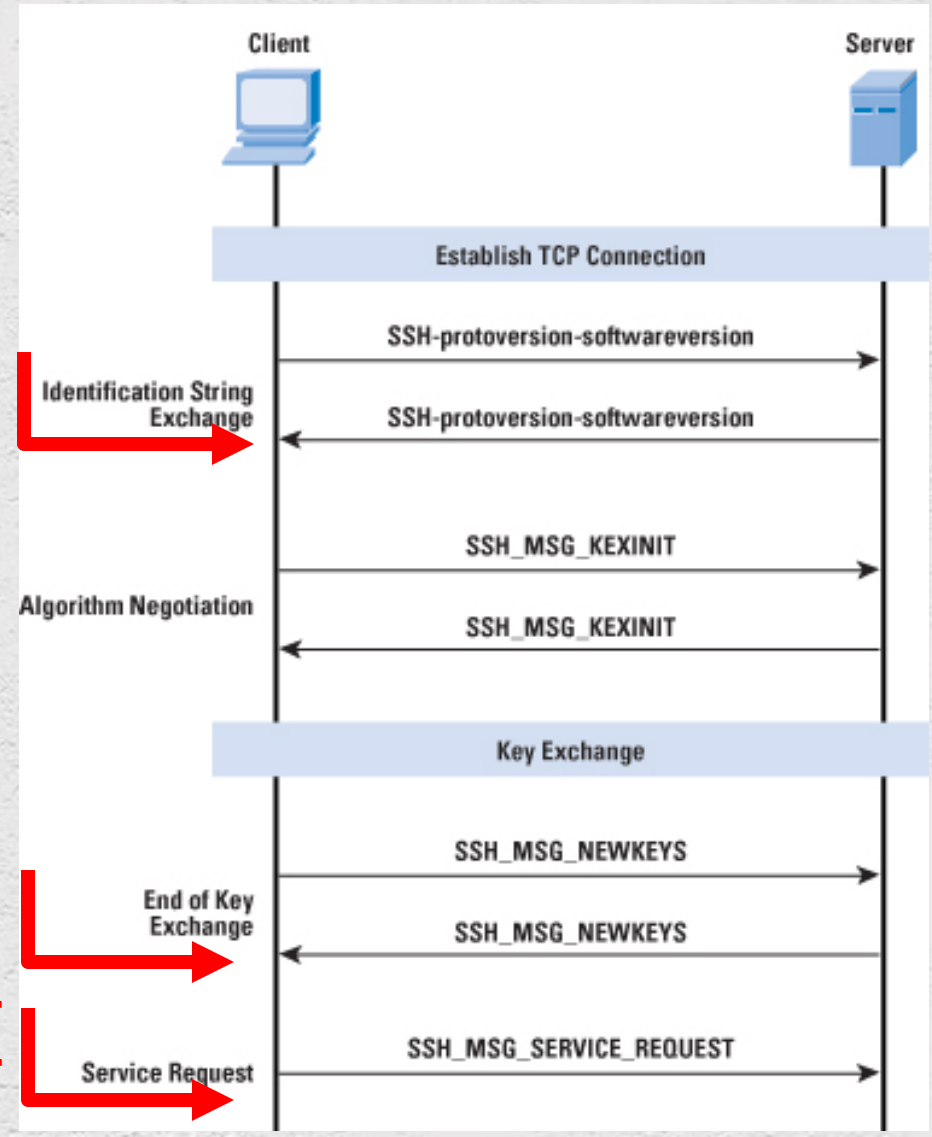
2018.ZERONIGHTS.ORG

SSH Fingerprinting

SD-WAN version in
`/etc/issue` message

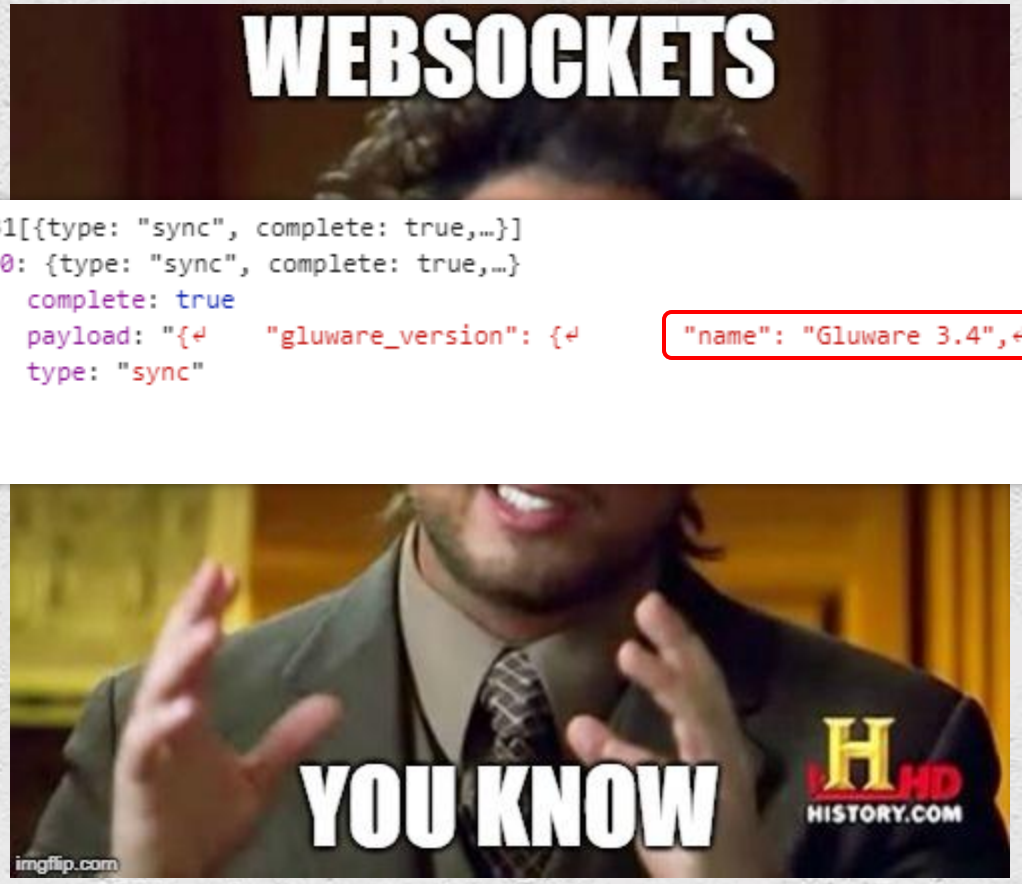
```
yalegko:~ $ ssh admin@REDACTED
viptela 17.2.4
admin@REDACTED password:
```

/nmap/nmap/issues/1389
/sdnewhop/zgrab2



Websocket

- Nmap can’t scan Websocket
- No **standard** NSE Websocket libraries
- Weird behavior in **custom** NSE Websocket libraries



2^3 EDITION

Indirect Version Leakage

Riverbed SteelHead

Dislosure: indirect version
Source: HTML
Example:

```
<meta name="application-name" content="web3 v0.15.8" />
```

VeloCloud Network Orchestrator

Dislosure: UI info
Source: HTTP response
Example:

```
<link href="/css/vco-ui.3.0.0.1509625568730.common.css" rel="stylesheet">
```

Teloip Orchestrator API

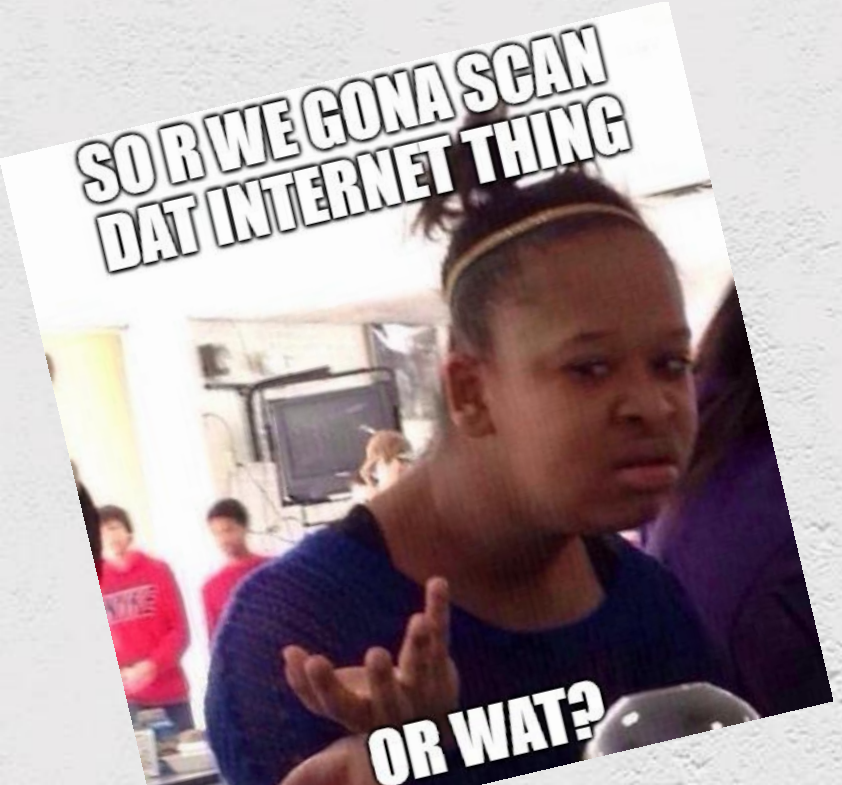
Dislosure: API version
Source: HTML
Example:

```
{"usage":"append '?debug=requestinfo' to any querystring. Optional params: virtualPathCount",
"host":"_v5.02_Teloip Orchestrator API","hostType":"SelfHost (AppHostBase)",...}
```

ZERO NIGHTS 2018

2^3 EDITION

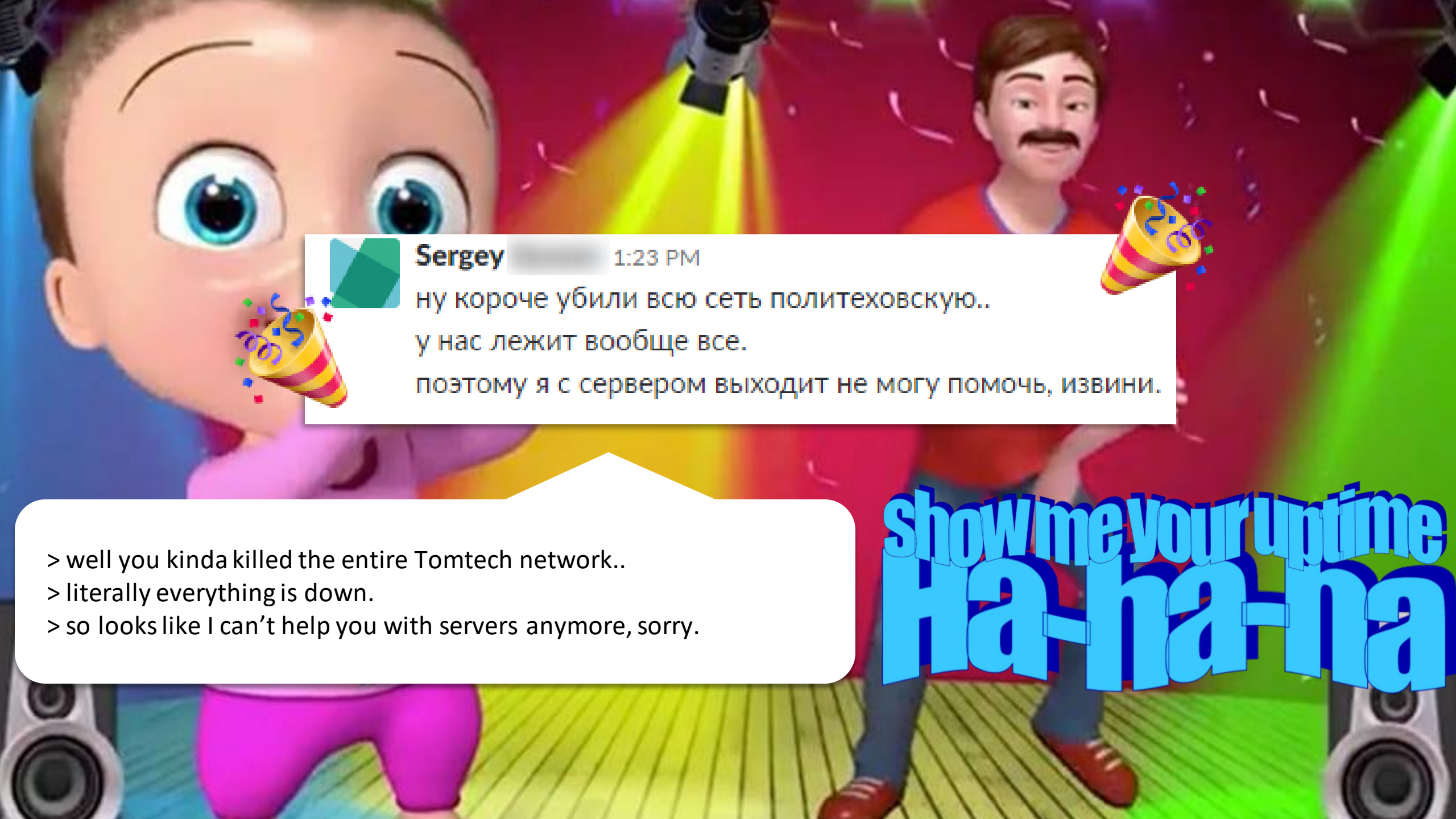
Stop! What about Internet scanning?



Almost same time
Almost same place


You should scan all Internet using
masscan

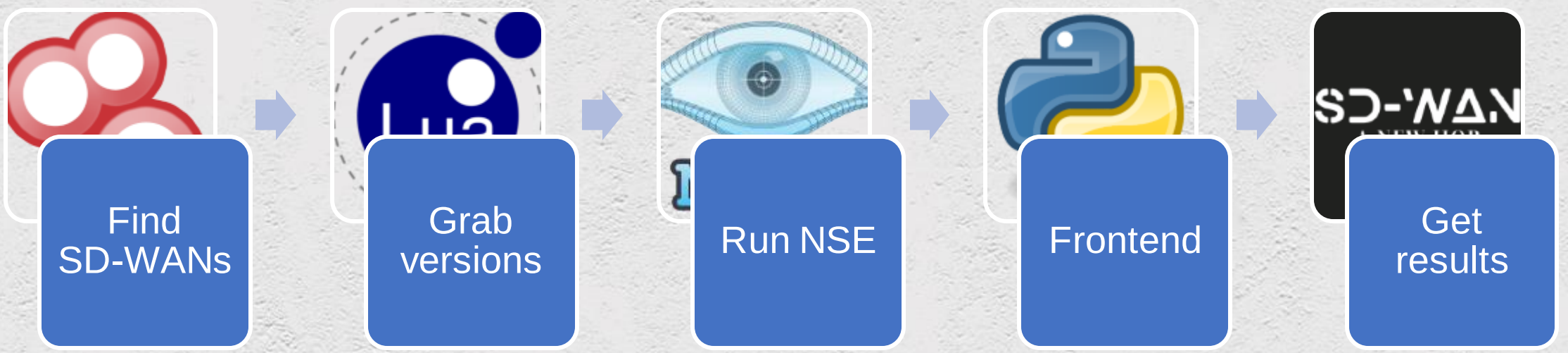
- Johny, Johny?
- Yes, papa
- Scanning Internet?
- No, papa
- Telling lies?
- No, papa


Sergey [redacted] 1:23 PM
ну короче убили всю сеть политеховскую..
у нас лежит вообще все.
поэтому я с сервером выходит не могу помочь, извини.
> well you kinda killed the entire Tomtech network..
> literally everything is down.
> so looks like I can’t help you with servers anymore, sorry.
Show me your uptime
Ha-ha-ha

And now back

SD-WAN Harvester

SD-WAN Harvester Workflow



ZERO NIGHTS 2018

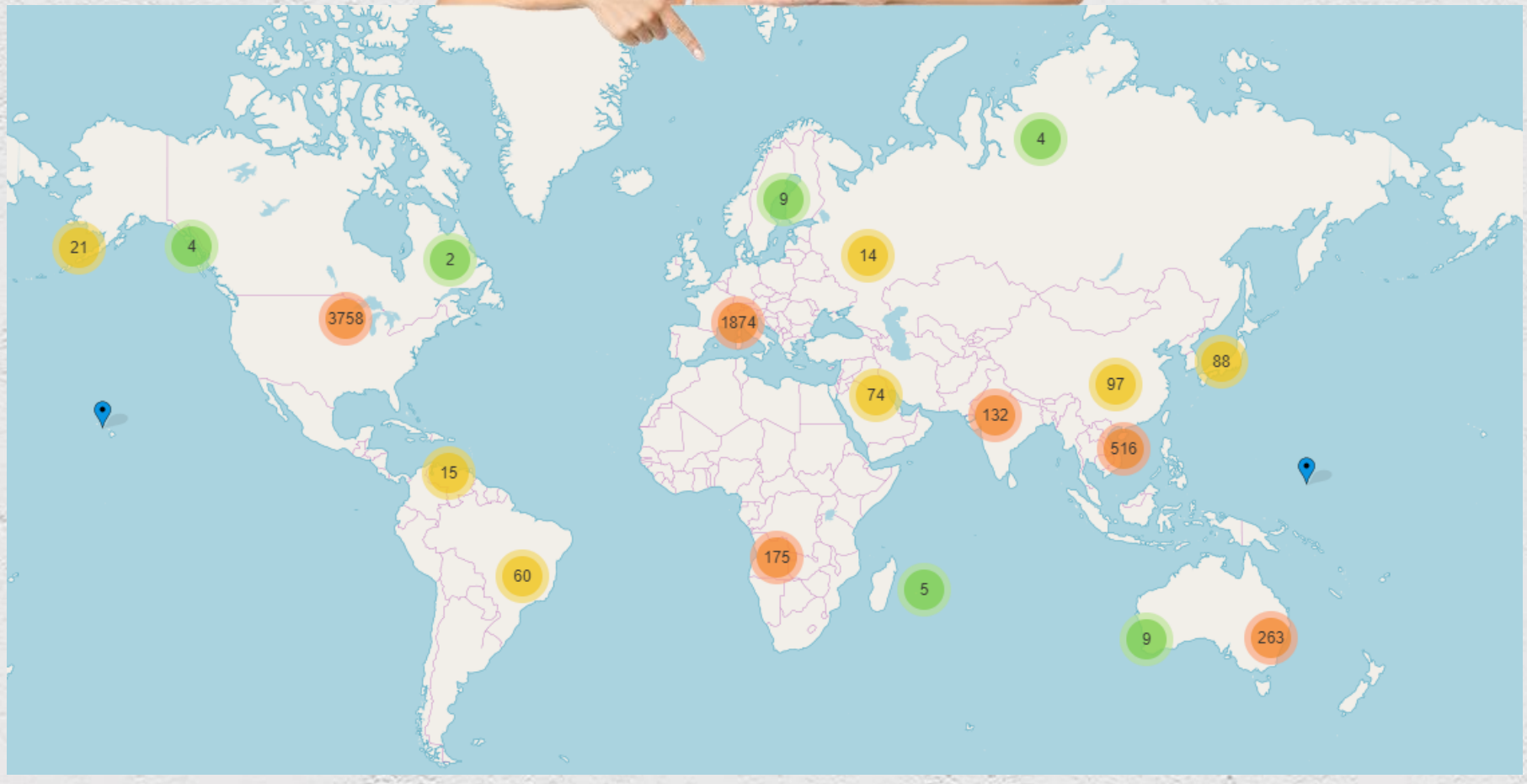
2^3 EDITION

Results

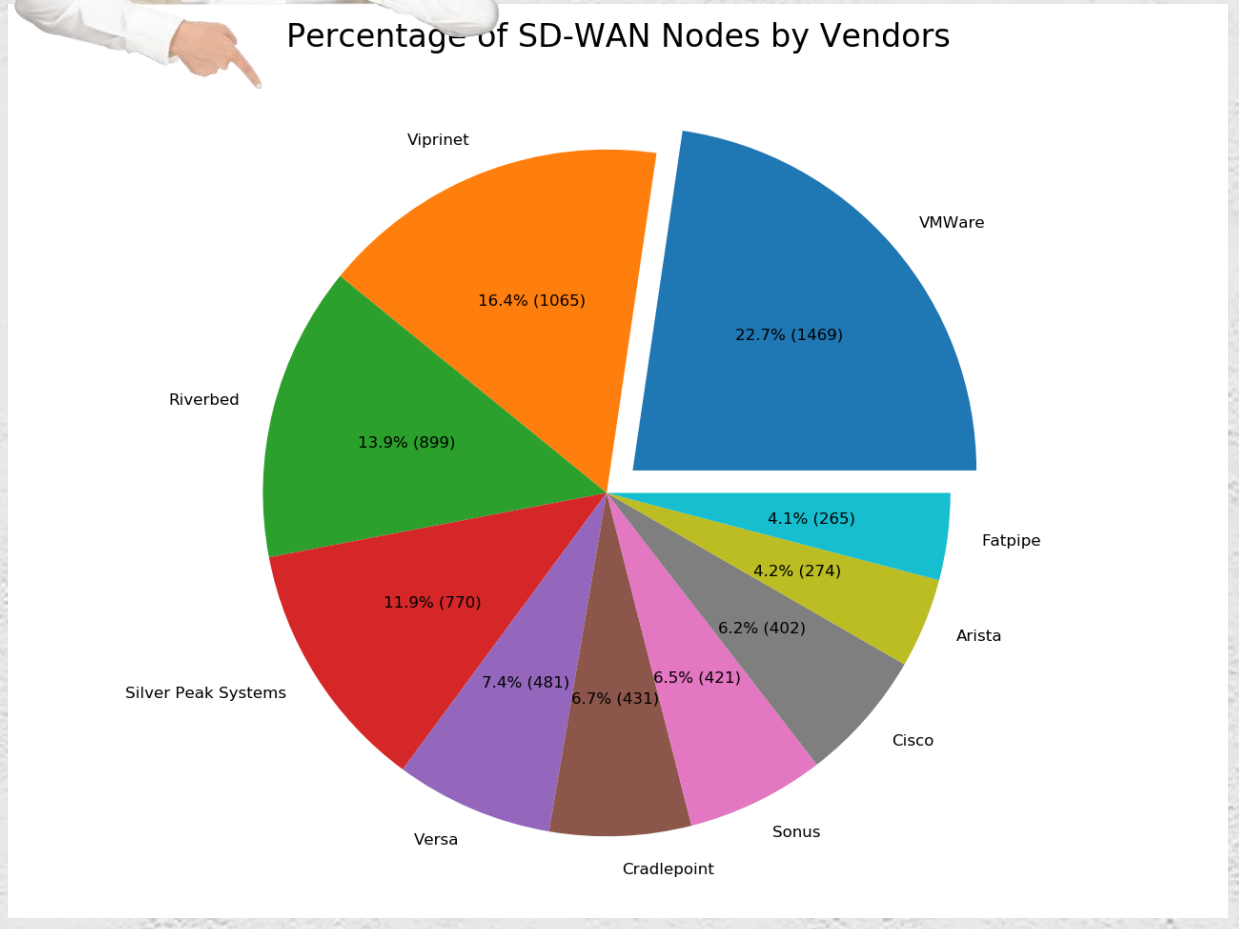
ZERO NIGHTS 2018

2^3 EDITION

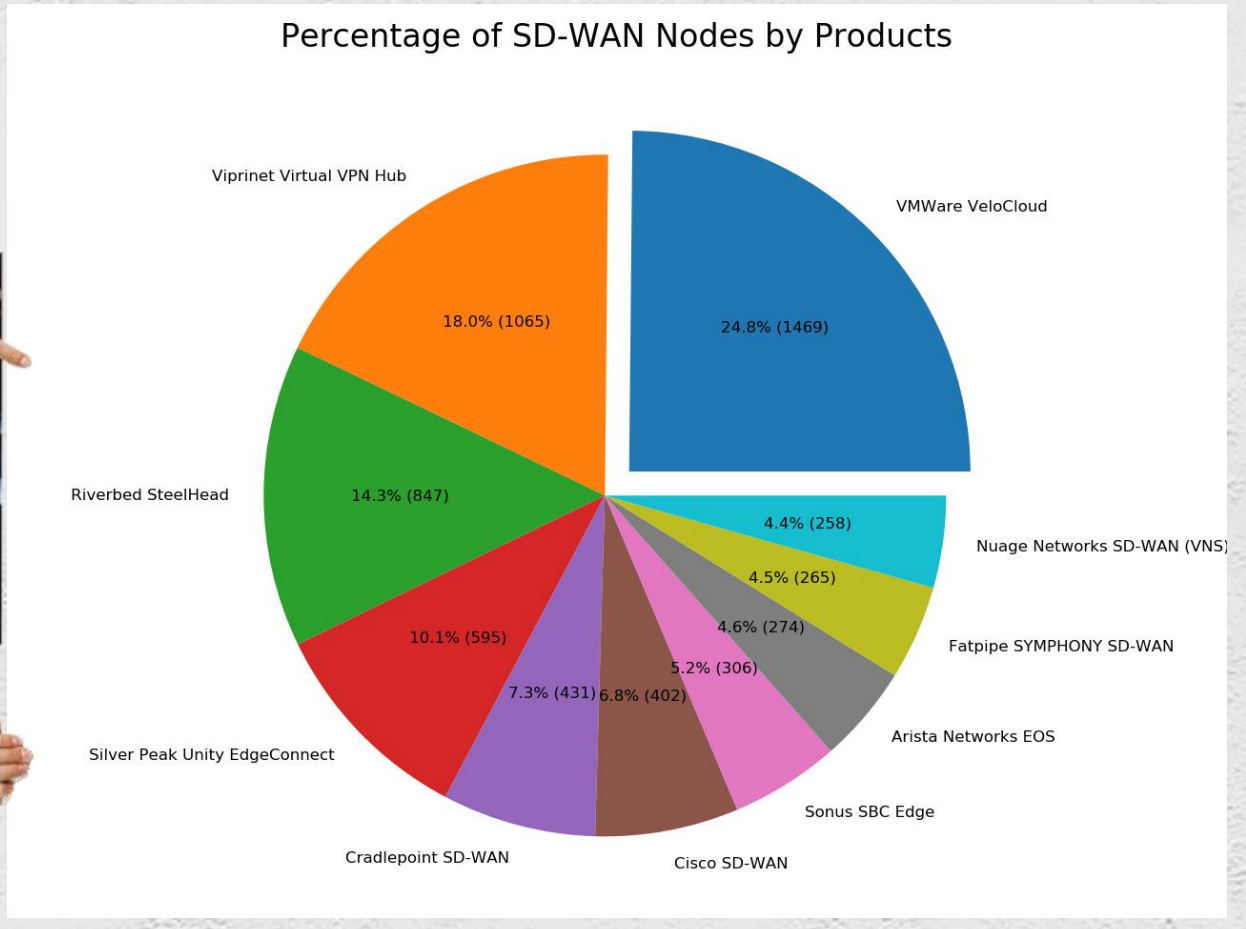
SD-WAN Map



Top of founded SD-WAN Vendors

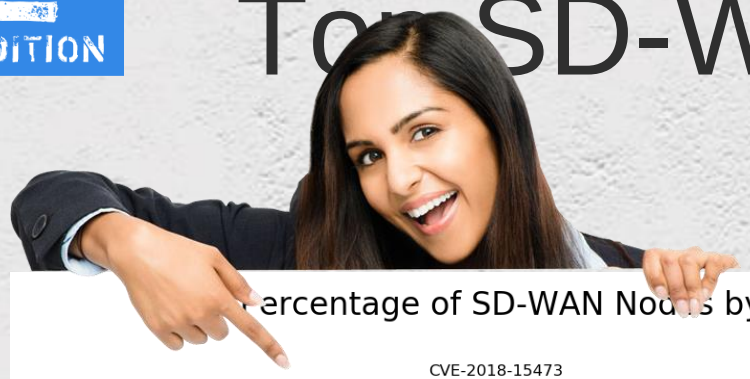


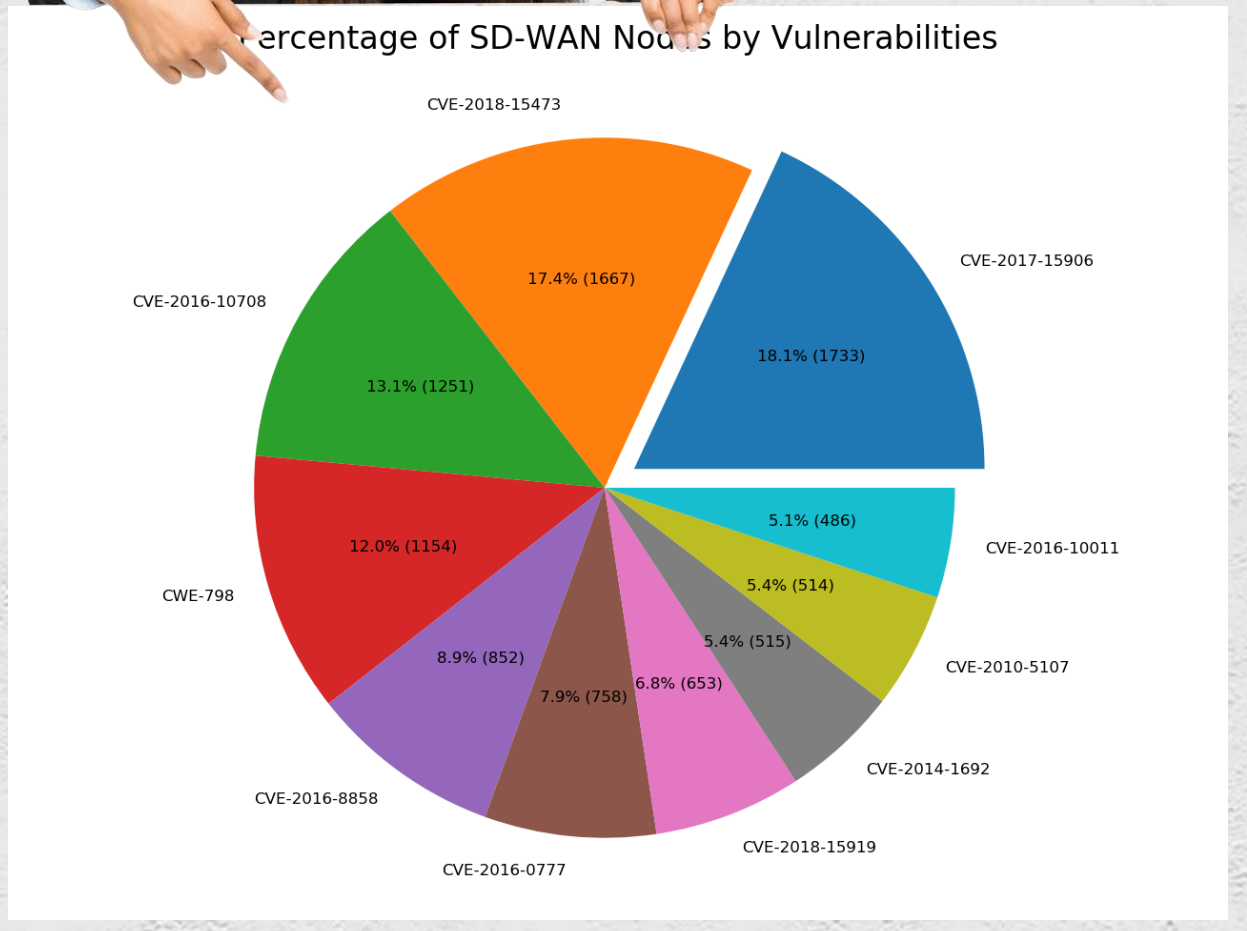
Top of founded SD-WAN Solutions



2^3 EDITION

Top SD-WAN Vulnerabilities



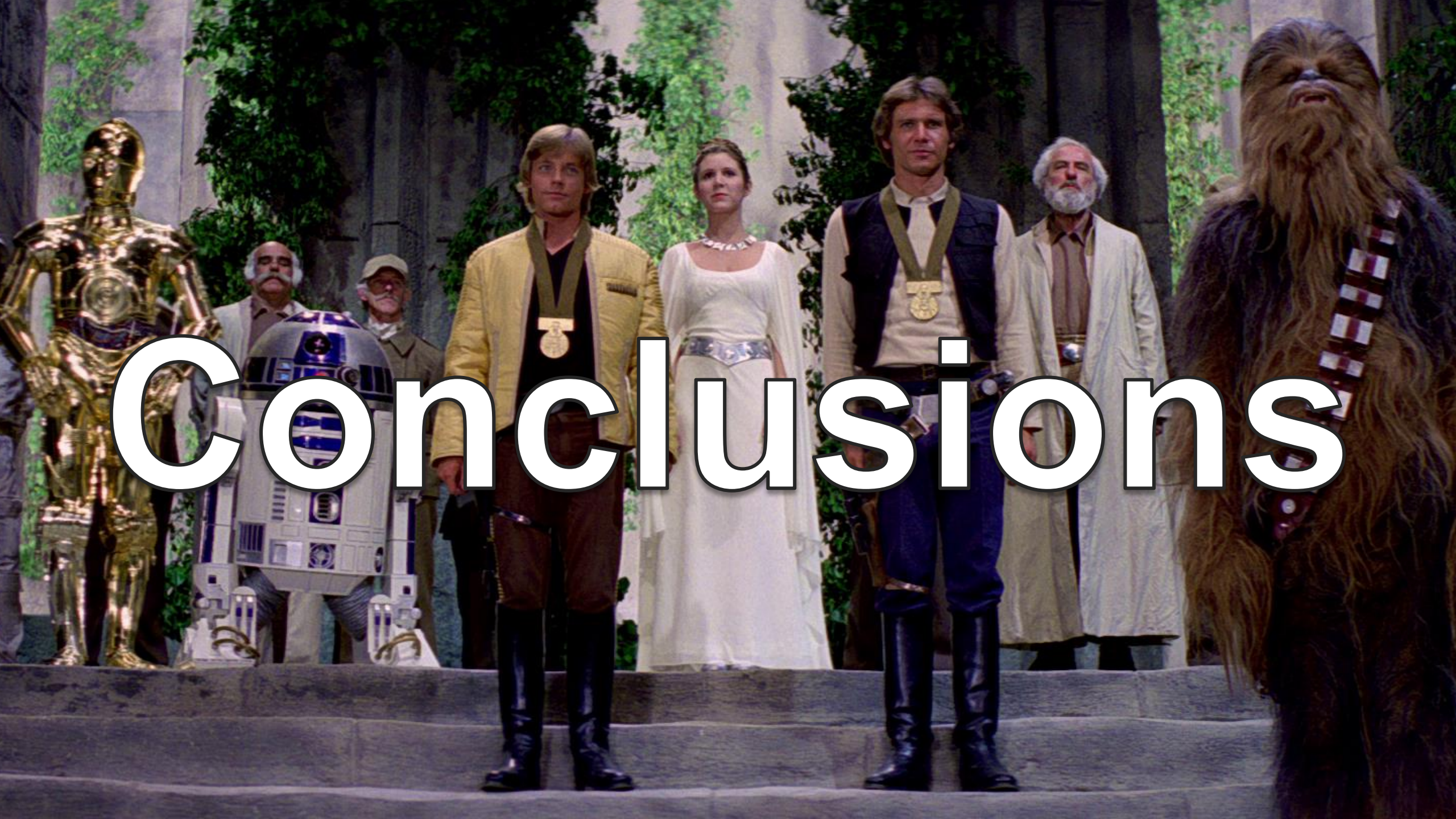


Harvester Charts

But seriously, harvester can build next pie charts by:

- vulnerabilities
- vendors
- products
- countries
- continents

https://github.com/sdnewhop/sdwan-harvester/tree/master/samples


Conclusions

2^3 EDITION

Conclusions

- Many different vendors and related products have been found
- Most products are susceptible to version leakage
- More often products are leaky and vulnerable

SD-WAN New Hope

- Sergey Gordeychik
- Denis Kolegov
- Oleg Broslavsky
- Max Gorbunov
- Nikita Oleksov
- Nikolay Tkachenko
- Anton Nikolaev

- SD-WAN Internet Census
- SD-WAN Harvester
- SD-WAN Infiltrator
- SD-WAN Threat Landscape

https://github.com/sdnewhop/

THANKS FOR ATTENTION

@dnkolegov

@yalegko

@manmoleculo