

(S//SI//REL) **What Your  
Mother Never Told  
You About SIGDEV  
Analysis**

**SSG21 Net Pursuit  
Network Analysis Center**

**Derived From: NSA/CSSM 1-52  
Dated: 20070108  
Declassify On: 20370401**

# (U//FOUO) What have I learned in my first two years in SIGDEV

- ⇒ (U//FOUO) Important to understand the data that you are searching against
- ⇒ (S//SI//REL) Important to understand the hidden treasures and nuances in various SIGDEV tools
- ⇒ (U//FOUO) Nothing is 100%: there are always exceptions to the tools and the rules
- ⇒ (S//SI//REL) Took a network view of VPNs

# (TS//SI//REL) What Makes SIGDEV Analysis Challenging?

- ⇒ (U//FOUO) Requires knowledge of.....
  - ⇒ (S//SI//REL) Access and collection
  - ⇒ (S//SI//REL) Network protocols
  - ⇒ (S//SI//REL) Routing
  - ⇒ (TS//SI//REL) Encryption

# (U//FOUO) Challenges etc....

(TS//SI//REL) Technical jargon and abbreviations

- ⇒ IPSEC
- ⇒ IKE
- ⇒ MPLS
- ⇒ PSK
- ⇒ PPTP
- ⇒ L2TP
- ⇒ GRE
- ⇒ Cisco commands

# (TS//SI//REL) Challenges etc....

## (S//SI//REL) Tools

- ⇒ How to use them
- ⇒ Knowing that they exist
- ⇒ Multiple query languages
- ⇒ SQL for TOYGRIPPE
- ⇒ Oracle Text Query in DISCOROUTE
- ⇒ Quantity

# (U//FOUO) Tools

- ⇒ DISCOROUTE
- ⇒ BLACKPEARL
- ⇒ TOYGRIPPE
- ⇒ GNETWORK GNOME
- ⇒ NKB & RONIN
- ⇒ XKEYSCORE
- ⇒ TREASUREMAP
- ⇒ RENOIR
- ⇒ ....and more....

# (S//SI//REL) Building Network

BLACKPEARL BLACKPEARL  
BLACKPEARL

# Knowledge

TOYGRIPPE TOYGRIPPE  
TOYGRIPPE

XKEYSCORE XKEYSCORE  
XKEYSCORE

Maximize the overlap of the tools for  
success

(S//SI//REL)

# DISCOROUTE

NAC's router configuration database



# (U//FOUO) DISCORROUTE

- ⇒ (C) NAC project to acquire, parse, database and display configuration files from network devices
- ⇒ (C) Allows analysts to mine device configs for SIGDEV discovery

Router configs are a rich source  
of  
network and VPN information



# (S//SI//REL) DISCOROUTE

## Methodology

- ⇒ (S//SI//REL) All IPs are important because they all belong to a device and they all have a purpose in the network
- ⇒ (S//SI//REL) Search for
  - ⇒ Endpoint IPs
  - ⇒ Loopback IPs
  - ⇒ Opposite end of a point-to-point connection
  - ⇒ IPs found in pings and telnets
- ⇒ (S//SI//REL) Make note of the source and destination IPs of the config

# (U//FOUO) DISCOROUTE Searches

- ⇒ (U//FOUO) Country
- ⇒ (U//FOUO) IP Search
- ⇒ (U//FOUO) Text Query
- ⇒ (TS//SI//REL) Manifest Tag Selection
  - ⇒ K - Crypto Keys
  - ⇒ H - TAO Pop
  - ⇒ M - Multihop
- ⇒ (S//SI//REL) VPN report



# (S//SI//REL) DISCOROUTE: Country Search


- ⇒ (S//SI//REL) IPGeo lookup on every IP address that is parsed
- ⇒ (S//SI//REL) Configs with only private IPs will not show up in the results of a country search

# (S//SI//REL) DISCOROUTE: Searching for IP

- ## Addresses
- ⇒ (S//SI//REL) Text query IP search
    - ⇒ searches through the payload
    - ⇒ If you only search using this field, then you will miss
      - ⇒ configs that have your IPs of interest as the source and destination address
      - ⇒ configs where your IP falls within the range of the interface mask
  - ⇒ (S//SI//REL) IP address field search
    - ⇒ searches through the parsed file
    - ⇒ If you only search using this field, then you will miss configs with your IPs of interest in pings, telnets, arp commands

# (S//SI//REL) DISCOROUTE Search 1Feb to 13 Apr:

- ⇒ (S//SI//REL) T [REDACTED] in the payload
  - ⇒ 3 results
- ⇒ (S//SI//REL) IP Address Search: searching for the IP in the parsed file
  - ⇒ Exact IP search
  - ⇒ De-duped by most recent
  - ⇒ 28 results (27 had [REDACTED] as the source IP)
- ⇒ (S//SI//REL) Somalia Country search: 66 results (12 of those had a source IP of [REDACTED])
- ⇒ (S//SI//REL) Difference: IP was the source IP for configs more times than it occurred in the payload data



(S//SI//REL) Why fewer configs for  
[REDACTED] in the country  
search?

- ⇒ (S//SI//REL) 12 as opposed to 27
- ⇒ (S//SI//REL) Geo location for [REDACTED] was Hong Kong for a period of time
- ⇒ (S//SI//REL) Geo is assigned to router configs at the time of ingest and not changed if the IP location is corrected

# (S//SI//REL) Data Found in a Text Query: Inner Network IPs in a Huawei Config

<LNS>dis firew se t  
04:19:05 2011/06/18  
Current total sessions : 19  
udp VPN: public -> public

[REDACTED]

Inner IPs

Press CTRL+K to abort  
Connected to [REDACTED] ...



# (S//SI//REL) DISCORROUTE

## Manifest Tag

- ⇒ (TS//SI//REL) H - TAO has a presence on the router
- ⇒ (S//SI//REL) M - multihop router. The admin telnetted into a router and then telnetted again to another device. Potential goldmine of information about your network, but be careful when looking through them to make sure you are associating an IP with the correct device.
- ⇒ (TS//SI//REL) K - crypto keys

# (S//SI//REL) VPNs in Router Configs

- ⇒ (TS//SI//REL) DISCORROUTE sets manifest tags to 'K' for configs with crypto information
- ⇒ (S//SI//REL) Separate parsers developed for each vendor to pull out the endpoints and the pre-shared keys
  - ⇒ Cisco
  - ⇒ Huawei
  - ⇒ Juniper

# (S//SI//REL) VPN Information in a Cisco

(S//SI//REL) Endpoint **Config** and Description Fields  
crypto isakmp key **VpnsAreCool** address [REDACTED]

crypto map **VPNS-ROCK** 10 ipsec-isakmp  
set peer [REDACTED]

interface Tunnel1  
**description Tunnel TO theStars**  
bandwidth 512  
ip address [REDACTED]  
ip tcp adjust-mss 1350  
load-interval 30 keepalive 5 2  
tunnel source [REDACTED]  
tunnel destination [REDACTED]  
crypto map **VPNS-ROCK**



(S//SI//REL) VPN Information in a

(S//SI//REL) Netstrings: Usernames, SNMP Community & Domain Names

# Cisco Config

```
Username deb privilege 5 password 7  
082C495A0C1617
```

```
snmp-server community dancer RW 70
```

```
snmp-server community tangosnmp RW 60
```

```
ip domain name lifesabeach
```

# (S//SI//REL) VPN Information in a Huawei Config

```
# ike proposal 60 authentication-algorithm md5
# ike peer e ---- More ----.[42D].[42D]
exchange-mode aggressive pre-shared-key GoHokies
ike-proposal 60
undo version 2
local-id-type name
remote-name svn
remote-address [REDACTED]
remote-address authentication-address [REDACTED]
nat traversal
# ipsec proposal GoHokies
# ipsec policy helloworld 60 isakmp
security acl 3060
ike-peer proposal GoHokies
# interface Virtual-Template1 ---- More ----.[42D].[42D]
ip address [REDACTED]
remote address pool 1
# interface GigabitEthernet0/0/0
ip address [REDACTED]
# interface GigabitEthernet0/0/1
description GigabitEthernet0/0/1 Interface
ip address [REDACTED]
ipsec policy helloworld
```

# (S//SI//REL) VPN Information in a Juniper Config

```
set ike gateway "BadguyVPN" address [REDACTED] Main outgoing-interface "untrust" preshare
"xGe7YOYfNx3DNGsp4GCq+fgCdondsCBQtVwo/3YfCvbR7zJyDUewVD4=" proposal "pre-g2-3des-sha" "pre-g2-
3des-md5"
set ike gateway "BadguyVPN" cert peer-ca all
set ike gateway "BadguyVPN Backup" address [REDACTED] Main outgoing-interface "untrust" preshare
"YWZpKbUvNGQvCbsiXdCwv3pxRDnLEAxo9877SfjFLBgg9utCdSyYPPI=" proposal "pre-g2-3des-sha" "pre-g2-
3des-md5"
set ike gateway "To Mouse" address [REDACTED] Main outgoing-interface "untrust" preshare
"fn3VG5E1NI+amHsDeyChciqYVHnuTsbj4w==" proposal "pre-g2-3des-sha"
set ike respond-bad-spi 1
set vpn "BadguyVPN" gateway "BadguyVPN" no-replay tunnel idletime 0 proposal "nopfs-esp-3des-sha"
set vpn "BadguyVPN" monitor optimized rekey
set vpn "BadguyVPN" id 5 bind interface tunnel.3
set vpn "backup BadguyVPN" gateway "BadguyVPN Backup" no-replay tunnel idletime 0 proposal "nopfs-esp-
3des-sha" "nopfs-esp-3des-sha" "nopfs-esp-3des-sha" "nopfs-esp-3des-md5"
set vpn "backup BadguyVPN" monitor optimized rekey
set vpn "backup BadguyVPN" id 4 bind interface tunnel.1
set vpn "From Rat" gateway "To Mouse" no-replay tunnel idletime 0 proposal "nopfs-esp-des-md5"
set vpn "From Rat" monitor optimized rekey
set vpn "From Rat" id 6 bind interface tunnel.2
```

# (S//SI//REL) VPN Report Search Fields

- ⇒ (S//SI//REL) Some of the fields that you can search in...
  - ⇒ Country
  - ⇒ IP Address
  - ⇒ SIGAD/Case Notation
  - ⇒ Descriptions: crypto map and interface
  - ⇒ Netstrings: Username, Domain Name
  - ⇒ Pre-shared keys
  - ⇒ Device Hostname
  - ⇒ TAO Project Name

# (S//SI//REL) DISCORROUTE VPN Report

The screenshot shows the 'VPN Report Form' interface. It includes a navigation bar with 'Query', 'Reports', 'Network Mgmt Query', 'Wiki', and 'Feedback'. The main form is divided into several sections:

- Date:** Contains 'Start Date' (2012-03-14 00:00:00) and 'End Date' (2012-04-13 23:59:59). Below are radio buttons for 'DOI', 'Load Date', and 'Entire Database'.
- IP Address:** Includes an 'IP Address' input field with a '(1.2.3.4)' hint and checkboxes for 'Tunnel Source', 'Tunnel Dest', 'Interface', 'VPN Source', and 'VPN Remote'.
- Other Fields:** Includes 'Pre-Shared Keys', 'Snmp Community', 'Interface Descr', 'Crypto Descr', 'Username', and 'Domain Name'.
- Form Fields:** 'Hostname', 'SIGAD', 'Case', 'Country', 'TAO Project Name', and 'Session ID'.
- Buttons:** 'Generate Report', 'Generate Report in New Window', and 'Clear Panel'.

Annotations on the screenshot include:

- 'Click to edit Master text styles' pointing to the top navigation bar.
- 'Second level' pointing to the 'VPN Report Form' header.
- 'Third level' pointing to the 'Date' section.
- 'Fourth level' pointing to the 'Start Date' field.
- 'Fifth level' pointing to the 'DOI' radio button.

At the bottom, there is a footer with the following text:

Powered by the SIGDEY Lab  
 Version Number: 2.17 **New!**  
 Last Modified Date: March 28, 2012  
 Last Reviewed Date: March 28, 2012  
 Content Steward: [Redacted]  
 Page Publisher: [Redacted]



# (S//SI//REL) VPN Report

Network Knowledge Base **DiscoRoute**

Query **Reports** New! Network Mgmt Query Wiki Feedback

DiscoRoute Reports

VPN Report Form

Query Results

Session ID: 1332289408998

Hostname	Vendor	Sigad	Case Notation	Collection Source	Country	TAO Project	TAO Pop
IBL_Baghdad_Router	cisco	USJ-759A	E9BDJ00000M0000	XKeyscore	LB		No

Interfaces

Interface ID	IP Address	Network Mask	Description
Loopback0		255.255.255.255	voice traffic
FastEthernet0/0		255.255.255.240	Connected To ASA/Firewall
FastEthernet0/1		255.255.255.248	Connected To 2MB DSL
Serial0/1/0		255.255.255.240	Connected To DVB

Tunnels

ID	Source	Dest	Description
Tunnel1			Tunnel TO Beirut
Tunnel1			Tunnel TO Beirut
Tunnel1			Tunnel TO Beirut
Tunnel1			Tunnel TO Beirut

VPN Peers

ID	Router IP	Remote IP	VPN Type	PSKs	Description
Serial0/1/0			ipsec	IblBaghdad	
Tunnel1			ipsec	IblvoiceVpn	
Serial0/1/0			ipsec	IblBaghdad	
Tunnel1			ipsec	IblvoiceVpn	
Serial0/1/0			ipsec	IblBaghdad	
Tunnel1			ipsec	IblvoiceVpn	
Serial0/1/0			ipsec	IblBaghdad	
Tunnel1			ipsec	IblvoiceVpn	

# (S//SI//REL) VPN Report

## Hints

- ⇒ (TS//SI//REL) Use the VPN report as a start but not as the final answer for VPNs from a country or a SIGAD
- ⇒ (C) Query in different ways to make sure you get as much of the data as possible
- ⇒ (TS//SI//REL) Depending on your scenario you may want to start with a country search, an IP range or a descriptive term

VPN Peers Section contains the endpoint IPs for your VPN which can be entered into TOYGRIPPE

# (S//SI//REL) Description & Net Strings Searches

- ⇒ (S//SI//REL) Suppose you do a general VPN report query
  - ⇒ Search by country
  - ⇒ Search by SIGAD
- ⇒ (S//SI//REL) Find a VPN of interest
- ⇒ (S//SI//REL) Analyze the NetStrings and the description fields

# (S//SI//REL) NetStrings

## Examples

- ⇒ (S//SI//REL) Do a follow-on VPN report using a netstring specific to your network
  - ⇒ Snmp community string: pegasus
  - ⇒ Domain name: badguy.com
  - ⇒ Username
- ⇒ (S//SI//REL) Search ROYALNET
  - ⇒ Analytics to find other netstrings related to your target
  - ⇒ Analytics to find links likely to carry your target's communications

# (U//FOUO) BLACKPEARL

(S//SI//REL) NAC tool enabling automated DNI link and network characterization against survey collection across the SIGINT system



(S//SI//REL) **BLACKPEARL**

# Searches

- ⇒ (U//FOUO) General Query
- ⇒ (S//SI//REL) Customized reports
  - ⇒ VPN report
  - ⇒ DNI Access Essentials
  - ⇒ MPLS report
  - ⇒ Five Tuple Report

# (S//SI//REL) BLACKPEARL IP

## Searches

- ⇒ Endpoint IPs
- ⇒ Interface IPs
- ⇒ Loopback IPs
- ⇒ Source or destination IPs of the router config file
- ⇒ Inner network IPs
- ⇒ Analyze other IPs on the link



# (U//FOUO) BLACKPEARL

- ⇒ (S//SI//REL) Search 'All traffic' and include subchannels and tunnels if no results found under limited search
- ⇒ (S//SI//REL) If link is identified as MPLS then look at the other IPs in inner labels, if present
- ⇒ (S//SI//REL) Use BLACKPEARL for finding access and gathering information on your network



# (S//SI//REL) Search for Inner Tunneled IPs

- ⇒ (S//SI//REL) Query BLACKPEARL with an endpoint IP
  - ⇒ Find other tunneled IPs - inner network IPs that you can do follow on searches
- ⇒ (S//SI//REL) Query DISCOROUTE with any new IPs found
- ⇒ (TS//SI//REL) Success: Discovered information on Somalia's Hormuud network

# (TS//SI//REL) Example: Hormuud Network

- ⇒ (S//SI//REL) Began with loopback IPs from a spreadsheet
  - ⇒ [REDACTED]
- ⇒ (S//SI//REL) Found configs for 2 of the 12 loopbacks in a text query in DISCOROUTE
  - ⇒ [REDACTED] and [REDACTED] were in the payload but not parsed
- ⇒ (S//SI//REL) Took the IPs from those configs and found other configs, one with hostname 'LNS'

# (U) Example continued

- ⇒ (S//SI//REL) BLACKPEARL hit on LNS IP  
████████████████████
- ⇒ Inner IPs in L2TP tunnels
- ⇒ DR search for inner IPs from the L2TP tunnels and found more configs
- ⇒ (U//FOUO) Many of the configs were multi-hop
- ⇒ (S//SI//REL) Information compiled for TAO
  - ⇒ ~400 IPs for over 50 devices

## (S//SI//REL) BLACKPEARL Search:



L2TP tunnel ⇒ Click to enter text  
 Number of Five Tuples: 1 ⇒ Source Address = [redacted] and Destination Address = [redacted]  
 43 total packets

#	Source Address	Dest Address	Source Port	Dest Port	Next Protocol	% Packets	# Packets
1	[redacted]	[redacted]	22	4527	TCP (6)	100.0	43

L2TP tunnel ⇒ Third level  
 Number of Five Tuples: 6 ⇒ Source Address = [redacted] and Destination Address = [redacted]  
 58 total packets

#	Source Address	Dest Address	Source Port	Dest Port	Next Protocol	% Packets	# Packets
1	[redacted]	[redacted]	9101	53771	TCP (6)	67.2	39
2	[redacted]	[redacted]	6006	53779	TCP (6)	8.6	5
3	[redacted]	[redacted]	6000	53050	TCP (6)	6.0	1
4	[redacted]	[redacted]	6006	53783	TCP (6)	6.9	4
5	[redacted]	[redacted]	6000	53778	TCP (6)	5.2	3
6	[redacted]	[redacted]	6000	53782	TCP (6)	5.2	3

L2TP tunnel ⇒ Second level  
 Number of Five Tuples: 2 ⇒ Source Address = [redacted] and Destination Address = [redacted]  
 24 total packets

#	Source Address	Dest Address	Source Port	Dest Port	Next Protocol	% Packets	# Packets
1	[redacted]	[redacted]	23	3078	TCP (6)	83.3	20
2	[redacted]	[redacted]	23	3080	TCP (6)	16.7	4

~~(S//SI//REL)~~ BLACKPEARL MPLS

6	7938	255	+ Tuple List (label stack 1046418, 7938):		
7	7211	255	+ Tuple List (label stack 1046418, 7211):		
8	6660	255	+ Tuple List (label stack 1046418, 6660):		
9	6306	255	- Tuple List (label stack 1046418, 6306):		
	#	Source Address	Dest Address	Protocol Number	Pkt Count
	1	[REDACTED]	[REDACTED]	SIPP-ESP (50)	1
	1 of 1				
10	7180	255	+ Tuple List (label stack 1046418, 7180):		
11	8120	255	+ Tuple List (label stack 1046418, 8120):		
12	6315	255	- Tuple List (label stack 1046418, 6315):		
	#	Source Address	Dest Address	Protocol Number	Pkt Count
	1	[REDACTED]	[REDACTED]	SIPP-ESP (50)	1
	2	[REDACTED]	[REDACTED]	SIPP-ESP (50)	6
	3	[REDACTED]	[REDACTED]	SIPP-ESP (50)	1
	4	[REDACTED]	[REDACTED]	SIPP-ESP (50)	1
	4 of 4				
13	6705	255	+ Tuple List (label stack 1046418, 6705):		

Find: 1046418    Next    Previous    Highlight all    Match case

# (U//FOUO) TOYGRIPPE

(S//SI//REL) VPN Metadata Repository

# (S//SI//REL) Building VPN Network Knowledge

- ⇒ (S//SI//REL) VPNs are part of a larger network
- ⇒ (S//SI//REL) Inner or tunneled IPs are a peek inside the target's network
- ⇒ (S//SI//REL) Beneficial to look beyond the endpoints of your VPN
- ⇒ (S//SI//REL) Combine information from as many SIGDEV databases as you can

# (U//FOUO) TOYGRIPPE

## Searches

- ⇒ (U//FOUO) Search 3 months at a time
- ⇒ (U//FOUO) Keep going back in time if no results found
- ⇒ (S//SI//REL) Take endpoint IPs found here and search in
  - ⇒ DISCOROUTE -- device information
  - ⇒ BLACKPEARL -- inner tunneled IPs
- ⇒ (S//SI//REL) Country report



# (U//FOUO) TOYGRIPPE

## Searches

- ⇒ (S//SI//REL) Make note of other connections to the IP of interest and search for them separately
- ⇒ (S//SI//REL) You might not find what you are looking for, but it still may be important
- ⇒ (S//SI//REL) Convert the target domain name to hex and search for it in the idData field
  - ⇒ badguy.com = 6261646775792e636f6d
  - ⇒ (idData LIKE '%6261646775792e636f6d')

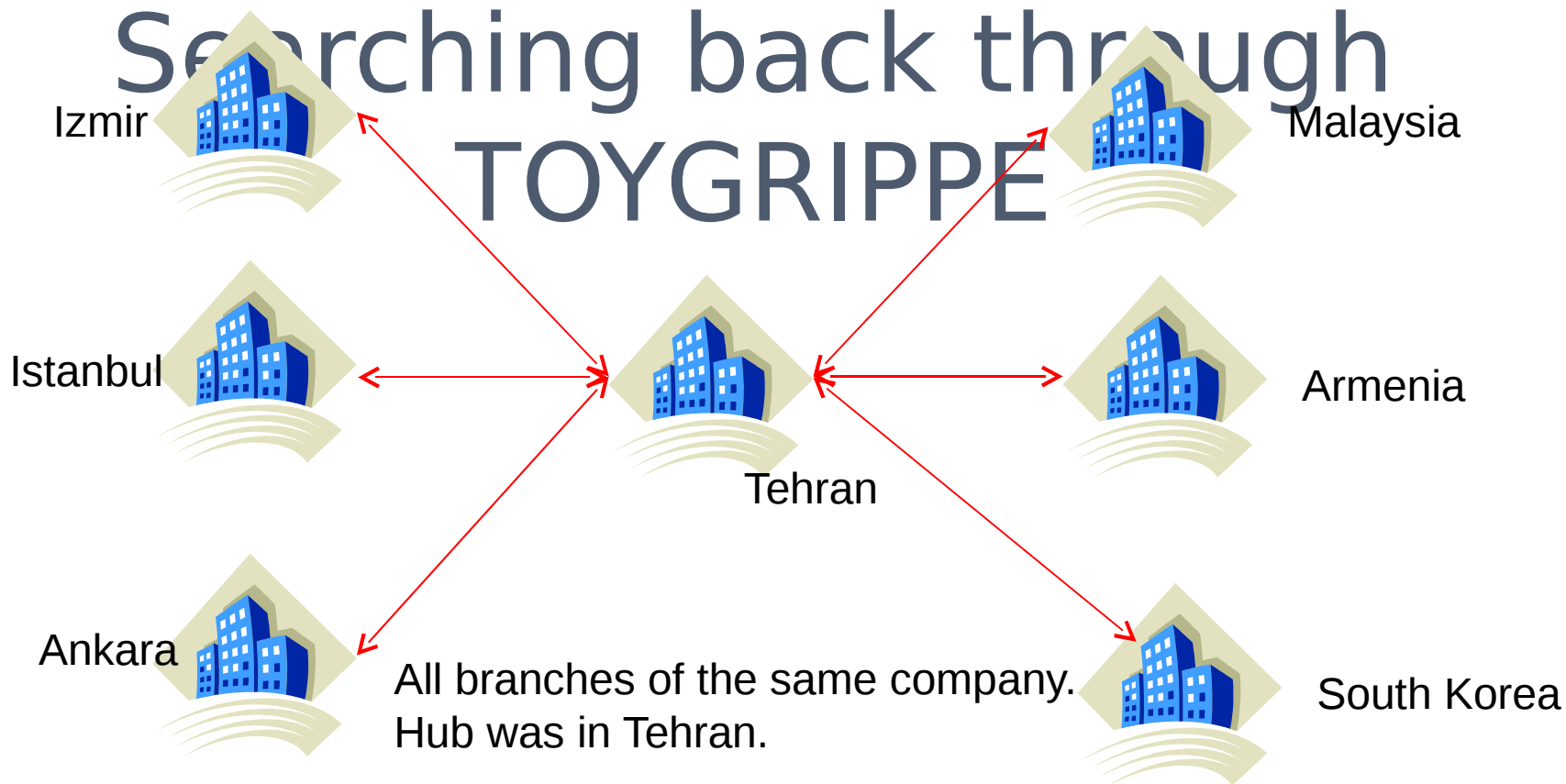
# (U//FOUO) Endpoint IP

## Search

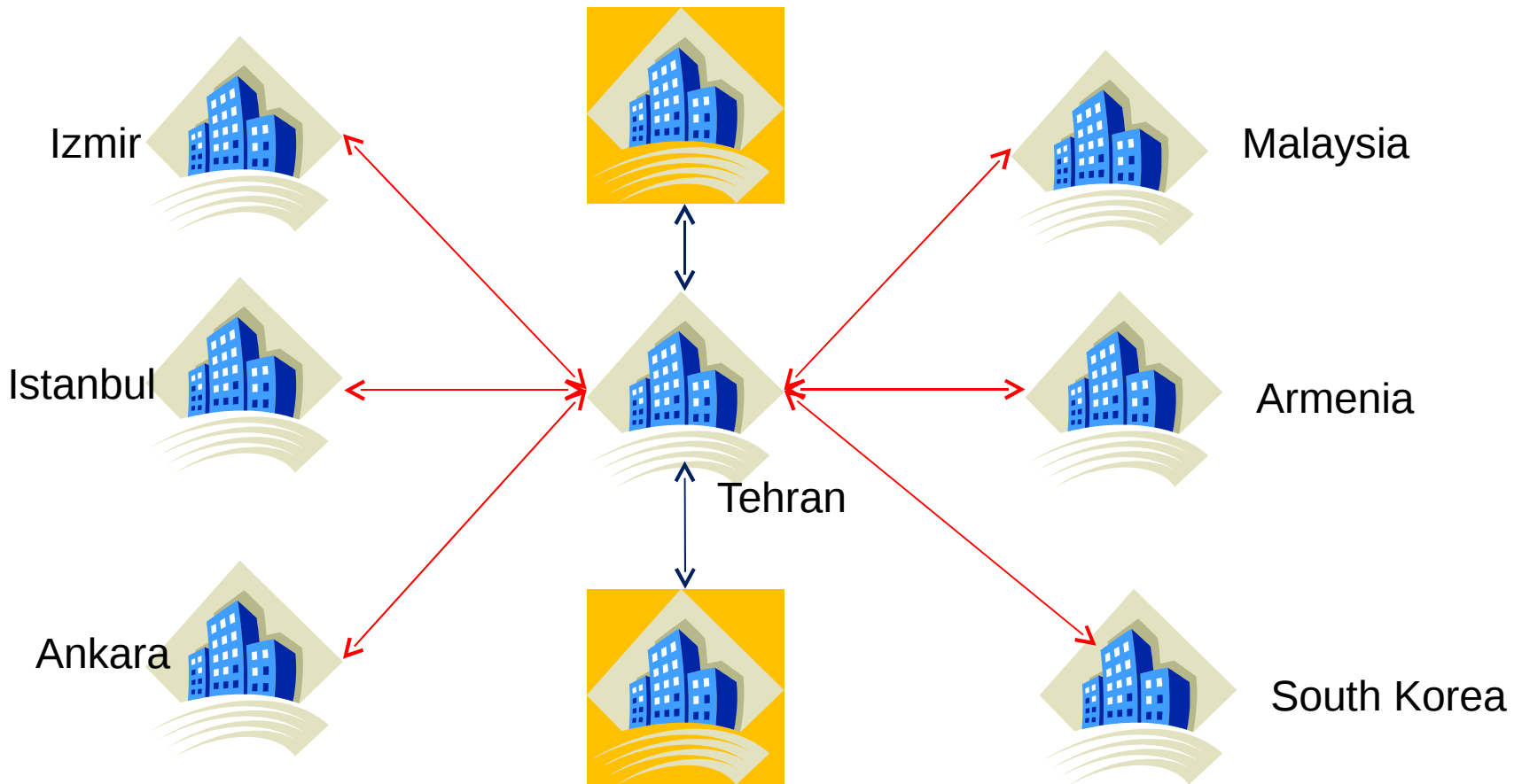
- ⇒ (TS//SI//REL) Query each IP in TOYGRIPPE separately
  - ⇒ Try to determine the importance of the connections
  - ⇒ Note other VPN connections: all IPs are important until proven otherwise
- ⇒ (TS//SI//REL) Success: Discovered Iranian corporate intranet

# (S//SI//REL) Building a VPN Intranet:

## Searching back through TOYGRIPPE



# (S//SI//REL) Finding Suspicious VPN Connections



(TS//SI//REL) Two connections outside the target company

# (S//SI//REL) Discovery of a Data Center

I had IP A, an endpoint IP from a router config...

And was looking for VPN connections to IP B, which I did not find...

....but in the process of looking, I found VPN connections to IP C in TOYGRIPPE....

# (S//SI//REL) Discovery of a Data Center

...and when I did a follow on search in TOYGRIPPE for IP C....

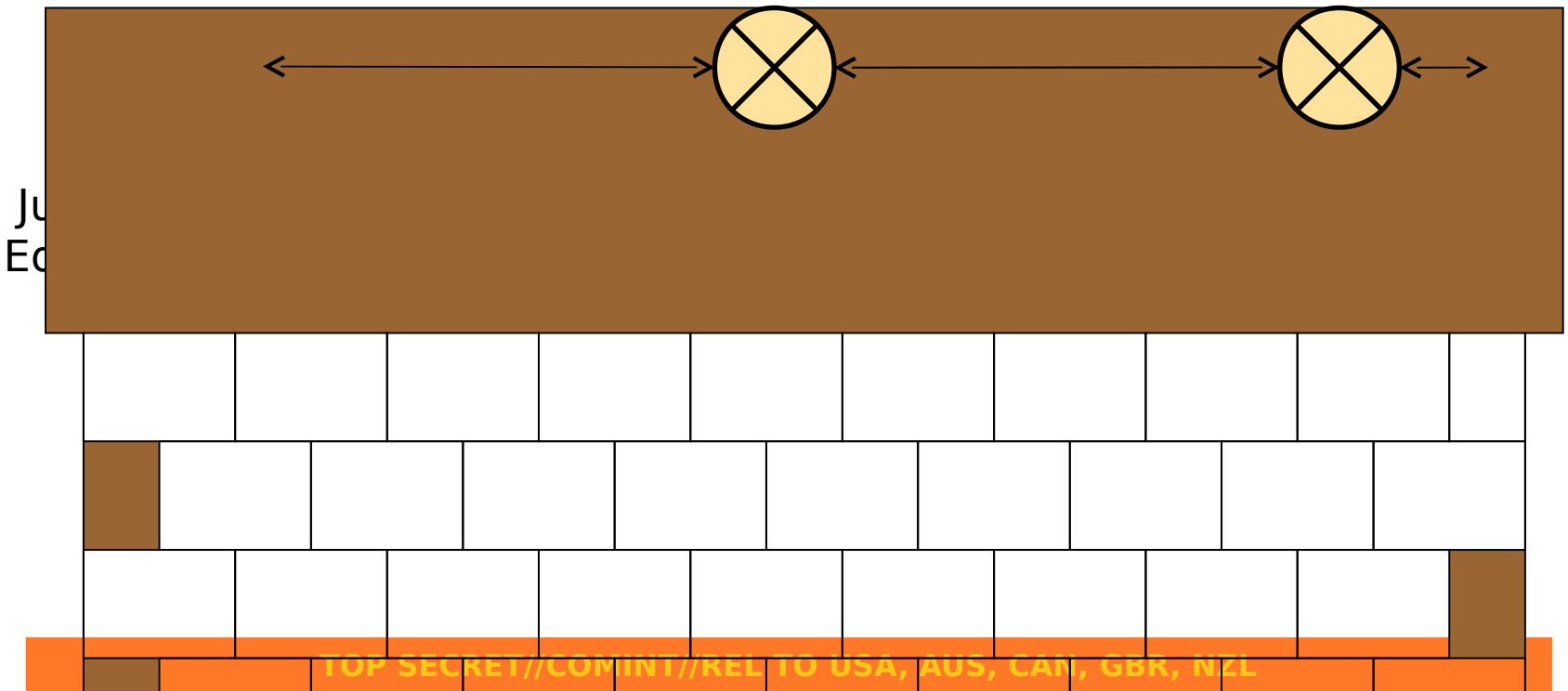
...I only found it only established VPN connections to IP A

Later discovered that IP C belonged to a data center in another country

# (S//SI//REL) Search for other end of the point-to-point connection

- ⇒ (S//SI//REL) What if you already have VPN endpoints from a GNOME report or a TOYGRIPPE search
- ⇒ (S//SI//REL) Search for that IP in the DISCOROUTE VPN report GUI - you don't find it
- ⇒ (S//SI//REL) Try to search for the other end of what would be a point-to-point connection in DISCOROUTE to find the customer edge router
- ⇒ (S//SI//REL) END GOAL: find more information about the network

# (S//SI//REL) Customer Edge Routers





# (U//FOUO) NKB and RONIN

(S//SI//REL) NKB is NSA's Network Knowledge Base delivering target communications' DNI and enrichment data

(S//SI//REL) RONIN is a device characterization database and one of the enrichments to NKB

# (U//FOUO) NKB

- ⇒ (S//SI//REL) RONIN data
  - ⇒ Server Analytics: VPN identified through application layer information in ASDF
  - ⇒ Wiki: VPN Metadata in ASDF
  - ⇒ VPN Analytics: endpoint in TOYGRIPPE
  - ⇒ Router Config: new descriptive information coming soon to include tunnel & VPN information for IPs
  - ⇒ Example: Kenya VPN IP [REDACTED]

# (TS//SI//REL) NKB Search for [REDACTED] : Device Details

The screenshot displays the NKB search interface with two panes: 'NKB: Home' and 'NKB: Results'. The 'NKB: Results' pane shows a list of device details for various interfaces and services. Below this list is a summary table with columns: DataSource, Service/Device, Type, Properties, Comments, and Last Seen.

DataSource	Service/Device	Type	Properties	Comments	Last Seen
RONIN	Hardware Interface:ROUTER	fast ethernet:IP	count=1 source=Router Config IP=[REDACTED]	[REDACTED] is serviced by interface "FastEthernet3" on the Cisco router named "onbo192", model "c870", with netmask [REDACTED] and description "--- To DSL provider". (Query DISCOROUTE)	2011-Aug-10
RONIN	Hardware Interface:ROUTER	fast ethernet:IP	count=5 source=Router Config IP=[REDACTED]	[REDACTED] is serviced by interface "FastEthernet4" on the Cisco router named "onbo192", model "c870", with netmask [REDACTED] and description "--- To DSL provider". (Query DISCOROUTE)	2011-Oct-12
RONIN	Hardware Interface:ROUTER	unknown:IP	count=1 source=Router Config IP=[REDACTED]	[REDACTED] is serviced by interface "FastEther.....N....." on the Cisco router named "onbo192", model "c870", with netmask [REDACTED] and description "--- To DSL provider". (Query DISCOROUTE)	2011-Oct-11
RONIN	Hardware Interface:ROUTER	unknown:IP	count=1 source=Router Config IP=[REDACTED]	[REDACTED] is serviced by interface "FastEther.....N.9.....net4" on the Cisco router named "onbo192", model "c870", with netmask [REDACTED] and description "--- To DSL provider". (Query DISCOROUTE)	2011-Oct-13
RONIN	Service Interface:ROUTER	IP ROUTE:Routed By	count=1 source=Router Config IP=[REDACTED]	[REDACTED] was seen in a static route with a subnet [REDACTED] on router "BP_AGG01".	2011-Sep-12
RONIN	Hardware Interface:ROUTER	fast ethernet:IP	count=1 source=Router Config IP=[REDACTED]	41.206.52.139/32 was found as the IP for interface "FastEthernet3" on the Cisco router named "onbo192"	
RONIN	Service Interface:SERVER	vpn:IKEv1	count=50 source=SERVER_ANALYTIC IP=[REDACTED]	vpn:IKEv1	
RONIN	Service Interface:SERVER	VPN:Cisco	count=195 source=VPN Analytic IP=[REDACTED]	VPN:Cisco	



# (U//FOUO) GNETWORK

## GNOME

(S//SI//REL) Tool used to extract and correlate information from a variety of NAC, SSG, SSO, NTOC and other metadata databases



# (S//SI//REL) Keep an Eye on the Entire Netblock

- ⇒ (S//SI//REL) Multiple VPNs for one target
  - ⇒ different purposes
  - ⇒ different clients



# (S//SI//REL) GNOME Task: Private IP VPNs

- ⇒ (S//SI//REL) Find a public IP associated with your private IP
  - ⇒ Loopback IP
  - ⇒ Another interface IP
- ⇒ (S//SI//REL) Use those for your GNOME report and look for your private IP on the same link
- ⇒ (S//SI//REL) Data presented in the VPN tab in GNOME report is limited



# (U//FOUO) Network Patterns...

# (S//SI//REL) IP Patterns

- ⇒ (S//SI//REL) Admins are people -- lean towards predictability in assignment of IPs to make their job easier
- ⇒ (S//SI//REL) IP or a combination of the octets could be an indication of:
  - ⇒ network provider
  - ⇒ location
  - ⇒ specific purpose in the network



# (S//SI//REL) Example #1: Private IP VPN

## Network Patterns

- ⇒ (S//SI//REL) Client side of the VPN: [REDACTED]
  - Second octet indicated the network provider
    - ⇒ 20 = network provider #1
    - ⇒ 21 = network provider #2
  - Second and third octet = country
    - ⇒ 20.30 and 21.30 were the same country but different providers
  - 40 = individual target entity in that country
  
- ⇒ (S//SI//REL) Server side of the VPN: [REDACTED]
  - Second octet indicated network provider
    - ⇒ 51 = network provider #1
    - ⇒ 52 = network provider #2

# (S//SI//REL) Example #2: Network Patterns

(S//SI//REL) Public IP VPN: [REDACTED].#

- ⇒ Third octet = country location of this IP (three possible)
- ⇒ Fourth octet = country location of the other side of the VPN connection

Analyzed the opposite side of this /24 and identified the country for 167 4th octet values (out of 209)  when this public IP connects to a private IP we know the country location of the private IP.

# (U//FOUO) Final Thoughts...

- ⇒ (S//SI//REL) Just because you don't get results doesn't mean the answer isn't there
  - ⇒ If you're looking for a connection from A to B and don't find it, then maybe you need to look for one from A to C to B
- ⇒ (S//SI//REL) Try the query a different way
  - ⇒ Widen the search either by wildcarding (if permitted) or by selecting a different drop-down option
  - ⇒ Enter information in a different field

# (U//FOUO) Final Thoughts...

- ⇒ (S//SI//REL) All IPs are important until proven otherwise
  - ⇒ They all serve a purpose and belong to a device
  - ⇒ Make note of what you find even if you don't know at the time what it means
- ⇒ (S//SI//REL) Search for data even if results are unlikely
- ⇒ (S//SI//REL) Don't necessarily discard dated information

# (U//FOUO) Final Thoughts...

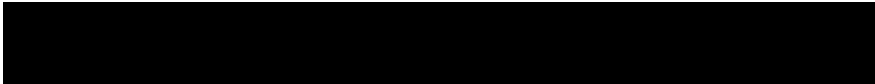
- ⇒ (U//FOUO) Understand the data that you are searching and what the fields in the GUI are searching for
- ⇒ (U//FOUO) Take an iterative approach: start searches wide, then narrow them down, then widen back out again
- ⇒ (S//SI//REL) Bounce between the different databases and use the tools for every aspect of your network analysis

## (S//SI//REL) VPN SIGDEV:

# Build the network knowledge...

- ⇒ (TS//SI//REL) Dig beyond paired collection, PSKs and persistence
- ⇒ (S//SI//REL) Discovery of the inner IPs of the VPN is possible in ways other than decryption
- ⇒ (S//SI//REL) Investigate device IPs
- ⇒ (U//FOUO) Look for patterns
- ⇒ (S//SI//REL) Discover the 'N' of your VPN

# (U//FOUO) Questions?

  
SSG21 Net Pursuit  
Network Analysis Center

**(S//SI//REL)**  
**Simplifying and**  
**Automating VPN**  
**SIGDEV**

SSG22

Network Analysis Center





(U//FOUO) **The Ultimate Goals**

- ⇒ (S//SI//REL) Integrate VPN information into mainstream analytic tools and knowledge bases.
- ⇒ (S//SI//REL) Give analysts the ability to discover, develop, and track known targets using VPNs.
- ⇒ (S//SI//REL) Give analysts the ability to discover new targets using VPNs.



# (U//FOUO) The Start . . .

- ⇒ (S//SI//REL) Develop new corporate VPN tool (DARKSUNRISE).
  - ⇒ Joint collaboration between CES and the NAC.
  - ⇒ Take advantage of cloud architecture.
  - ⇒ Strive to meet the needs of the entire VPN community.

# (U//FOUO) To The Cloud!

- (S//SI//REL) Data stored in MDR-2, the corporate metadata repository.
  - ⇒ Stores one year of DNI metadata.
  - ⇒ Enables filtering, aggregating, and transforming large datasets quickly.
  - ⇒ Manage high data volumes.
  - ⇒ Answer VPN questions efficiently and easily.

# (S//SI//REL) What are Some of the Needs of the VPN SIGDEV Community?

(S//SI//REL) Answer VPN SIGDEV questions quickly.

- ⇒ (S//SI//REL) Allow SIGDEVers to spend time analyzing data instead of gathering and processing the data first.
- ⇒ (S//SI//REL) Make VPN SIGDEV more widely understood by simplifying and automating the SIGDEV process.
- ⇒ (S//SI//REL) Robust Structure
  - ⇒ Allow for multiple VPN and network encryption protocols
  - ⇒ Allow for incorporation of new analytics.



(S//SI//REL) What are Some of the Questions?

- ⇒ (S//SI//REL) Basic Questions
  - ⇒ Is my target using a VPN?
  - ⇒ What are all of the VPNs from country BadGuyLand?
  - ⇒ Tell me all of the VPNs where domain = sita\*.
  - ⇒ Tell me all of the VPNs where the vendor ID = Cisco.



(S//SI//REL) What are Some of the  
Specialized Questions?

- ⇒ (S//SI//REL) Specialized Questions
  - ⇒ What are all of the VPNs that are bi-directional?
  - ⇒ What are all of the VPNs that are paired?
  - ⇒ Tell me all of the VPNs (and how many) that a particular VPN talks to (persistent hubs/centrality).
  - ⇒ What are all of the VPNs that are of interest (via Target Network Service)?
  - ⇒ What VPNs are associated to a router config?
  - ⇒ What are all of the VPNs that are persistent?
  - ⇒ For which VPNs do we have a PSK?



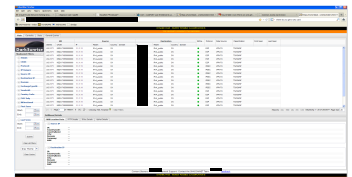
(S//SI//REL) What are Some of the  
Questions?

- ⇒ (S//SI//REL) Synthesizing Information
  - ⇒ What are all of the VPNs that are bi-directional, persistent, and of interest?
  - ⇒ What are all of the VPNs that are paired, persistent, and for which we have a PSK?
  - ⇒ What are all of the VPNs from country BadGuyLand that are paired, associated to a router config, and of interest?

# (U//FOUO) DARKSUNRISE

⇒ (U//FOUO) This is a prototype GUI.

⇒ (U//FOUO) Comingg Fall 2012





# (S//SI//REL) DARKSUNRISE

Mozilla Firefox

File Edit View History Bookmarks Tools Help

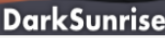
Virtual Private Network Working Group - ... x [Redacted] x RoyalNet "Prototype" x Free Form x BLACKPEARL - WikiInfo x [Redacted] x +

← [Redacted] ☆ Google

DNI Presenter - index TOYGRIPPE XKEYSCORE dsridge

DYNAMIC PAGE - HIGHEST POSSIBLE CLASSIFICATION IS  
TOP SECRET//COMINT//TK//NOFORN

Main Centrality Stats General Queries



**DarkSunrise**

Shadownet Filters

- + SIGAD:
- + CASN:
- + Protocol:
- + IP Ranges:
- + Source IP:
- + Destination IP:
- + Domain:
- + ExchangeTypeId:
- + VendorId:
- + Country Code:
- + FVEY Only
- + BiDirectional
- + First Seen:
 

Start:

End:
- + Last Seen:
 

Start:

End:

Submit

Clear all Filters

Gray Theme

Clear Cache

SRI		Source				Destination				BIDir...	Protocol	Data Source	Classification	First Seen	Last Seen
SIGAD	CASN	IP	Realm	Country	Domain	IP	Realm	Country	Domain						
DS-200B	PK1S011	[Redacted]	IPv4_public	SE	[Redacted]	[Redacted]	IPv4_public	PK	[Redacted]	●	IPSEC	VPN-TU	TS//SI//REL TO USA...		
DS-200B	PK1S011	[Redacted]	IPv4_public	RO	[Redacted]	[Redacted]	IPv4_public	PK	[Redacted]	●	IPSEC	VPN-TU	TS//SI//REL TO USA...		
DS-200B	PK1S011	[Redacted]	IPv4_public	RO	[Redacted]	[Redacted]	IPv4_public	PK	[Redacted]	●	IPSEC	VPN-TU	TS//SI//REL TO USA...		
DS-200B	PK1S011	[Redacted]	IPv4_public	TR	[Redacted]	[Redacted]	IPv4_public	PK	[Redacted]	●	IPSEC	VPN-TU	TS//SI//REL TO USA...		
DS-200B	PK1S011	[Redacted]	IPv4_public	TR	[Redacted]	[Redacted]	IPv4_public	PK	[Redacted]	●	IPSEC	VPN-TU	TS//SI//REL TO USA...		
DS-200B	PK1S011	[Redacted]	IPv4_public	AE	[Redacted]	[Redacted]	IPv4_public	AF	[Redacted]	●	IPSEC	VPN-TU	TS//SI//REL TO USA...		
DS-200B	PK1S011	[Redacted]	IPv4_public	AE	[Redacted]	[Redacted]	IPv4_public	PK	[Redacted]	●	IPSEC	VPN-TU	TS//SI//REL TO USA...		
DS-200B	PK1S011	[Redacted]	IPv4_public	AE	[Redacted]	[Redacted]	IPv4_public	PK	[Redacted]	●	IPSEC	VPN-TU	TS//SI//REL TO USA...		
DS-200B	PK1S011	[Redacted]	IPv4_public	AE	[Redacted]	[Redacted]	IPv4_public	PK	[Redacted]	●	IPSEC	VPN-TU	TS//SI//REL TO USA...		
DS-200B	PK1S011	[Redacted]	IPv4_public	CZ	[Redacted]	[Redacted]	IPv4_public	PK	[Redacted]	●	IPSEC	VPN-TU	TS//SI//REL TO USA...		
DS-200B	PK1S011	[Redacted]	IPv4_public	CZ	[Redacted]	[Redacted]	IPv4_public	PK	[Redacted]	●	IPSEC	VPN-TU	TS//SI//REL TO USA...		
DS-200B	PK1S011	[Redacted]	IPv4_public	AE	[Redacted]	[Redacted]	IPv4_public	AF	[Redacted]	●	IPSEC	VPN-TU	TS//SI//REL TO USA...		
DS-200B	PK1S011	[Redacted]	IPv4_public	TR	[Redacted]	[Redacted]	IPv4_public	PK	[Redacted]	●	IPSEC	VPN-TU	TS//SI//REL TO USA...		
DS-200B	PK1S011	[Redacted]	IPv4_public	TR	[Redacted]	[Redacted]	IPv4_public	PK	[Redacted]	●	IPSEC	VPN-TU	TS//SI//REL TO USA...		
DS-200B	PK1S011	[Redacted]	IPv4_public	NL	[Redacted]	[Redacted]	IPv4_public	PK	[Redacted]	●	IPSEC	VPN-TU	TS//SI//REL TO USA...		
DS-200B	PK1S011	[Redacted]	IPv4_public	NL	[Redacted]	[Redacted]	IPv4_public	PK	[Redacted]	●	IPSEC	VPN-TU	TS//SI//REL TO USA...		

Page 1 of 3 | Checking TNS... Finished! | Clear Filters

Reports: csv html xls ren ivml | Displaying 1 - 100 of 236 | Page Size 100

Drilldown/Details

NKB Location Data PPTP Details IPsec Details VipNet Details

Source IP

IP: [Redacted]  
CountryCode: RO  
CountryName: ROMANIA  
City: BUCHAREST  
Domain: ROMTELECOM.NET  
Company: ROMTELECOM DATA NETWORK  
ASN: 9050

Destination IP

IP: [Redacted]  
CountryCode: PK  
CountryName: PAKISTAN  
City: KARACHI  
Domain: TWI.COM  
Company: GRUPM  
ASN: 38193

Content Steward [Redacted] General Support: Contact the SHADOWNET Team [Redacted] [feedback](#)

DYNAMIC PAGE - HIGHEST POSSIBLE CLASSIFICATION IS  
TOP SECRET//COMINT//TK//NOFORN

# (TS//SI//REL) The NKB Location Data

## Drilldown

Mozilla Firefox

Virtual Private Network Working Group - ... JSigint: User [REDACTED] RoyalNet "Prototype" [REDACTED]

DYNAMIC PAGE - HIGHEST POSSIBLE CLASSIFICATION IS TOP SECRET//COMINT//TK//NOFORN

Main Centrality Stats General Queries

SRI		Source				Destination				BIDir...	Protocol	Data Source	Classification	First Seen	Last Seen
SIGAD	CASN	IP	Realm	Country	Domain	IP	Realm	Country	Domain						
DS-200B	PK1S011	[REDACTED]	IPv4_public	SE	[REDACTED]	[REDACTED]	IPv4_public	PK	[REDACTED]	●	IPSEC	VPN-TU	TS//SI//REL TO USA...		
DS-200B	PK1S011	[REDACTED]	IPv4_public	RO	[REDACTED]	[REDACTED]	IPv4_public	PK	[REDACTED]	●	IPSEC	VPN-TU	TS//SI//REL TO USA...		
DS-200B	PK1S011	[REDACTED]	IPv4_public	RO	[REDACTED]	[REDACTED]	IPv4_public	PK	[REDACTED]	●	IPSEC	VPN-TU	TS//SI//REL TO USA...		
DS-200B	PK1S011	[REDACTED]	IPv4_public	TR	[REDACTED]	[REDACTED]	IPv4_public	PK	[REDACTED]	●	IPSEC	VPN-TU	TS//SI//REL TO USA...		
DS-200B	PK1S011	[REDACTED]	IPv4_public	TR	[REDACTED]	[REDACTED]	IPv4_public	PK	[REDACTED]	●	IPSEC	VPN-TU	TS//SI//REL TO USA...		
DS-200B	PK1S011	[REDACTED]	IPv4_public	AE	[REDACTED]	[REDACTED]	IPv4_public	AF	[REDACTED]	●	IPSEC	VPN-TU	TS//SI//REL TO USA...		
DS-200B	PK1S011	[REDACTED]	IPv4_public	AE	[REDACTED]	[REDACTED]	IPv4_public	PK	[REDACTED]	●	IPSEC	VPN-TU	TS//SI//REL TO USA...		
DS-200B	PK1S011	[REDACTED]	IPv4_public	AE	[REDACTED]	[REDACTED]	IPv4_public	PK	[REDACTED]	●	IPSEC	VPN-TU	TS//SI//REL TO USA...		
DS-200B	PK1S011	[REDACTED]	IPv4_public	CZ	[REDACTED]	[REDACTED]	IPv4_public	PK	[REDACTED]	●	IPSEC	VPN-TU	TS//SI//REL TO USA...		
DS-200B	PK1S011	[REDACTED]	IPv4_public	CZ	[REDACTED]	[REDACTED]	IPv4_public	PK	[REDACTED]	●	IPSEC	VPN-TU	TS//SI//REL TO USA...		
DS-200B	PK1S011	[REDACTED]	IPv4_public	AE	[REDACTED]	[REDACTED]	IPv4_public	AF	[REDACTED]	●	IPSEC	VPN-TU	TS//SI//REL TO USA...		
DS-200B	PK1S011	[REDACTED]	IPv4_public	TR	[REDACTED]	[REDACTED]	IPv4_public	PK	[REDACTED]	●	IPSEC	VPN-TU	TS//SI//REL TO USA...		
DS-200B	PK1S011	[REDACTED]	IPv4_public	NL	[REDACTED]	[REDACTED]	IPv4_public	PK	[REDACTED]	●	IPSEC	VPN-TU	TS//SI//REL TO USA...		

Page 1 of 3 | Checking TNS. Finished! Finished! | Clear Filters | Reports: csv html xls ren ivml | Displaying 1 - 100 of 236 | Page Size 100

Drilldown/Details

NKB Location Data PPTP Details IPsec Details VipNet Details

Source IP

IP: [REDACTED]  
 CountryCode: RO  
 CountryName: ROMANIA  
 City: BUCHAREST  
 Domain: ROMTELECOM.NET  
 Company: ROMTELECOM DATA NETWORK  
 ASN: 9050

Destination IP

IP: [REDACTED]  
 CountryCode: PK  
 CountryName: PAKISTAN  
 City: KARACHI  
 Domain: TW1.COM  
 Company: GRUPM  
 ASN: 38193

Shadownet Filters

- SIGAD:
- CASN:
- Protocol:
- IP Ranges:
- Source IP:
- Destination IP:
- Domain:
- ExchangeTypeId:
- VendorId:
- Country Code:
- FVEY Only
- BiDirectional
- First Seen:

Submit

Clear all Filters

Gray Theme

Clear Cache

# (TS//SI//REL) The IPSec Details Drilldown

The screenshot displays the ShadowNet web interface. The top section shows a table with columns for SIGAD, SRI, Country, Source, Realm, IP, Destination, Protocol, and Data Source. A red circle highlights the 'IP' column in the table. Below the table, the 'Drilldown/Details' section provides specific information for the selected IP address, including:

- IPSec:** Encryption Alg ID: 7, Authentication Method ID: 3
- Encryption Algorithm:** AES-CBC
- Authentication Method:** RSA Signature
- Group ID:** Private Attr Type: 2
- ID Data:** Vendor Name: Vista/Longhorn (AuthIP supported)
- Vendor ID:** 314c44fa7a7f32d6748e5303395ae83
- VID Type:** Vendor
- Brand/Provider:** Microsoft
- Details/Version:** Vista/Longhorn (AuthIP supported)

The interface also includes a sidebar with various filters such as CASE, Protocol, IP Ranges, Source IP, Destination IP, Domain, Exchange Type ID, Vendor ID, Country Code, and FVEY Only. The bottom of the page contains a footer with contact information for the SHADOWNET Team.

# (TS//SI//REL) Automatic Identification of Bi-directional VPNs

The screenshot displays the SHADOWNET web interface within a Mozilla Firefox browser. The interface includes a navigation menu, a filter sidebar, a main data table, and a detailed view section. The table lists VPN connections with columns for Source and Destination details, including IP, Country, and Protocol. Red circles highlight specific entries in the table, and the detailed view below shows information for a selected source and destination IP.

SIGAD	CASN	IP	Realm	Country	Domain	IP	Realm	Country	Domain	BiDirectic	Protocol	Data Source
DS-200B	PK15011	[REDACTED]	IP4_public	US	[REDACTED]	[REDACTED]	IP4_public	PK	[REDACTED]	Green	IPSEC	VPN-TU
DS-200B	PK15011	[REDACTED]	IP4_public	US	[REDACTED]	[REDACTED]	IP4_public	PK	[REDACTED]	Green	IPSEC	VPN-TU
DS-200B	PK15011	[REDACTED]	IP4_public	SG	[REDACTED]	[REDACTED]	IP4_public	PK	[REDACTED]	Green	IPSEC	VPN-TU
DS-200B	PKS1011	[REDACTED]	IP4_public	PK	[REDACTED]	[REDACTED]	IP4_public	SG	[REDACTED]	Green	IPSEC	VPN-TU
DS-200B	PKS1011	[REDACTED]	IP4_public	PK	[REDACTED]	[REDACTED]	IP4_public	EG	[REDACTED]	Green	IPSEC	VPN-TU
DS-200B	PK15011	[REDACTED]	IP4_public	US	[REDACTED]	[REDACTED]	IP4_public	PK	[REDACTED]	Green	IPSEC	VPN-TU
DS-200B	PKS1011	[REDACTED]	IP4_public	PK	[REDACTED]	[REDACTED]	IP4_public	US	[REDACTED]	Green	IPSEC	VPN-TU
DS-200B	PKS1011	[REDACTED]	IP4_public	PK	[REDACTED]	[REDACTED]	IP4_public	RO	[REDACTED]	Green	IPSEC	VPN-TU
DS-200B	PK15011	[REDACTED]	IP4_public	RO	[REDACTED]	[REDACTED]	IP4_public	PK	[REDACTED]	Green	IPSEC	VPN-TU
DS-200B	PK15011	[REDACTED]	IP4_public	PK	[REDACTED]	[REDACTED]	IP4_public	RO	[REDACTED]	Green	IPSEC	VPN-TU
DS-200B	PK15011	[REDACTED]	IP4_public	RO	[REDACTED]	[REDACTED]	IP4_public	PK	[REDACTED]	Green	IPSEC	VPN-TU
DS-200B	PK15011	[REDACTED]	IP4_public	KZ	[REDACTED]	[REDACTED]	IP4_public	PK	[REDACTED]	Green	IPSEC	VPN-TU

**Source IP Details:**  
IP: [REDACTED]  
CountryCode: SG  
CountryName: SINGAPORE  
City: SINGAPORE  
Domain: HLAGCCPAC.COM  
Company: STARHUB INTERNET PTE LTD  
ASN: 9874

**Destination IP Details:**  
IP: [REDACTED]  
CountryCode: PK  
CountryName: PAKISTAN  
City: ISLAMABAD  
Domain: NAVATEL.PK  
Company: NICEONET BROADBAND (PVT) LTD.  
ASN: 23674

(TS//SI//REL)

# Automatic Identification of VPNs Of Interest

The screenshot shows the SHADOWNET interface with a table of VPN records. The table has columns for Source and Destination, including fields like SIGAD, CASN, IP, Realm, Country, and Domain. A red circle highlights the 'Group ID: Private Attr Type' field in the details view, which is currently empty.

Source		Destination			BIDirectic	Protocol	Data Source					
SIGAD	CASN	IP	Realm	Country	Domain	IP	Realm	Country	Domain			
DS-200B	PK15011	[REDACTED]	IPv4_public	RO	[REDACTED]	IPv4_public	PK	RO	[REDACTED]	●	IPSEC	VPN-TU
DS-200B	PKS1011	[REDACTED]	IPv4_public	PK	[REDACTED]	IPv4_public	RO	RO	[REDACTED]	●	IPSEC	VPN-TU
DS-200B	PK15011	[REDACTED]	IPv4_public	RO	[REDACTED]	IPv4_public	PK	RO	[REDACTED]	●	IPSEC	VPN-TU
DS-200B	PK15011	[REDACTED]	IPv4_public	KZ	[REDACTED]	IPv4_public	PK	PK	[REDACTED]	●	IPSEC	VPN-TU
DS-200B	PK15011	[REDACTED]	IPv4_public	ES	[REDACTED]	IPv4_public	PK	PK	[REDACTED]	●	IPSEC	VPN-TU
DS-200B	PKS1011	[REDACTED]	IPv4_public	PK	[REDACTED]	IPv4_public	US	US	[REDACTED]	●	IPSEC	VPN-TU
DS-200B	PKS1011	[REDACTED]	IPv4_public	PK	[REDACTED]	IPv4_public	US	US	[REDACTED]	●	IPSEC	VPN-TU
DS-200B	PKS1011	[REDACTED]	IPv4_public	PK	[REDACTED]	IPv4_public	US	US	[REDACTED]	●	IPSEC	VPN-TU
DS-200B	PKS1011	[REDACTED]	IPv4_public	PK	[REDACTED]	IPv4_public	US	US	[REDACTED]	●	IPSEC	VPN-TU
DS-200B	PKS1011	[REDACTED]	IPv4_public	GB	[REDACTED]	IPv4_public	PK	PK	[REDACTED]	●	IPSEC	VPN-TU
DS-200B	PKS1011	[REDACTED]	IPv4_public	PK	[REDACTED]	IPv4_public	GB	GB	[REDACTED]	●	IPSEC	VPN-TU

Details view for IPsec:

- Encryption Alg ID: 1
- ID Type: ---
- Authentication Method Id: 65005
- Encryption Algorithm: DES-CBC
- Private Attr Value: RSA Signature with Initiator
- Authentication Method: ---
- Group ID: Private Attr Type: ---
- ID Data: Vendor Name: ---

(S//SI//REL) The  icon means this record hits against the Target Network Service (TNS).

(TS//SI//REL)

# Automatic Identification of

# VPNs Of Interest

The screenshot displays the SHADOWNET application interface. On the left, there are filter sections for SIGAD, CASN, Protocol, IP Ranges, Source IP, Destination IP, Domain, Exchange Type ID, Vendor ID, Country Code, FVEY Only, BiDirectional, and Exchange Type Ids. The main table lists VPNs with columns: SRI, CASN, IP, Realm, Country, Domain, Realm, Destination, Country, Domain, BIDirectic, Protocol, and Data Source. A 'Target Networks' dialog box is open, showing search results for the IP 202.69.15.145 in the IPv4\_public realm. The results table includes columns for Target Indicator, Realm, Category, Classification, Agency, Priority, Description, and Source.

SRI	CASN	IP	Realm	Country	Domain	Realm	Destination	Country	Domain	BIDirectic	Protocol	Data Source
DS-200B	PK1S011	[Redacted]	IPv4_public	RO	[Redacted]	IPv4_public	PK	[Redacted]	[Redacted]	Green	IPSEC	VPN-TU
DS-200B	PKS1011	[Redacted]	IPv4_public	PK	[Redacted]	IPv4_public	RO	[Redacted]	[Redacted]	Green	IPSEC	VPN-TU
DS-200B	PK1S011	[Redacted]	IPv4_public	RO	[Redacted]	IPv4_public	PK	[Redacted]	[Redacted]	Green	IPSEC	VPN-TU
DS-200B	PK1S011	[Redacted]	IPv4_public	RO	[Redacted]	IPv4_public	PK	[Redacted]	[Redacted]	Green	IPSEC	VPN-TU
DS-200B	PK1S011	[Redacted]	IPv4_public	KZ	[Redacted]	IPv4_public	PK	[Redacted]	[Redacted]	Green	IPSEC	VPN-TU
DS-200B	PK1S011	[Redacted]	IPv4_public	ES	[Redacted]	IPv4_public	PK	[Redacted]	[Redacted]	Green	IPSEC	VPN-TU
DS-200B	PKS1011	[Redacted]	IPv4_public	PK	[Redacted]	IPv4_public	US	[Redacted]	[Redacted]	Yellow	IPSEC	VPN-TU
DS-200B	PKS1011	[Redacted]	IPv4_public	PK	[Redacted]	IPv4_public	US	[Redacted]	[Redacted]	Green	IPSEC	VPN-TU
DS-200B	PKS1011	[Redacted]	IPv4_public	PK	[Redacted]	IPv4_public	US	[Redacted]	[Redacted]	Green	IPSEC	VPN-TU
DS-200B	PKS1011	[Redacted]	IPv4_public	PK	[Redacted]	IPv4_public	PK	[Redacted]	[Redacted]	Green	IPSEC	VPN-TU

Target Indicator	Realm	Category	Classification	Agency	Priority	Description	Source
[Redacted]	IPv4_public	TARGET	TS//SI//REL TO USA, FVEY	NSA		Strateg PK Telenor VPN/vpn node	GNETWORKGNOME
[Redacted]	IPv4_public	TARGET	S//SI//REL TO USA, FVEY	NSA		Routine Telenor GPRS/Telenor's GPRS Subne	GNETWORKGNOME
[Redacted]	IPv4_public	TARGET	TOP SECRET//COMINT//REL TO USA	NSA	pri3	TELENOR PK; Karachi, PK; [TELENOR TU PROMOTION	

(S//SI//REL)

# The Centrality Tab

• (S//SI//REL) Find all VPNs that talk to a base VPN.

- ⇒ Discover persistent hubs.
- ⇒ Can continue chaining outwards.

(S//SI//REL)

# The Centrality Tab

The screenshot shows a Mozilla Firefox browser window with the following details:

- Browser Title:** Mozilla Firefox
- Address Bar:** DNI Presenter - Index
- Page Header:** DYNAMIC PAGE - HIGHEST POSSIBLE CLASSIFICATION IS TOP SECRET//COMINT//TK//NOFORN
- Navigation:** Main, Centrality, Stats, General Queries
- Centrality Filters:** IP Ranges (dropdown menu)
- Table:**

Address	Realm	Centrality
[REDACTED]	IPv4_public	2
- Overlaid Window:** Shows a detailed view of a centrality entry with columns for Name, Centrality, and Date. It lists three entries with values like 'IP\_PUBLIC', 'IP\_PUBLIC', and 'IP\_PUBLIC'.
- Page Footer:** Displaying 1 - 1 of 1 | Page Size: 30



(S//SI//REL) The Centrality Tab

The screenshot shows a Mozilla Firefox browser window with several tabs open. The active tab is titled 'Centrality'. The browser's address bar shows a URL starting with 'DNI Presenter - index'. The main content area of the browser displays a web application interface for 'Centrality'. The interface includes a 'Centrality Filters' section on the left with an 'IP Ranges' dropdown and a 'Submit' button. The main area shows a table with columns for 'Address', 'Realm', and 'Centrality'. The table contains one row with the value 'IPv4\_public' under 'Address' and '2' under 'Centrality'. Below this table, there are two smaller tables, each titled 'Parties of [redacted]'. The first table has columns for 'Room' and 'Centrality', with rows showing 'IPv4\_public' with values 3 and 3. The second table has columns for 'Address', 'Room', and 'Centrality', with rows showing 'IPv4\_public' with values 7, 3, and 2. The browser's status bar at the bottom indicates 'Displaying 1 - 1 of 1 | Page Size: 30'.

(S//SI//REL)

# The Centrality Tab

The screenshot shows a web application interface with a navigation menu on the left. The 'Centrality' tab is highlighted with a red circle. The main content area displays a table with columns for Address, Realm, and Centrality. Below this table, there are three smaller tables, each titled 'Partners of [redacted]', showing related data for specific IP addresses.

Address	Realm	Centrality
[redacted]	Pv4_public	2

Partners of [redacted]		
Address	Realm	Centrality
[redacted]	Pv4_public	3
[redacted]	Pv4_public	3

Partners of [redacted]		
Address	Realm	Centrality
[redacted]	Pv4_public	7
[redacted]	Pv4_public	3
[redacted]	Pv4_public	2

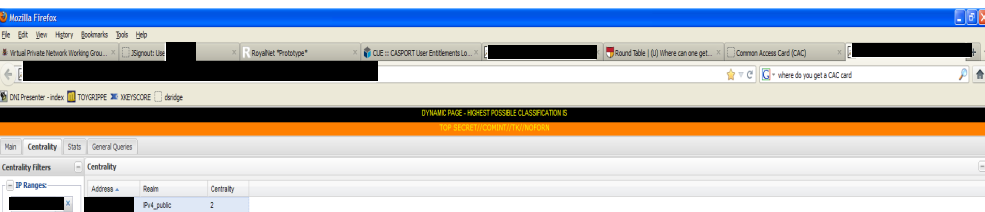
Partners of [redacted]		
Address	Realm	Centrality
[redacted]	Pv4_public	4
[redacted]	Pv4_public	3
[redacted]	Pv4_public	3
[redacted]	Pv4_public	3
[redacted]	Pv4_public	3
[redacted]	Pv4_public	3
[redacted]	Pv4_public	3
[redacted]	Pv4_public	1

Page 1 of 1 | Page Size: 30

Content Steward: [redacted] General Support: Contact the SHADOWNET Team [redacted] [feedback](#)

(S//SI//REL)

# The Centrality Tab



Address	Realm	Centrality
IPv4_public		2

Address	Realm	Centrality
[redacted]	IPv4_public	3
[redacted]	IPv4_public	3

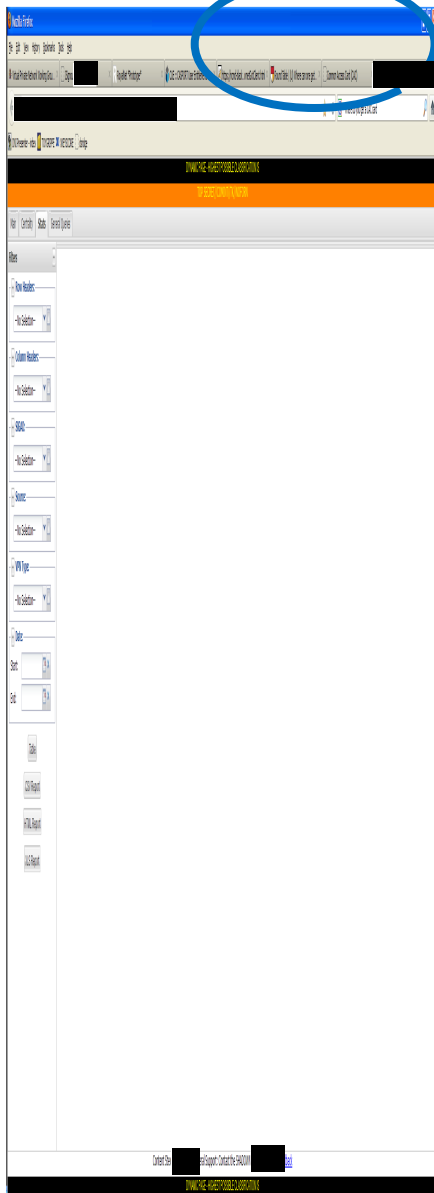
Address	Realm	Centrality
[redacted]	IPv4_public	7
[redacted]	IPv4_public	3
[redacted]	IPv4_public	2

Address	Realm	Centrality
[redacted]	IPv4_public	4
[redacted]	IPv4_public	3
[redacted]	IPv4_public	3
[redacted]	IPv4_public	3
[redacted]	IPv4_public	3
[redacted]	IPv4_public	3
[redacted]	IPv4_public	1

Address	Realm	Centrality
[redacted]	IPv4_public	31
[redacted]	IPv4_public	29
[redacted]	IPv4_public	7

Page 1 of 1 | Clear Filters | Displaying 1 - 1 of 1 | Page Size 30

Content Steward [redacted] General Support: Contact the SHADOWNET Team [redacted] [feedback](#)



# (U//FOUO) The Metrics Tab

- (S//SI//REL) Count distinct VPN records, grouping them by one or more of the following attributes:
  - ⇒ SIGAD
  - ⇒ Source
  - ⇒ VPN Type
  - ⇒ Case Notation
  - ⇒ Date

(U//FOUO)

# The Metrics Tab: One

## Example

The screenshot displays a web application interface with a table showing metrics for SIGAD and VPN Type. The table is titled "SIGAD X" and has the following columns: SIGAD, ESP, IKE\_ESP\_NAT, IKEV1, IKEV2, IPSEC, PPTP, RDP, SSH, and VPNET. The data is filtered by SIGAD: DS-2008, LNC-1155W, US-3140, US-3141B, US-1001TEC, USF-790, USJ-759, USJ-759A, USJ-759, and USF-759.

SIGAD	ESP	IKE_ESP_NAT	IKEV1	IKEV2	IPSEC	PPTP	RDP	SSH	VPNET	Total
USJ-759A	60677	7								60684
DS-2008	31931	64								31995
USJ-759	238									238
USD-1001TEC	10793									10793
USJ-759	1									1
US-3141B	551	45978			144688			5341	196558	196558
LNC-1155W	24									24
USF-700		12								12
USJ-759	4919									4919
US-3140	1	1956								1957
	109110	48042			144688			5341	307161	307161

Row Headers: SIGAD  
 Column Headers: VPN Type  
 Filter by SIGAD: DS-2008,LNC-1155W,US-3140,US-3141B,USD-1001TEC,USF-790,USJ-759,USJ-759A,USJ-759  
 Filter by Source: --No Selection--  
 Filter by VPN Type: ESP,IKEV1,PPTP,VPNET

SIGAD X

Content Steward [redacted] General Support: Contact the SHADOWNET Team [redacted] [Feedback](#)

DYNAMIC PAGE - HIGHEST POSSIBLE CLASSIFICATION

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

Content Steward [redacted] General Support: Contact the SHADOWNET Team [redacted] [Feedback](#)

DYNAMIC PAGE - HIGHEST POSSIBLE CLASSIFICATION

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

Content Steward [redacted] General Support: Contact the SHADOWNET Team [redacted] [Feedback](#)

DYNAMIC PAGE - HIGHEST POSSIBLE CLASSIFICATION

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

- (TS//SI//REL) Total number of VPN type per SIGAD.



(U//FOUO) **The Ultimate Goals**

- ⇒ (S//SI//REL) Integrate VPN information into mainstream analytic tools and knowledge bases.
- ⇒ (S//SI//REL) Give analysts the ability to discover, develop, and track known targets using VPNs.
- ⇒ (S//SI//REL) Give analysts the ability to discover new targets using VPNs.

(U//FOUO) **Questions?**



SSG22

Network Analysis Center