

# (TS//SI//REL)VPN SigDev Basics



S31244 - OTTERCREEK

Derived From: NSA/CSSM 1-52  
Dated: 20070108  
Declassify On: 20341101

Overall Classification:

TOP SECRET//COMINT//REL TO USA, FVEY

# (U) What is a VPN?

- (U) A Virtual Private Network or VPN is a computer network that uses encryption to securely connect remote users/networks over an otherwise insecure network, usually the public internet.
- (U) Common Types:
  - PPTP, IPSec, SSL
- (U) Public Key Encryption
  - Diffie-Hellman, RSA

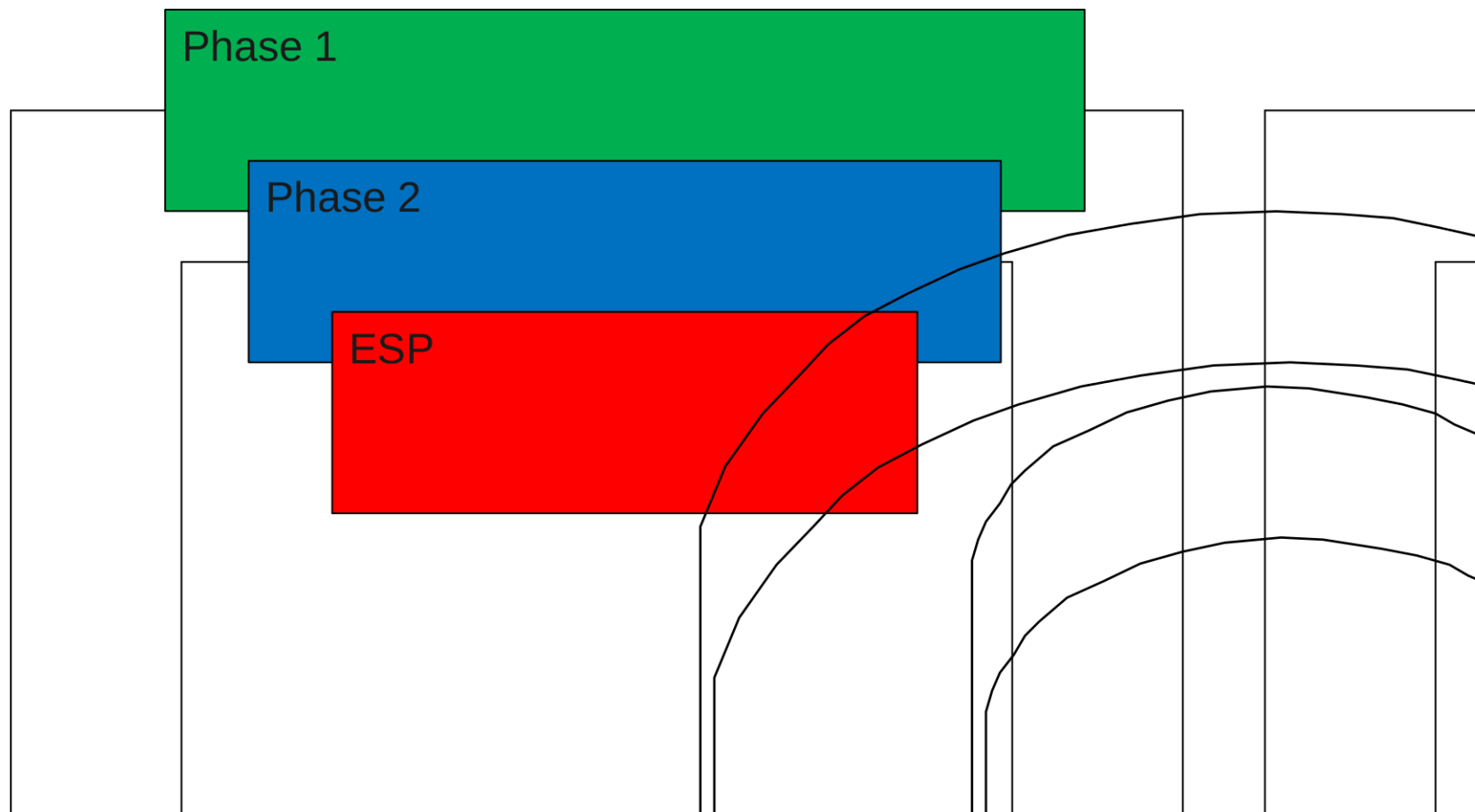
# (U) PPTP

- (U) Microsoft Point-to-Point Tunneling Protocol
- (U) Control Channel
  - TCP port 1723
- (U) Data Channel
  - GRE-Next Protocol 47
- (U) RFC 2637, RFC 3078

# (U) IPSec

- (U) Authentication
  - Pre-shared key (PSK) or Public key certificates
- (U) ISAKMP/IKE packets are used for key exchange and to establish the secure connection
  - UDP port 500, 4500; TCP port 500
- (U) ESP packets contain the encrypted data
  - IP Next Protocol 50; UDP port 500
- (U) RFC2402, RFC2406, RFC2409, RFC4306, RFC2408

# (U) IPSec in a nutshell

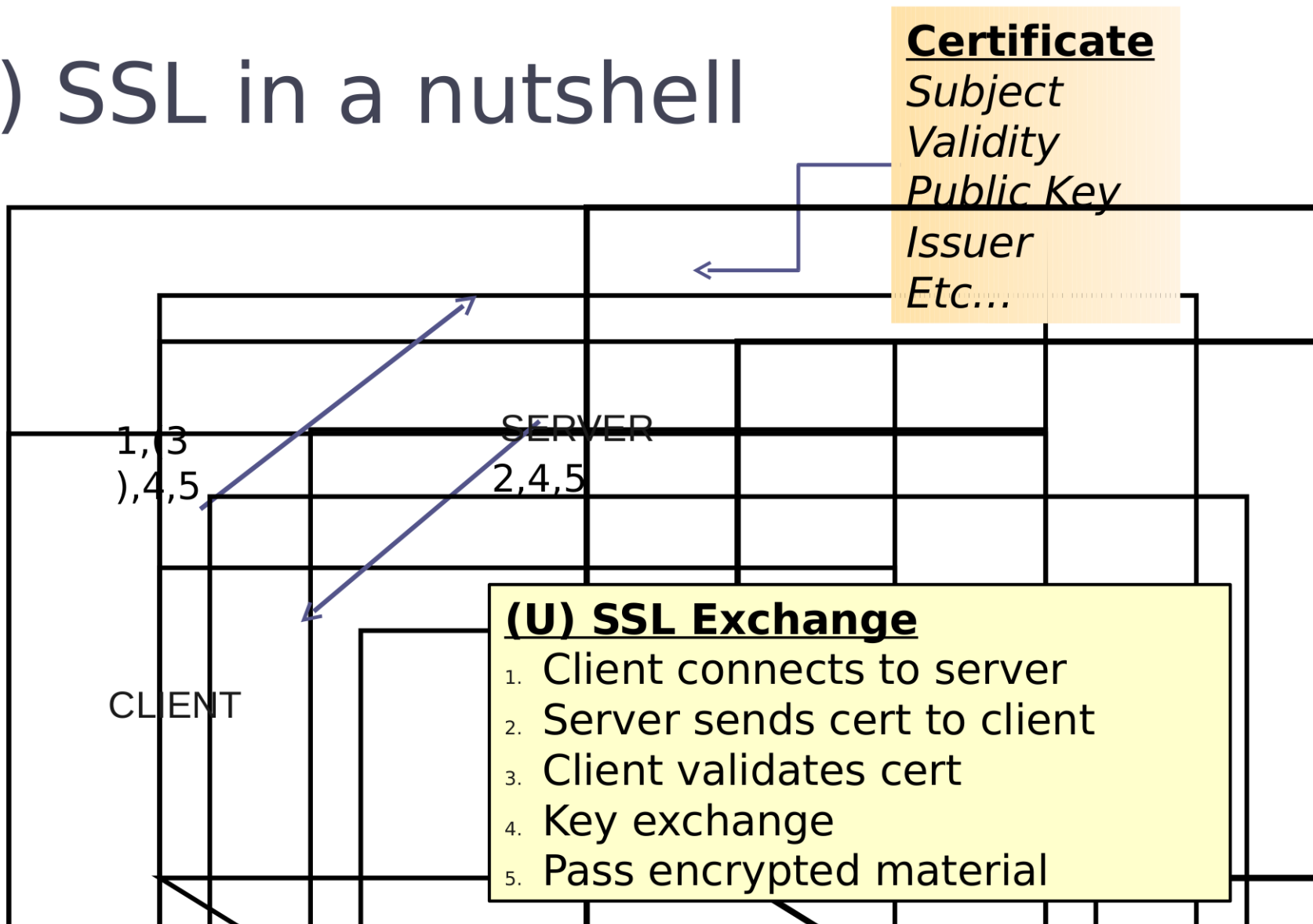


# (U) SSL/TLS

- (U) Secure Sockets Layer/Transport Layer Security
- (U) WARNING! e-commerce = tons of uninteresting SSL traffic
- (U) Common ports: TCP ports 443, 995
- (U) RFC2246, RFC4346, RFC5246

□

# (U) SSL in a nutshell

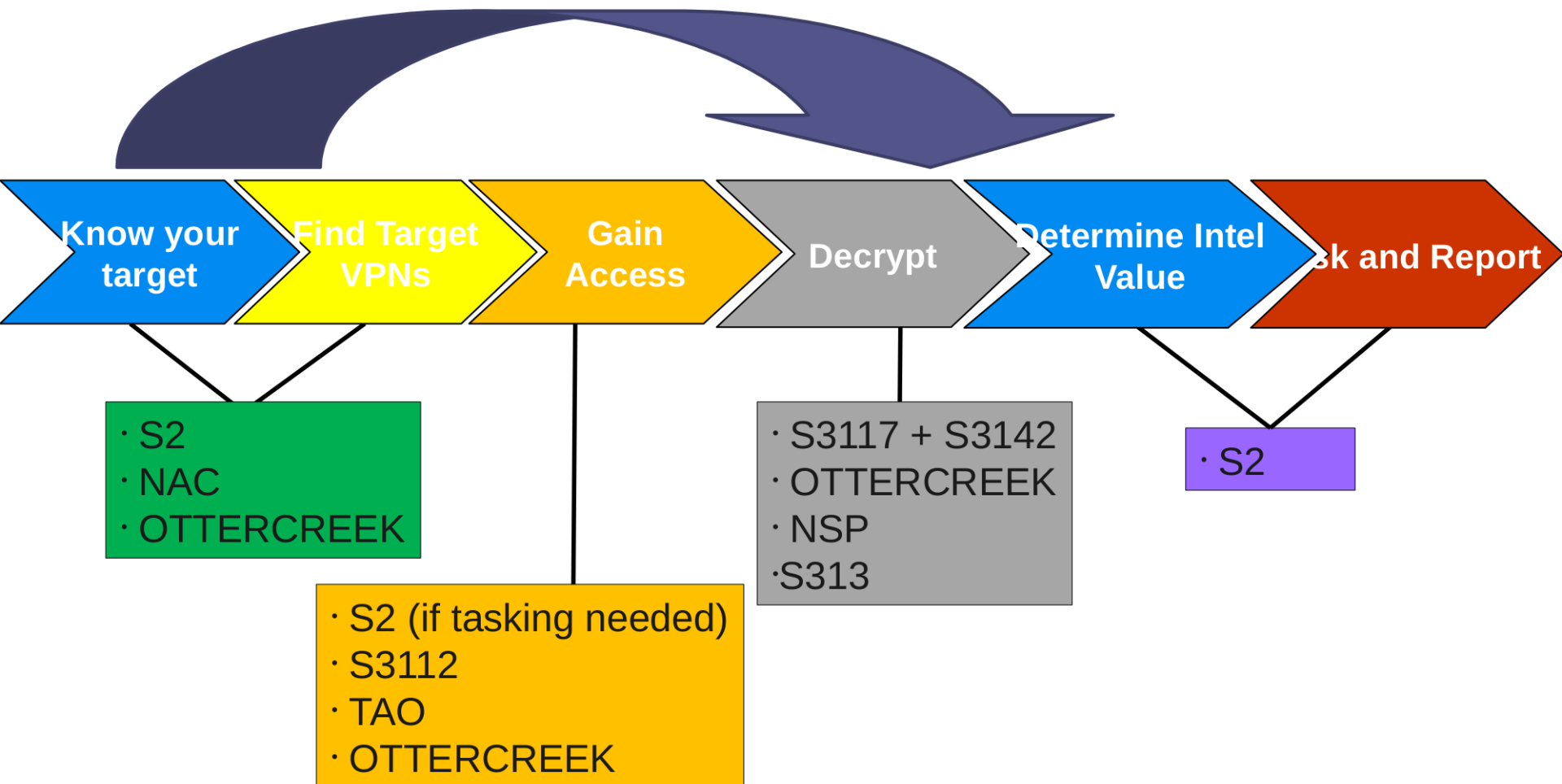




# (TS//SI//REL) Who works VPNs?

- (TS//SI//REL) VPN Working Group (go vpn)  
[REDACTED]
  - S2, SSG, CES (OTTERCREEK, NSP, S31322, S3117, S3112), TAO, etc.
- (TS//SI//REL) Alias: [REDACTED]  
(Board alias: [REDACTED])
- (TS//SI//REL) Meets every other Thursday at 1300

# (TS//SI/REL) Who works VPNs?



(TS//SI//REL) So you think your target is using a VPN...

# (TS//SI//REL) SigDev Tools

## (TS//REL) VPN Specific

- ~~BLEAKINQUIRY~~
- **DISCOROUTE**
- **TOYGRIPPE**

## (TS//REL) Also useful

- MARINA
- MASTERSHAKE
- NKB
- PINWALE
- RENOIR
- TREASUREMAP
- TUNINGFORK
- **XKEYSCORE**

# (TS//SI//REL) TOYGRIPPE

- (TS//SI//REL) Database of VPN metadata
  - IPsec, PPTP, ViPNet

Click to edit Master text styles

Second level

Third level

Fourth level

Fifth level

**(TS//REL) TYG Tips:**

- ∅ Populate "Display Fields"
- ∅ For both directions between 2 Ips, use **AND**
- ∅ For either direction connecting to a single IP, put IP in both "Source" and "Destination" boxes, and use **OR**

The screenshot shows a web application window titled "Standard Form - Mozilla Firefox". The interface is divided into several sections:

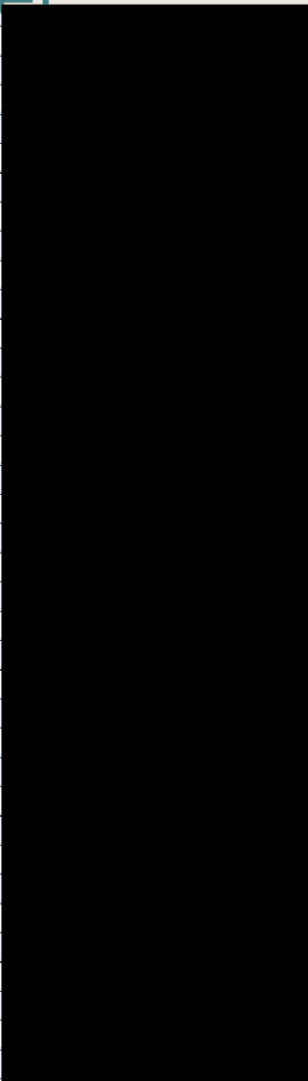
- Date Range(Required):** START: 4 / 1 / 2011 - 00 : 00 ; END: 4 / 5 / 2011 - 00 : 00
- Data Fields:** A list of fields with checkboxes and "Add/Remove" buttons. A red star highlights the "ACTIVE\_SURVEY" source field.
- Display Fields:** A list of fields to be displayed in the results, including "Timestamp", "Case Notation", "Site", "VPN Type", "Geo Source Country", "Source IP Address", "Destination IP Address", "Geo Destination Country", and "IPSEC Authentication Name".
- IP Addresses(Ranges and Wildcards Accepted):** Two columns for "Source IP Addresses" and "Destination IP Addresses" with "Clear" and "Addresses File..." buttons.

Navigation and control elements include "Execute", "Clear All", "Save as default", "Clear", and "Reset to Default" buttons. The interface also features a sidebar with "Query", "Results", "Preferences", and "Help" sections.

# Click to edit Master text styles

TS//SI//REL TO USA, FVEY	2011-04-02 08:29:38.0	KLDAB00001M1100	UKJ-260D	IKEV1	IR	DE	pre-shared key
TS//SI//REL TO USA, FVEY	2011-04-02 09:13:14.0	KLDAB00001M1100	UKJ-260D	IKEV1	IR	DE	pre-shared key
TS//SI//REL TO USA, FVEY	2011-04-02 10:48:10.0	KLDAB00001M1100	UKJ-260D	IKEV1	IR	DE	pre-shared key
TS//SI//REL TO USA, FVEY	2011-04-02 11:31:53.0	KLDAB00001M1100	UKJ-260D	IKEV1	IR	DE	pre-shared key
TS//SI//REL TO USA, FVEY	2011-04-03 12:22:03.0	KLDAB00001M1100	UKJ-260D	IKEV1	IR	DE	pre-shared key
TS//SI//REL TO USA, FVEY	2011-04-03 01:08:00.0	KLDAB00001M1100	UKJ-260D	IKEV1	IR	DE	pre-shared key
TS//SI//REL TO USA, FVEY	2011-04-03 01:54:35.0	KLDAB00001M1100	UKJ-260D	IKEV1	IR	DE	pre-shared key
TS//SI//REL TO USA, FVEY	2011-04-03 03:24:56.0	KLDAB00001M1100	UKJ-260D	IKEV1	IR	DE	pre-shared key
TS//SI//REL TO USA, FVEY	2011-04-03 04:58:08.0	KLDAB00001M1100	UKJ-260D	IKEV1	IR	DE	pre-shared key
TS//SI//REL TO USA, FVEY	2011-04-01 11:37:49.0	KLDAB00001M1100	UKJ-260D	ESP	IR	DE	
TS//SI//REL TO USA, FVEY	2011-04-01 17:37:33.0	KLV125899750000	US-966E	ESP	DE	IR	
TS//SI//REL TO USA, FVEY	2011-04-01 12:51:08.0	KLDAB00001M1100	UKJ-260D	IKEV1	IR	DE	
TS//SI//REL TO USA, FVEY	2011-04-01 00:08:15.0	IRS1037	DS-300	ESP	IR	DE	
TS//SI//REL TO USA, FVEY	2011-04-01 00:23:25.0	IRS1037	DS-300	IKEV1	IR	DE	
TS//SI//REL TO USA, FVEY	2011-04-03 05:41:27.0	KLDAB00001M1100	UKJ-260D	IKEV1	IR	DE	pre-shared key
TS//SI//REL TO USA, FVEY	2011-04-03 06:25:53.0	KLDAB00001M1100	UKJ-260D	IKEV1	IR	DE	pre-shared key
TS//SI//REL TO USA, FVEY	2011-04-03 07:56:09.0	KLDAB00001M1100	UKJ-260D	IKEV1	IR	DE	pre-shared key
TS//SI//REL TO USA, FVEY	2011-04-03 08:42:05.0	KLDAB00001M1100	UKJ-260D	IKEV1	IR	DE	pre-shared key
TS//SI//REL TO USA, FVEY	2011-04-03 09:32:55.0	KLDAB00001M1100	UKJ-260D	IKEV1	IR	DE	pre-shared key
TS//SI//REL TO USA, FVEY	2011-04-03 10:16:16.0	KLDAB00001M1100	UKJ-260D	IKEV1	IR	DE	pre-shared key
TS//SI//REL TO USA, FVEY	2011-04-03 10:59:38.0	KLDAB00001M1100	UKJ-260D	IKEV1	IR	DE	pre-shared key
TS//SI//REL TO USA, FVEY	2011-04-03 11:50:29.0	IR1S035	DS-200B	IKEV1	DE	IR	pre-shared key
TS//SI//REL TO USA, FVEY	2011-04-03 12:34:43.0	IR1S035	DS-200B	IKEV1	DE	IR	pre-shared key
TS//SI//REL TO USA, FVEY	2011-04-03 12:34:45.0	IR1S035	DS-200B	IKEV1	DE	IR	
TS//SI//REL TO USA, FVEY	2011-04-03 12:34:44.0	KLDAB00001M1100	UKJ-260D	IKEV1	IR	DE	pre-shared key
TS//SI//REL TO USA, FVEY	2011-04-03 01:23:51.0	KLDAB00001M1100	UKJ-260D	IKEV1	IR	DE	pre-shared key
TS//SI//REL TO USA, FVEY	2011-04-03 13:23:50.0	IR1S035	DS-200B	IKEV1	DE	IR	pre-shared key
TS//SI//REL TO USA, FVEY	2011-04-03 13:23:51.0	IR1S035	DS-200B	IKEV1	DE	IR	
TS//SI//REL TO USA, FVEY	2011-04-02 06:52:02.0	KLDAB00001M1100	UKJ-260D	ESP	IR	DE	
TS//SI//REL TO USA, FVEY	2011-04-02 05:07:51.0	KLDAB00001M1100	UKJ-260D	ESP	IR	DE	
TS//SI//REL TO USA, FVEY	2011-04-02 06:16:31.0	KLDAB00001M1100	UKJ-260D	ESP	IR	DE	
TS//SI//REL TO USA, FVEY	2011-04-02 07:48:23.0	KLDAB00001M1100	UKJ-260D	ESP	IR	DE	
TS//SI//REL TO USA, FVEY	2011-04-02 05:34:51.0	KLDAB00001M1100	UKJ-260D	ESP	IR	DE	
TS//SI//REL TO USA, FVEY	2011-04-02 00:18:42.0	KLDAB00001M1100	UKJ-260D	IKEV1	IR	DE	
TS//SI//REL TO USA, FVEY	2011-04-02 00:01:51.0	KLDAB00001M1100	UKJ-260D	ESP	IR	DE	
TS//SI//REL TO USA, FVEY	2011-04-02 00:18:41.0	IRS1037	DS-300	IKEV1	IR	DE	
TS//SI//REL TO USA, FVEY	2011-04-02 00:16:51.0	IRS1037	DS-300	ESP	IR	DE	

Second level  
Third level  
Fourth level  
Fifth level



Ø (U) Export results to excel or text doc for easier sorting.

# (TS//SI//REL) XKEYSCORE

## (TS//REL) Fingerprints

- IPsec
  - vpn/esp
  - vpn/isakmp
- PPTP
  - vpn/pptp\*
- SSL
  - network\_encryption/ssl

## (TS//REL) Search Forms

- Start with **FULL DNI**
  - **vpn/\***
  - **network\_encryption/\***
- IPsec
  - IKE Parser
- SSL
  - SSL Parser



Browser window: XK Search: Full Log - Mozilla Firefox

Address bar: ic.gov

Page Title: XK Search: Full Log

System Messages: This system is audited for USSID 18 and Human Rights Act compliance. TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, and NZL 20328108. XKEYSCORE Welcome srwils2! Warning: your password has expired! Log Out

Navigation Filter: Search Wizard, CNE, Classic, MultiSearch, Classic AM, Alert, BlackBerry, Call Logs, Category 2N, Cellular DNI, Cisco Passwords, Clarent, DNS, Document Metadata, Document Tagging, Email Addresses, Extracted Files, Full Log DNI, Geo Info, HTTP Activity, IKE Parser, Keylogger, Logins and Passwords, Machine Info, Microplug n Metadata, Obfuscation(Munged), Classic NZ, Network Information, Network Logs, PILBEAM, PPF VoIP Metacata, Passports from Images, Phone Number Extract, RBGAN, RTP, Radius Logs, Registry, SIP, SSH Parser, SSL Parser, Shellcode, TDI, TIPOFF Collection, Topic / Tech Strings, User Activity, User Activity (New/Exp)

Search: Full Log

Query Name: [Redacted]

Justification: (\*)//SI//REL Looking for IPsec traffic to perform vulnerability assessment. Recent Justifications

Additional Justification: [Dropdown]

Miranda Number: [Text Box]

Current Time: 2011-04-04 14:04:04 GMT

Datetime: 1 Day Start: 2011-04-03 00:00 Stop: 2011-04-05 00:00

Client IP (X-Forwarded-For): [Text Box] [Address Field Builder]

DVBS MAC: [Text Box]

DVBS PID: [Text Box]

WLAN Channel: [Text Box]

WLAN SSID: [Text Box]

WLAN BSSID: [Text Box]

WLAN DMAC: [Text Box]

WLAN SMAC: [Text Box]

SGAD: [Dropdown]

GPRS TLLI: [Text Box]

Active User-realm: [Text Box]

IP Address: [Text Box] [Dropdown] [Address Field Builder]

IP Address: [Text Box] [Dropdown] [Address Field Builder]

System Messages: This system is audited for USSID 18 and Human Rights Act compliance. TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, and NZL 20328108

File Edit View History Bookmarks Tools Help

ic.gov

XKEYSCORE TOYGRIPPE NKB: Home NKB Disco Route Roadbed.net MyPage GoldPoint

XK Search Full Lcg Standard Form

This system is audited for USSID 18 and Human Rights Act compliance  
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, and NZL/20329108

XKEYSCORE Welcome srwls2! [Warning: your password has expired!](#) [Log Out](#)

Home Search Workflow Central Results Fingerprints Statistics Map My Account XK Forum Help

Navigation Filter

Search Wizard

- CNE
- Classic
  - MultiSearch
  - Classic A-M
    - Alert
    - BlackBerry
    - Call Logs
    - Category DNI
    - Cellular DNI
    - Cisco Passwords
    - Clarent
    - DNS
    - Document Metadata
    - Document Tagging
    - Emai Addresses
    - Extracted Files
    - Full Log DNI
    - Geo Info
    - HTTP Activity
    - IKE Parser
    - Keylogger
    - Logins and Password
    - Machine Info
    - Microplugin Metadata
    - Obfuscation(Blunged T
  - Classic V-Z
    - Network Information
    - Network Logs
    - PILBEAM
    - PPF VoIP Metadata
    - Passports from Images
    - Phone Number Extra
    - RBGAN
    - RTP
    - Radius Logs
    - Registry
    - SIP
    - SSH Parser
    - SSL Parser
    - Shellcode
    - TDI
    - TIPOFF Collection
    - Topic/ Tech Strings
    - User Activity
    - User Activity (NewExp

Port: [ ] From [ ]

Port: [ ] To [ ]

Country: ILS AND IGB AND ICA AND INZ AND IAU From [ ]  One side is not 5-eyes

Country: ILS AND IGB AND ICA AND INZ AND IAU To [ ]  Both sides are not 5-eyes

City (IP): [ ] From [ ]

City (IP): [ ] To [ ]

Latitude (IP): [ ] From [ ]

Latitude (IP): [ ] To [ ]

Longitude (IP): [ ] From [ ]

Longitude (IP): [ ] To [ ]

Map Field Builder regions (IP): [ ] [Map Field Builder](#)

Outer Tunnel IP Address: [ ] From [ ] [IP Address Field Builder](#)

Outer Tunnel IP Address: [ ] To [ ] [IP Address Field Builder](#)

Outer Tunnel Port: [ ] From [ ]

Outer Tunnel Port: [ ] To [ ]

Application Type: [ ]

Application Info: [ ]

Application: **vpn\***

Apaid (+Fingerprints) [fulltext](#) [Populate with Field Builder](#) [Populate with Tree Field Builder](#)

Geolocation: [ ]

This system is audited for USSID 18 and Human Rights Act compliance  
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, and NZL/20329108

Done

∅ (TS//REL) For initial searches, you may want to leave this blank to see all of the different kinds of traffic are found on the IP pair.

XK Metaviewer: [redacted] vpn - Mozilla Firefox

File Edit View History Bookmarks Tools Help

ic.gov

XKEYSCORE TOYGRIPPE NKB Home NKB Disco Route Roadbed.net MyPage GoldPoint

XK Metaviewer: 84.11.25.13... x Standard Form x NKB Disco Route x https://ncmd...248823681254 x

This system is audited for USSID18 and Human Rights Act compliance  
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

XKEYSCORE Welcome swrls2! [Warning: your password has expired!](#) [Log Out](#)

Home Search Workflow Central Results Fingerprints Statistics Map My Account XK Forum Help

Navigation Filter [redacted] vpn

Search Wizard

- CNE
- Classic
  - MultiSearch
  - Classic A-M
    - Alert
    - BlackBerry
    - Call Logs
    - Category DNI
    - Cellular DNI
    - Cisco Passwords
    - Clarent
    - DNS
    - Document Metadata
    - Document Tagging
    - Email Addresses
    - Extracted Files
    - Full Log DNI
    - Geo Info
    - HTTP Activity
    - IKE Parser
    - Keylogger
    - Logins and Passwords
    - Machine Info
    - Microplugin Metadata
    - Obfuscation(Munged T
  - Classic N-Z
    - Network Information
    - Network Logs
    - PILBEAM
    - PPF VoIP Metadata
    - Passports from Images
    - Phone Number Extract
    - RBGAN
    - RTP
    - Radius Logs
    - Registry
    - SIP
    - SSH Parser
    - SSL Parser
    - Shellcode
    - TDI
    - TIPOFF Collection
    - Topic / Tech Strings
    - User Activity
    - User Activity (NewExp

Sigad	Casnotation	Datetime	Datetime E	Fm Port	Fm City (IP)	Fm Co Fm IP	To IP	To Co	To City (IP)	To Port	Application	AppID (+Fingerprints)
UKJ-260D	KLDAB00001M1100	2011-04-03 00:00:52	2011-04-03 0 0	0	[redacted]					0	vpnie.sp	vpnie.sp nac/vpn/protocoll
UKJ-260D	KLDAB00001M1100	2011-04-03 00:03:52	2011-04-03 0 0	0	[redacted]					0	vpnie.sp	vpnie.sp nac/vpn/protocoll
UKJ-260D	KLDAB00001M1100	2011-04-03 00:06:52	2011-04-03 0 0	0	[redacted]					0	vpnie.sp	vpnie.sp nac/vpn/protocoll
UKJ-260D	KLDAB00001M1100	2011-04-03 00:09:52	2011-04-03 0 0	0	[redacted]					0	vpnie.sp	vpnie.sp nac/vpn/protocoll
UKJ-260D	KLDAB00001M1100	2011-04-03 00:12:52	2011-04-03 0 0	0	[redacted]					0	vpnie.sp	vpnie.sp nac/vpn/protocoll
UKJ-260D	KLDAB00001M1100	2011-04-03 00:15:52	2011-04-03 0 0	0	[redacted]					0	vpnie.sp	vpnie.sp nac/vpn/protocoll
UKJ-260D	KLDAB00001M1100	2011-04-03 00:18:52	2011-04-03 0 0	0	[redacted]					0	vpnie.sp	vpnie.sp nac/vpn/protocoll
UKJ-260D	KLDAB00001M1100	2011-04-03 00:21:52	2011-04-03 0 0	0	[redacted]					0	vpnie.sp	vpnie.sp nac/vpn/protocoll
UKJ-260D	KLDAB00001M1100	2011-04-03 00:22:01	2011-04-03 0 500	500	[redacted]					500	vpni/sakmp	vpni/sakmp vpni/pscc/sakmp/main_mode/kev_exchange_message vpni/re_4 vpni/sakmp_content
UKJ-260D	KLDAB00001M1100	2011-04-03 00:24:52	2011-04-03 0 0	0	[redacted]					0	vpnie.sp	vpnie.sp nac/vpn/protocoll
UKJ-260D	KLDAB00001M1100	2011-04-03 00:27:52	2011-04-03 0 0	0	[redacted]					0	vpnie.sp	vpnie.sp nac/vpn/protocoll
UKJ-260D	KLDAB00001M1100	2011-04-03 00:30:52	2011-04-03 0 0	0	[redacted]					0	vpnie.sp	vpnie.sp nac/vpn/protocoll
UKJ-260D	KLDAB00001M1100	2011-04-03 00:33:52	2011-04-03 0 0	0	[redacted]					0	vpnie.sp	vpnie.sp nac/vpn/protocoll
UKJ-260D	KLDAB00001M1100	2011-04-03 00:36:52	2011-04-03 0 0	0	[redacted]					0	vpnie.sp	vpnie.sp nac/vpn/protocoll
UKJ-260D	KLDAB00001M1100	2011-04-03 00:39:52	2011-04-03 0 0	0	[redacted]					0	vpnie.sp	vpnie.sp nac/vpn/protocoll
UKJ-260D	KLDAB00001M1100	2011-04-03 00:42:52	2011-04-03 0 0	0	[redacted]					0	vpnie.sp	vpnie.sp nac/vpn/protocoll
UKJ-260D	KLDAB00001M1100	2011-04-03 00:45:52	2011-04-03 0 0	0	[redacted]					0	vpnie.sp	vpnie.sp nac/vpn/protocoll
UKJ-260D	KLDAB00001M1100	2011-04-03 00:51:52	2011-04-03 0 0	0	[redacted]					0	vpnie.sp	vpnie.sp nac/vpn/protocoll
UKJ-260D	KLDAB00001M1100	2011-04-03 00:54:52	2011-04-03 0 0	0	[redacted]					0	vpnie.sp	vpnie.sp nac/vpn/protocoll
UKJ-260D	KLDAB00001M1100	2011-04-03 00:57:52	2011-04-03 0 0	0	[redacted]					0	vpnie.sp	vpnie.sp nac/vpn/protocoll
UKJ-260D	KLDAB00001M1100	2011-04-03 01:00:52	2011-04-03 0 0	0	[redacted]					0	vpnie.sp	vpnie.sp nac/vpn/protocoll
UKJ-260D	KLDAB00001M1100	2011-04-03 01:06:31	2011-04-03 0 0	0	[redacted]					0	vpnie.sp	vpnie.sp nac/vpn/protocoll
UKJ-260D	KLDAB00001M1100	2011-04-03 01:07:58	2011-04-03 0 500	500	[redacted]					500	vpni/sakmp	vpni/sakmp vpni/pscc/sakmp/main_mode/kev_exchange_message vpni/re_4 vpni/sakmp_content
UKJ-260D	KLDAB00001M1100	2011-04-03 01:09:53	2011-04-03 0 0	0	[redacted]					0	vpnie.sp	vpnie.sp nac/vpn/protocoll
UKJ-260D	KLDAB00001M1100	2011-04-03 01:12:53	2011-04-03 0 0	0	[redacted]					0	vpnie.sp	vpnie.sp nac/vpn/protocoll
UKJ-260D	KLDAB00001M1100	2011-04-03 01:15:53	2011-04-03 0 0	0	[redacted]					0	vpnie.sp	vpnie.sp nac/vpn/protocoll
UKJ-260D	KLDAB00001M1100	2011-04-03 01:18:53	2011-04-03 0 0	0	[redacted]					0	vpnie.sp	vpnie.sp nac/vpn/protocoll
UKJ-260D	KLDAB00001M1100	2011-04-03 01:21:53	2011-04-03 0 0	0	[redacted]					0	vpnie.sp	vpnie.sp nac/vpn/protocoll
UKJ-260D	KLDAB00001M1100	2011-04-03 01:24:53	2011-04-03 0 0	0	[redacted]					0	vpnie.sp	vpnie.sp nac/vpn/protocoll
UKJ-260D	KLDAB00001M1100	2011-04-03 01:30:53	2011-04-03 0 0	0	[redacted]					0	vpnie.sp	vpnie.sp nac/vpn/protocoll
UKJ-260D	KLDAB00001M1100	2011-04-03 01:33:53	2011-04-03 0 0	0	[redacted]					0	vpnie.sp	vpnie.sp nac/vpn/protocoll
UKJ-260D	KLDAB00001M1100	2011-04-03 01:36:53	2011-04-03 0 0	0	[redacted]					0	vpnie.sp	vpnie.sp nac/vpn/protocoll
UKJ-260D	KLDAB00001M1100	2011-04-03 01:39:53	2011-04-03 0 0	0	[redacted]					0	vpnie.sp	vpnie.sp nac/vpn/protocoll
UKJ-260D	KLDAB00001M1100	2011-04-03 01:42:53	2011-04-03 0 0	0	[redacted]					0	vpnie.sp	vpnie.sp nac/vpn/protocoll
UKJ-260D	KLDAB00001M1100	2011-04-03 01:45:53	2011-04-03 0 0	0	[redacted]					0	vpnie.sp	vpnie.sp nac/vpn/protocoll

Page: 1 of 24 Page Size: 50 (Max 100 rows per page) Displaying 1 - 50 of 1171

jb\_58f22\_0097867001301926190\_1

This system is audited for USSID18 and Human Rights Act compliance  
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

XK Metaviewer: CREAKSTILE\_HW\_PK - Mozilla Firefox

ic.gov

XKEYSCORE TOYGRIPPE NKB: Home NKB Discs Route Roadbed.net MyPage GoldPoint

XK Results XK Metaviewer: CREAKSTIL... Query Results

This system is audited for USSID 18 and Human Rights Act compliance  
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

XKEYSCORE Welcome snwils2! [Warning: your password has expired!](#) [Log Out](#)

Home Search Workflow Central Results Fingerprints Statistics Map My Account XK Forum

Navigation Filter Histogram Grid

Page 1 of 1 Clear Selection Export

Filter: From IP To IP Count

		132
		72
		56
		38

CREAKSTILE\_HW\_PK

Help Actions Reports View Map View FILTERS:

	State	ID	Classification	Sigad	Casenoation	Datetime	Fm Port	Fm City (IP)	Fm Co	Fm IP	To IP	To Cou	To City (IP)	To Port	Applicat on	AppID (+Fingerprints)
1		226	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I UKC-302A	PKCSE018A000HD0	PKCSE018A000HD0	2011-04-01 00:41:04	500							500	vpn/sakmp	vpn/sakmp vpn/sakmp content vpn/sakmp ph...
2		263	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I UKC-302A	PKCSE018A000HD0	PKCSE018A000HD0	2011-04-01 00:41:04	500							500	vpn/sakmp	vpn/sakmp vpn/sakmp phase1_policy
3		264	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I UKC-302A	PKCSE018A000HD0	PKCSE018A000HD0	2011-04-01 00:41:04	500							500	vpn/sakmp	vpn/sakmp vpn/sakmp phase1_policy
4		234	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I UKC-302A	PKCSE018A000HD0	PKCSE018A000HD0	2011-04-01 00:41:04	500							500	vpn/sakmp	vpn/sakmp vpn/sakmp content vpn/sakmp ph...
5		261	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I UKC-302A	PKCSE018A000HD0	PKCSE018A000HD0	2011-04-01 00:46:33	500							500	vpn/sakmp	vpn/sakmp vpn/sakmp content
6		262	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I UKC-302A	PKCSE018A000HD0	PKCSE018A000HD0	2011-04-01 00:46:33	500							500	vpn/sakmp	vpn/sakmp vpn/sakmp content
7		259	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I UKC-302A	PKCSE018A000HD0	PKCSE018A000HD0	2011-04-01 00:49:00	500							500	vpn/sakmp	vpn/sakmp vpn/sakmp content
8		260	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I UKC-302A	PKCSE018A000HD0	PKCSE018A000HD0	2011-04-01 00:49:00	500							500	vpn/sakmp	vpn/sakmp vpn/sakmp content
9		265	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I UKC-302A	PKCSE018A000HD0	PKCSE018A000HD0	2011-04-01 01:45:31	500							500	vpn/sakmp	vpn/sakmp vpn/sakmp content
10		266	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I UKC-302A	PKCSE018A000HD0	PKCSE018A000HD0	2011-04-01 01:45:31	500							500	vpn/sakmp	vpn/sakmp vpn/sakmp content
11		267	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I UKC-302A	PKCSE018A000HD0	PKCSE018A000HD0	2011-04-01 02:42:40	500							500	vpn/sakmp	vpn/sakmp vpn/sakmp content
12		268	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I UKC-302A	PKCSE018A000HD0	PKCSE018A000HD0	2011-04-01 02:42:40	500							500	vpn/sakmp	vpn/sakmp vpn/sakmp content
13		162	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I UKC-302A	PKCSE087A000HD0	PKCSE087A000HD0	2011-04-01 03:27:09	500							500	vpn/sakmp	vpn/sakmp vpn/device/ipsecc vpn/sakmp phase...
14		237	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I UKC-302A	PKCSE087A000HD0	PKCSE087A000HD0	2011-04-01 03:27:09	500							500	vpn/sakmp	vpn/sakmp vpn/device/ipsecc vpn/sakmp phase...
15		271	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I UKC-302A	PKCSE087A000HD0	PKCSE087A000HD0	2011-04-01 03:27:10	500							500	vpn/sakmp	vpn/sakmp vpn/sakmp content vpn/sakmp ph...
16		272	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I UKC-302A	PKCSE087A000HD0	PKCSE087A000HD0	2011-04-01 03:27:10	500							500	vpn/sakmp	vpn/sakmp vpn/sakmp content vpn/sakmp ph...
17		163	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I UKC-302A	PKCSE018A000HD0	PKCSE018A000HD0	2011-04-01 03:34:12	500							500	vpn/sakmp	vpn/sakmp vpn/sakmp content
18		236	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I UKC-302A	PKCSE018A000HD0	PKCSE018A000HD0	2011-04-01 03:34:12	500							500	vpn/sakmp	vpn/sakmp vpn/sakmp content
19		1	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I UKC-302A	PKCSE087A000HD0	PKCSE087A000HD0	2011-04-01 03:58:52	500							500	vpn/sakmp	vpn/sakmp vpn/sakmp content
20		2	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I UKC-302A	PKCSE087A000HD0	PKCSE087A000HD0	2011-04-01 03:58:52	500							500	vpn/sakmp	vpn/sakmp vpn/sakmp content
21		10	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I UKC-302A	PKCSE018A000HD0	PKCSE018A000HD0	2011-04-01 07:15:29	500							500	vpn/sakmp	vpn/sakmp vpn/sakmp content
22		247	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I UKC-302A	PKCSE018A000HD0	PKCSE018A000HD0	2011-04-01 07:15:29	500							500	vpn/sakmp	vpn/sakmp vpn/sakmp content
23		175	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I UKC-302A	PKCSE018A000HD0	PKCSE018A000HD0	2011-04-01 08:24:36	500							500	vpn/sakmp	vpn/sakmp vpn/sakmp content
24		230	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I UKC-302A	PKCSE018A000HD0	PKCSE018A000HD0	2011-04-01 08:24:36	500							500	vpn/sakmp	vpn/sakmp vpn/sakmp content
25		3	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I UKC-302A	PKCSE018A000HD0	PKCSE018A000HD0	2011-04-01 08:24:36	500							500	vpn/sakmp	vpn/sakmp vpn/sakmp content

Page 1 of 6 Page Size: 50 (Max 100 rows per page)

Displaying 1 - 50 of 298

jb\_58f22\_00966248001301946356\_1

This system is audited for USSID 18 and Human Rights Act compliance  
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

# (TS//SI//REL) PINWALE

- (TS//SI//REL) Both VPN traffic and Sys Admins passing information about VPN setup
- (TS//SI//REL) IP addresses and port numbers (ex. AP 00500) \*\*\***Document Zone = C2C**
- (TS//SI//REL) Display 'DZ Protocol SRC Port', 'DZ Protocol DEST Port', 'Next Protocol Name'

# (TS//SI//REL) DISCORROUTE

- (TS//SI//REL) Router configuration data
  - From passive and active collection
  - Key terms to search for within configs:
    - 'crypto map', 'isakmp', 'ipsec', 'pre-shared-key'

NKB Disco Route - Mozilla Firefox

File Edit View History Bookmarks Tools Help

ic.gov

XKEYSCORE TOYGRIPPE NKB: Home NKB Disco Route Roadbed.net MyPage GoldPoint

XK Results Query Results NKB Disco Route TREASUREMAP - TOOLS

Network Knowledge Base DiscoRoute (Version 2.14) NKB HOME

Combined Query Network Mgmt Query (Coming Soon) Help Feedback

### DiscoRoute Combined Query

Submit CSV Tips: If TAO has a Point-of-presence, you will see H manifest tag in results. Query History:

Collapse Results by Hostname/Sigad

#### General Query Terms

Text Query:

Date

Start Date:  End Date:

DOI  Load Date  Entire Database

Vendor

Cisco  Huawei  Infinet  
 Juniper  Mikrotik  Tenorswitch

Select All Clear All

IP Address

IP Address:

(1.2.3.4 or 1.2.3.4[CIDR] or 1.2.3.4-3.4.5.4)

IP Range Search

Interfaces - Subnet  Static Route IP  Access Lists  Routing Protocol IP

Exact IP Search

IP Header FROM/TO  Interfaces - Exact  Anywhere else in the XML

Limit Search to CIDR Ranges Smaller Than (or equal to): /24

Select All Clear All Any checked items can be found (OR condition) in config

Manifest (Cisco Only)

A - EQUANT  I - Show Interfaces  P - Voip  
 B - BGP  K - Crypto Keys  R - Show Run  
 D - Show CDP  M - Multihop  T - Tacacs  
 G - GPRS  N - Tgt Net Service  V - Show Version  
 H - TAO Pop  O - OSPF

Clear All All checked items must be found (AND condition) in config

Session ID:

Clear Panel

Hostname:   
SIGAD:   
Case:   
Country:   
TAO Project Name:

AS Number

AS:

Seen in Config  Derived

Snmp Community:   
IOS Image Name:   
Device Type:

Done

NKB Disco Route - Mozilla Firefox

Dynamic Page -- Highest Possible Classification is TOP SECRET//COMINT//ORCON//NOFORN//20320108

Network Knowledge Base DiscoRoute (Version 2.14) NKB HOME

Combined Query Network Mgmt Query (Coming Soon) Help Feedback

Detailed Combined Command Results

Hostname	Model	DOI	Vendor	Sigad	Case	Manifest	IOS Image N	Source IP	S Country	S City	Session	Quality	SPort	DPort	B
GW_SMS		200912-29	huawei	USD-1001TE	MNDAQ						4432	18	00023	12488	
GW_SMS		200912-15	huawei	USD-1001TE	MNDAQ						25956	20	00023	13320	
GW_SMS		200912-15	huawei	USD-1001TE	MNDAQ						25956	20	00023	13320	
		200911-13	cisco	USD-1001TE	MNDAQ						96	9	00023	13429	
A6-VPN		200910-22	huawei	USF-790	5CDVB000001MWC	R					23965	51	00023	01327	
A6-VPN		200910-22	huawei	USF-790	5CDVB000001MWC	R					17894	55	00023	01327	
A6-VPN		200910-13	huawei	USF-790	5CDVB000001MWC	R					8809	47	00023	01089	
		200910-02	huawei	USD-1001TE	MNDAQ						57299	1	23	13332	
		200909-10	huawei	USD-1001TE	MNDAQ						4210	1	23	15973	
		200909-10	huawei	USD-1001TE	MNDAQ						4905	1	23	13841	
		200906-15	huawei	USF-790	5CDVB000001MWC						31407	54	23	1031	

Page 1 of 1 Save as CSV Save Files to Disk Compare Results Summary Mailorder Out Map in Renoir Map Multiple Configs in Renoir Find Related Results 1 - 33

password cipher JS,[51EA,%B,.\#C3YB91!!  
service-type telnet terminal  
level 3...I..L  
#  
ike proposal 10  
encryption-algorithm 3des-cbc  
dh group21..U..  
#  
ike peer peer\_hq  
exchange-mode aggressive  
pre-shared-key Key4Cuba-A6  
id-type name  
remote-address [REDACTED]  
nat traversal  
peer multi-subnet.I..v..  
ipsec proposal proposal\_ph2  
esp authentication-algorithm sha1

Powered by the SIGDEV Lab  
Version Number: 2.14 New!  
Last Modified Date: March 14, 2011  
Last Reviewed Date: March 14, 2011  
Content Steward: SSG21, 969-3941  
Page Publisher: [REDACTED] CON; SSG21, 969-0942

Dynamic Page -- Highest Possible Classification is TOP SECRET//COMINT//ORCON//NOFORN//20320108

Find: Previous Next Highlight all Match case

Done



NKB Disco Route - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://ic.gov

XKEYSCORE TOYGRIPPE NKB: Home NKE Disco Route Roadbed.net MyPage GodPoint

XK Results Standard Form NKB Disco Route https://rcmd...248823681254

Dynamic Page -- Highest Possible Classification is TOP SECRET//COMINT//ORCON//NOFORN//20320108

Network Knowledge Base DiscoRoute (Version 2.14) NKB HOME

Combined Query Network Mgmt Query (Coming Soon) Help Feedback

DiscoRoute Combined Query

Submit CSV Tips: This is the new DISCORoute webserver. Update a bookmark to bring you here. Query History:

General Query Terms

Text Query: UNAMI

Date: Start Date, End Date, DOI, Load Date, Entire Database

IP Address: IP Address: (1.2.3.4 or 1.2.3.4/CIDR or 1.2.3.4-3.4.5.6)

IP Range Search: Interfaces - Subnet, Static Route IP, Access Lists, Routing Protocol IP

Exact IP Search: IP Header FROM/TO, Interfaces - Exact, Anywhere else in the XML

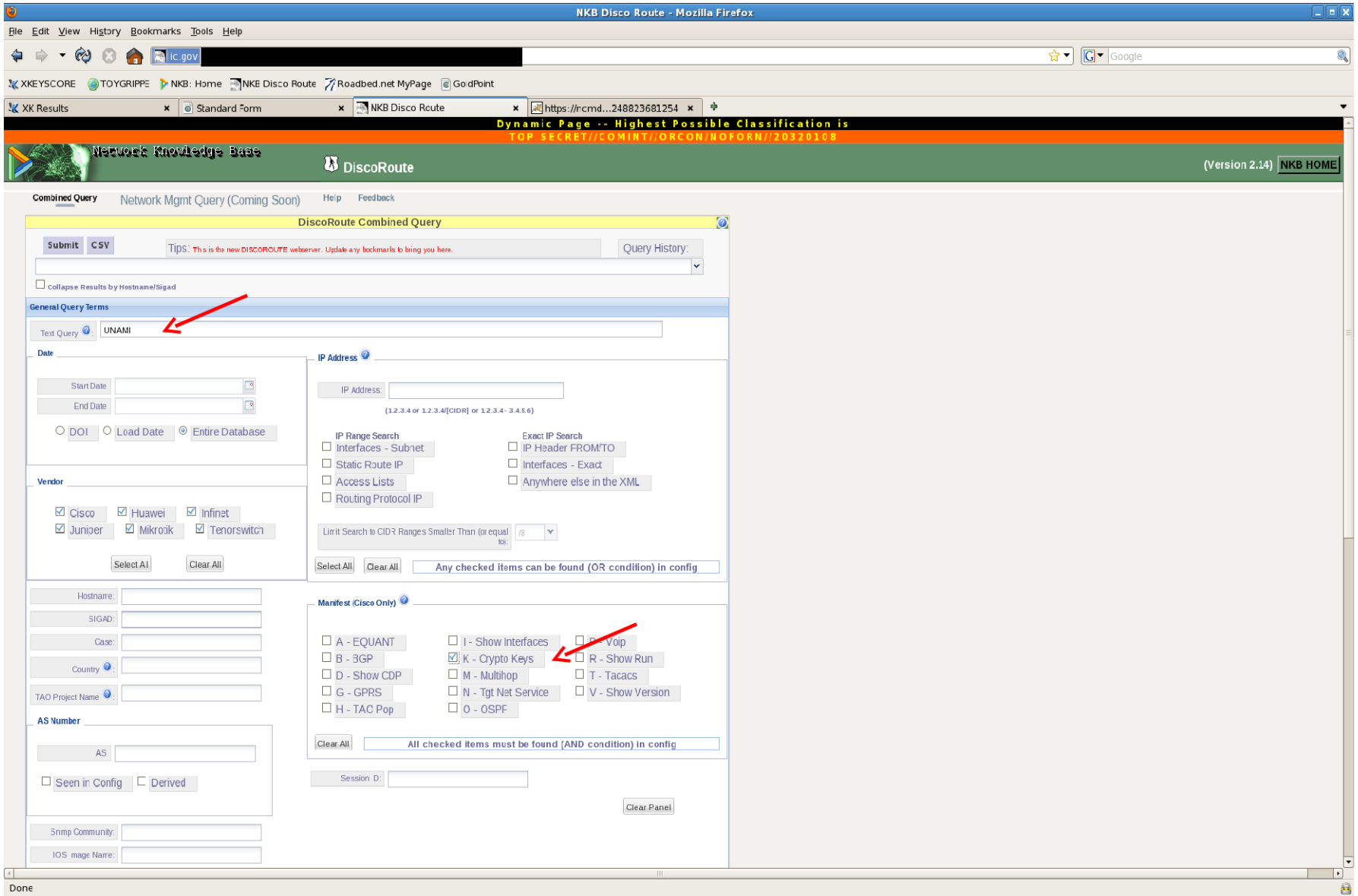
Vendor: Cisco, Huawei, Infinet, Juniper, Mikrotik, Tenorswitch

Manifest (Cisco Only): A - EQUANT, B - BGP, D - Show CDP, G - GPRS, H - TAC Pop, I - Show Interfaces, K - Crypto Keys, M - Multihop, N - Tgt Net Service, O - OSPF, P - Voip, R - Show Run, T - Tacacs, V - Show Version

Clear All: All checked items can be found (OR condition) in config

Clear All: All checked items must be found (AND condition) in config

Session ID: Clear Panel



Combined Query Network Mgmt Query (Coming Soon) Help Feedback

Detailed Combined Command Results

Hostname	Model	DOI	Vendor	Sigad	Case	Manifest	IOS Image N	Source IP	S Country	S City	Session	Qualit	SPort	DPort	B
<input checked="" type="checkbox"/> VPN01-UNAMI-E		2009-06-09T	cisco	UKC-125W	G2B7000001MWC	K_PR				RESERVED	109460	78	23	61470	
<input type="checkbox"/> GILAT-HRTS5826	c2600	2009-10-15T	cisco	UKC-125W	G2B8200001MWC	D_K_RT	c2600-advsn			RESERVED	134422	75	00023	00319	
<input type="checkbox"/> GILAT-HRTS5826	c2600	2009-10-31T	cisco	UKC-125W	G2B8200001MWC	D_K_R	c2600-advsn			RESERVED	38202	75	00023	02012	
<input type="checkbox"/> kuw-hub		2009-10-15T	cisco	UKC-125W	G2B6900001MWC	D_K_R				RESERVED	32879	74	00023	50554	
<input type="checkbox"/> kuw-hub		2009-10-15T	cisco	UKC-125W	G2B6900001MWC	D_K_R				RESERVED	32879	74	00023	50554	
<input type="checkbox"/> kuw-hub		2009-10-15T	cisco	UKC-125W	G2B7900001MWC	D_K_R				RESERVED	30000	74	00023	50554	
<input type="checkbox"/> VPN02-UNAMI-K		2009-09-10T	cisco	UKC-125W	G2B8200001MWC	K_PR	c2800nm-ad			RESERVED	58980	73	23	3408	
<input type="checkbox"/> r-unami-kuw-isp		2009-01-16T	cisco	UKC-125W	G2B6900001MWC	D_K_R				RESERVED	26342	71	23	59226	
<input type="checkbox"/> ISPO2-UNAMI-AP		2009-07-03T	cisco	US-967J	1AH116337454200	B_K_OPR				RESERVED	29872	71	23	27714	
<input type="checkbox"/> bdr01-unami-kir		2009-06-07T	cisco	UKC-125W	G2B7000001MWC	K_PR				DUBAI	23927	69	23	64278	
<input type="checkbox"/> bdr01-unami-mc	c2800nm	2010-06-22T	cisco	UKC-125W	G2B67000001MWC	K_N_PR	c2800nm-ad			RESERVED	40264	68	00023	44033	

Page 1 of 2 Save as CSV Save Files to Disk Compare Results Summary Mailorder Out Map in Renoir Map Multiple Configs in Renoir Find Related Results 1 - 200

Payload XML Summary Map Query Parameters Open in New Window

```

*****
*
* UNAMI
*
* Authorized Personnel Only
* If you do not have explicit authorization issued by UNAMI NMU to access
* this H
*
* C device, leave now!
*
* System:
* IP Add:
*
* DESCRIPTION : THIS ROUTER IS THEVOICE GATEWAY INTENDED FOR USE WITH THE
* H
*
* g{
*
*
* FEATURES

```

Powered by the SIGDEV Lab  
 Version Number: 2.14 - NEW  
 Last Modified Date: March 14, 2011  
 Last Reviewed Date: March 14, 2011  
 Content Steward:  
 Page Publisher:

# (U) Others

- (TS//REL) NKB
- (TS//REL) TUNINGFORK
- (TS//REL) TREASUREMAP
- (TS//REL) RENOIR
- (TS//REL) MASTERSHAKE
- (TS//REL) ROADBED
- (TS//REL) ~~BLEAKINQUIRY~~

# (TS//SI//REL) Basic VPN rules of thumb

## (TS//REL) If you have an IP address...

- Check TOYGRIPPE and XKS
  - Look for paired traffic
- For IPsec, check sys admin chatter for PSK (DISCOROUTE; PINWALE; MARINA)
- Share your data with OTTERCREEK for vulnerability assessment (XKEYSCORE or DROPBOX)
- Submit tasking

## (TS//REL) If you don't ...

- Look in DISCOROUTE
- Query Sys Admins in PINWALE and MARINA
- Check your targets TAO projects

EITHER WAY,  
JOIN THE  
**VPN WORKING GROUP**  
FOR ALL OF YOUR  
VPN SIGDEV NEEDS

# (U//FOUO) Useful Links

- (TS//SI//REL) VPN Working Group (go vpn) [REDACTED]
- (TS//SI//REL) OTTERCREEK (go VPN XFT)  
[REDACTED]
  - VPNXFT DROPBOX[REDACTED]
- (TS//SI//REL) Network Security Products (go NSP)  
[REDACTED]

# (U) Questions?

[REDACTED]

[REDACTED]

OTTERCREEK

[REDACTED]