

(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

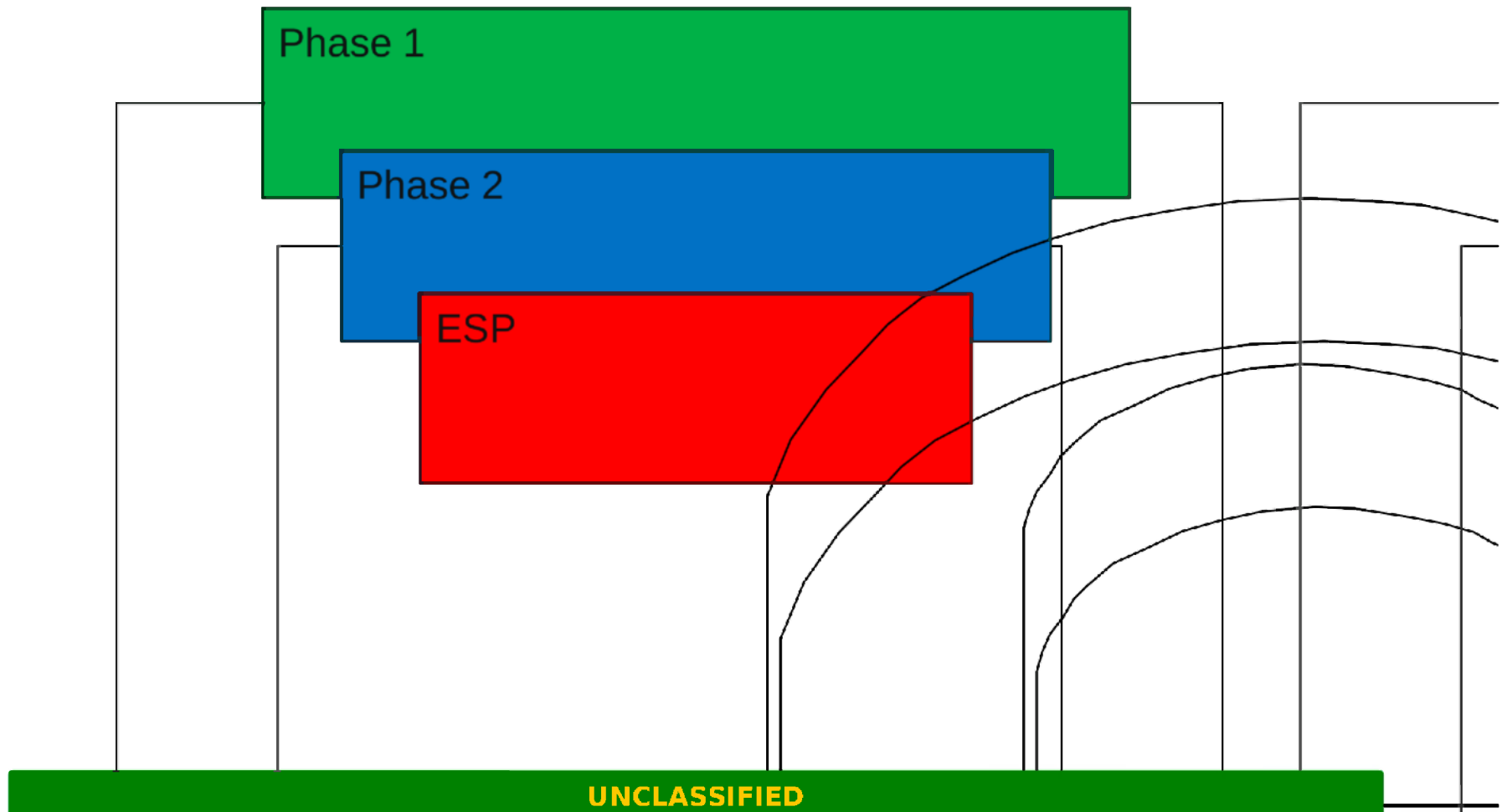
(U) PPTP

- (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

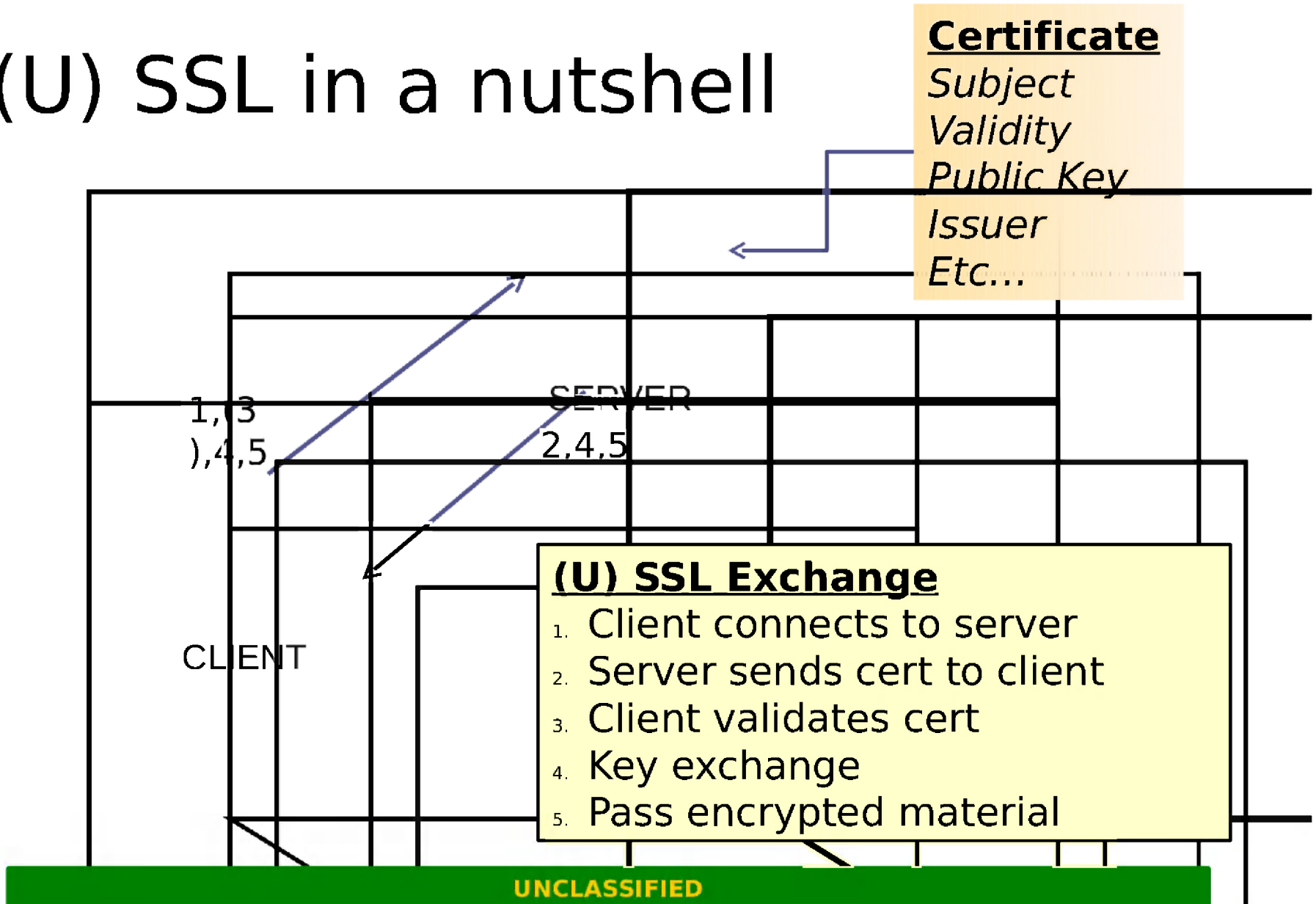


(U) SSL/TLS

- (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

□

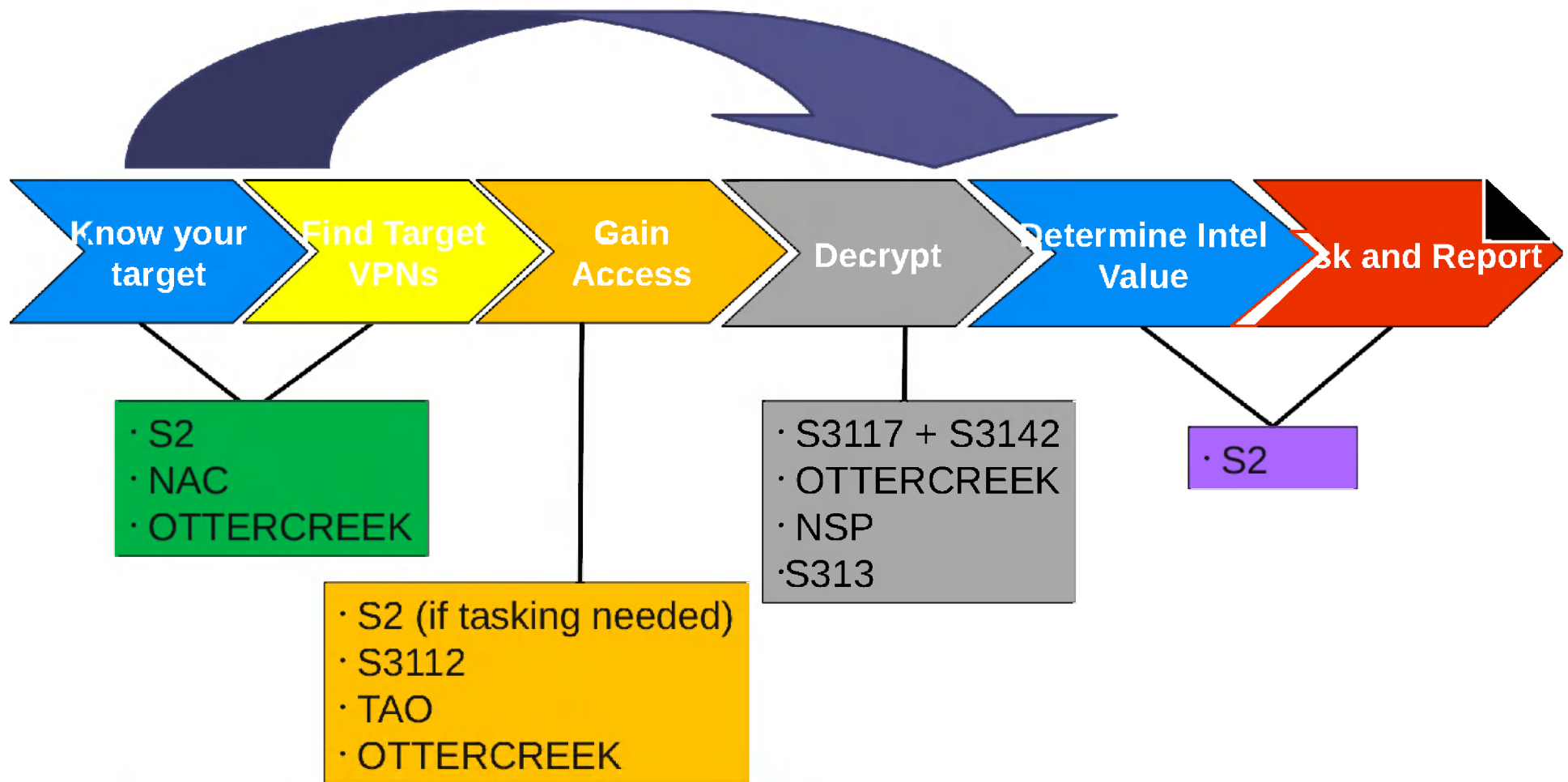
(U) SSL in a nutshell



(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

The screenshot shows a web browser window displaying a query tool interface. The browser's address bar shows a URL starting with 'Roadbed.net'. The interface includes a 'Query' section with a 'Date Range' field set to 'START: 4 / 1 / 2011 00:00' and 'END: 4 / 5 / 2011 00:00'. Below this is a 'Data Fields' section with a list of fields including 'Sites', 'Sources', 'Selected Sites', 'Selected Sources', 'Case Notation', 'Vendor Name', 'Source CIDR', 'Destination CIDR', 'Source Company', 'Dest. Company', 'Source Country', 'Dest. Country', 'Source Domain', 'Dest. Domain', and 'Info Name'. A red star is placed over the 'Add' button next to the 'Sources' field, which is set to 'ACTIVE_SURVEY'. To the right, a 'Display Fields' section lists fields like 'Timestamp', 'IP Address', 'Geo Location', etc. Below that is an 'IP Addresses' section with 'Source IP Addresses' and 'Destination IP Addresses' fields. The interface also has a 'Save Standard Query' section and an 'Execute' button. Annotations in blue and purple text are overlaid on the image: 'Click to edit Master' at the top, 'Second level' pointing to the 'Date Range' field, 'Third level' pointing to the 'Data Fields' section, 'Fourth level' pointing to the 'Sources' field, and 'Fifth level' pointing to the 'Add' button. A red arrow points from the 'Add' button to the 'Display Fields' section.

r text styles

(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**

Query Results - Mozilla Firefox

Click to edit Master text styles

Second level

Third level

Fourth level

Fifth level

TS//SWREL TO USA, FVEY	2011-04-02 08:28:38.0	KLDAB00001M1100	JKJ-2600	IKEV1	IR	DE	pro-shared key
TS//SWREL TO USA, FVEY	2011-04-02 09:13:14.0	KLDAB00001M1100	JKJ-2600	IKEV1	IR	DE	pro-shared key
TS//SWREL TO USA, FVEY	2011-04-02 10:48:13.0	KLDAB00001M1100	JKJ-2600	IKEV1	IR	DE	pro-shared key
TS//SWREL TO USA, FVEY	2011-04-02 11:31:53.0	KLDAB00001M1100	JKJ-2600	IKEV1	IR	DE	pro-shared key
TS//SWREL TO USA, I VLY	2011-04-03 12:22:03.0	KLDAB00001M1100	JKJ-2600	IKEV1	IR	DE	pro-shared key
TS//SWREL TO USA, FVEY	2011-04-03 01:08:00.0	KLDAB00001M1100	JKJ-2600	IKEV1	IR	DE	pro-shared key
TS//SWREL TO USA, FVEY	2011-04-03 01:54:35.0	KLDAB00001M1100	JKJ-2600	IKEV1	IR	DE	pro-shared key
TS//SWREL TO USA, FVEY	2011-04-03 03:24:56.0	KLDAB00001M1100	JKJ-2600	IKEV1	IR	DE	pro-shared key
TS//SWREL TO USA, FVEY	2011-04-03 04:58:08.0	KLDAB00001M1100	JKJ-2600	IKEV1	IR	DE	pro-shared key
TS//SWREL TO USA, I VLY	2011-04-01 11:37:48.0	KLDAB00001M1100	JKJ-2600	LSP	IR	DE	
TS//SWREL TO USA, FVEY	2011-04-01 17:37:33.0	KLV125899750000	US 066E	ESP	DE	IR	
TS//SWREL TO USA, FVEY	2011-04-01 12:51:08.0	KLDAB00001M1100	JKJ-2600	IKEV1	IR	DE	
TS//SWREL TO USA, FVEY	2011-04-01 00:00:15.0	IR51037	DS-300	FSP	IR	DE	
TS//SWREL TO USA, FVEY	2011-04-01 00:23:25.0	IR51037	DS-300	IKEV1	IR	DE	
TS//SWREL TO USA, I VLY	2011-04-03 05:41:27.0	KLDAB00001M1100	JKJ-2600	IRLV1	IR	DE	pro-shared key
TS//SWREL TO USA, FVEY	2011-04-03 06:25:53.0	KLDAB00001M1100	JKJ-2600	IKEV1	IR	DE	pro-shared key
TS//SWREL TO USA, FVEY	2011-04-03 07:56:09.0	KLDAB00001M1100	JKJ-2600	IKEV1	IR	DE	pro-shared key
TS//SWREL TO USA, FVEY	2011-04-03 08:42:05.0	KLDAB00001M1100	JKJ-2600	IKEV1	IR	DE	pro-shared key
TS//SWREL TO USA, FVEY	2011-04-03 09:32:55.0	KLDAB00001M1100	JKJ-2600	IKEV1	IR	DE	pro-shared key
TS//SWREL TO USA, FVEY	2011-04-03 10:16:16.0	KLDAB00001M1100	JKJ-2600	IKFV1	IR	DE	pro-shared key
TS//SWREL TO USA, FVEY	2011-04-03 10:59:38.0	KLDAB00001M1100	JKJ-2600	IKEV1	IR	DE	pro-shared key
TS//SWREL TO USA, I VLY	2011-04-03 11:50:28.0	IR15035	DS-2003	IRLV1	DL	IR	pro-shared key
TS//SWREL TO USA, FVEY	2011-04-03 12:34:43.0	IR15035	DS-2003	IKEV1	DE	IR	pro-shared key
TS//SWREL TO USA, FVEY	2011-04-03 12:34:45.0	IR15035	DS-2003	IKEV1	DE	IR	
TS//SWREL TO USA, FVEY	2011-04-03 12:34:44.0	KLDAB00001M1100	JKJ-2600	IKFV1	IR	DE	pro-shared key
TS//SWREL TO USA, FVEY	2011-04-03 01:23:51.0	KLDAB00001M1100	JKJ-2600	IKEV1	IR	DE	pro-shared key
TS//SWREL TO USA, I VLY	2011-04-03 13:23:50.0	IR15035	DS-2003	IRLV1	DL	IR	pro-shared key
TS//SWREL TO USA, FVEY	2011-04-03 13:23:51.0	IR15035	DS-2003	IKEV1	DE	IR	
TS//SWREL TO USA, FVEY	2011-04-02 06:52:02.0	KLDAB00001M1100	JKJ-2600	ESP	IR	DE	
TS//SWREL TO USA, FVEY	2011-04-02 05:07:51.0	KLDAB00001M1100	JKJ-2600	FSP	IR	DE	
TS//SWREL TO USA, FVEY	2011-04-02 06:16:31.0	KLDAB00001M1100	JKJ-2600	ESP	IR	DE	
TS//SWREL TO USA, I VLY	2011-04-02 07:48:23.0	KLDAB00001M1100	JKJ-2600	LSP	IR	DE	
TS//SWREL TO USA, FVEY	2011-04-02 05:34:51.0	KLDAB00001M1100	JKJ-2600	ESP	IR	DE	
TS//SWREL TO USA, FVEY	2011-04-02 00:18:42.0	KLDAB00001M1100	JKJ-2600	IKEV1	IR	DE	
TS//SWREL TO USA, FVEY	2011-04-02 00:01:51.0	KLDAB00001M1100	JKJ-2600	FSP	IR	DE	
TS//SWREL TO USA, FVEY	2011-04-02 00:18:41.0	IR51037	DS-300	IKEV1	IR	DE	
TS//SWREL TO USA, FVEY	2011-04-02 00:16:51.0	IR51037	DS-300	LSP	IR	DE	

⌀ (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

The screenshot shows a web browser window titled "XK Search: Full Log - Mozilla Firefox". The browser's address bar contains "kxi.gov". The page header includes "XKEYSCORE" and a warning: "Warning: your password has expired!". The main content area is titled "Search: Full Log" and displays a search result for a query named "Full Log". The justification for the search is "(TS//SI//REL) Looking for 72Sec traffic to perform vulnerability assessment." The search parameters include a date range from 2011-04-03 00:00 to 2011-04-05 00:00. The results table lists various fields: Client IP (X-Forwarded-For), DVRG MAC, DVSS PID, WLAN Channel, WLAN BSSID, WLAN BSSID, WLAN DMAC, WLAN SMAC, SSAC, and SPF SLLT. Two IP addresses in the results are circled in red. The footer of the page contains the text "TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, and NZL-20251108".

∅ (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.gm [redacted] | Google

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

XK Metaviewer: 84.11.25.13... Standard Form NKB Disco Route https://ncmd...248823581254

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

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

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

Navigation Filter [redacted] vpn

Search Wizard

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

Help Actions Reports View Map View

Signal	Casematlon	Datetime	Datetime E	Fin Port	Fin City (IP)	Fin Co	Fin IP	To IP	To Cnty	To City (IP)	To Port	Application	AppID (+Fingerprints)
UKJ-260D	KI DAP0001M1100	2011-04-03 00:00:52	2011-04-03 0 0								0	vn!esp	vn!esp nac/vpn!rtr/ocole!sp
UKJ-260D	KLDAP0001M1100	2011-04-03 00:05:52	2011-04-03 0 0								0	vn!esp	vn!esp nac/vpn!rtr/ocole!sp
UKJ-260D	KLDAP0001M1100	2011-04-03 00:06:52	2011-04-03 0 0								0	vn!esp	vn!esp nac/vpn!rtr/ocole!sp
UKJ-260D	KLDAP0001M1100	2011-04-03 00:09:52	2011-04-03 0 0								0	vn!esp	vn!esp nac/vpn!rtr/ocole!sp
UKJ-260D	KLDAP0001M1100	2011-04-03 00:12:52	2011-04-03 0 0								0	vn!esp	vn!en nac/vpn!rtr/ocole!sp
UKJ-260D	KLDAP0001M1100	2011-04-03 00:15:52	2011-04-03 0 0								0	vn!esp	vn!esp nac/vpn!rtr/ocole!sp
UKJ-260D	KLDAP0001M1100	2011-04-03 00:18:52	2011-04-03 0 0								0	vn!esp	vn!esp nac/vpn!rtr/ocole!sp
UKJ-260D	KLDAP0001M1100	2011-04-03 00:21:52	2011-04-03 0 0								0	vn!esp	vn!esp nac/vpn!rtr/ocole!sp
UKJ-260D	KLDAP0001M1100	2011-04-03 00:22:01	2011-04-03 500								500	vn!es!skmp	vn!es!skmp vn!es!sec!s!skmp!main_model!ev_exchange_message_vpn!re_4_vpn!es!skmp_cone...
UKJ-260D	KLDAP0001M1100	2011-04-03 00:24:52	2011-04-03 0 0								0	vn!esp	vn!esp nac/vpn!rtr/ocole!sp
UKJ-260D	KLDAP0001M1100	2011-04-03 00:27:52	2011-04-03 0 0								0	vn!esp	vn!esp nac/vpn!rtr/ocole!sp
UKJ-260D	KI DAP0001M1100	2011-04-03 00:30:52	2011-04-03 0 0								0	vn!esp	vn!en nac/vpn!rtr/ocole!sp
UKJ-260D	KLDAP0001M1100	2011-04-03 00:33:52	2011-04-03 0 0								0	vn!esp	vn!esp nac/vpn!rtr/ocole!sp
UKJ-260D	KLDAP0001M1100	2011-04-03 00:36:52	2011-04-03 0 0								0	vn!esp	vn!esp nac/vpn!rtr/ocole!sp
UKJ-260D	KI DAP0001M1100	2011-04-03 00:39:52	2011-04-03 0 0								0	vn!esp	vn!en nac/vpn!rtr/ocole!sp
UKJ-260D	KLDAP0001M1100	2011-04-03 00:42:52	2011-04-03 0 0								0	vn!esp	vn!esp nac/vpn!rtr/ocole!sp
UKJ-260D	KLDAP0001M1100	2011-04-03 00:45:52	2011-04-03 0 0								0	vn!esp	vn!esp nac/vpn!rtr/ocole!sp
UKJ-260D	KI DAP0001M1100	2011-04-03 00:51:52	2011-04-03 0 0								0	vn!esp	vn!en nac/vpn!rtr/ocole!sp
UKJ-260D	KLDAP0001M1100	2011-04-03 00:54:52	2011-04-03 0 0								0	vn!esp	vn!esp nac/vpn!rtr/ocole!sp
UKJ-260D	KI DAP0001M1100	2011-04-03 00:57:52	2011-04-03 0 0								0	vn!esp	vn!esp nac/vpn!rtr/ocole!sp
UKJ-260D	KLDAP0001M1100	2011-04-03 01:00:52	2011-04-03 0 0								0	vn!esp	vn!esp nac/vpn!rtr/ocole!sp
UKJ-260D	KLDAP0001M1100	2011-04-03 01:06:31	2011-04-03 0 0								0	vn!esp	vn!esp nac/vpn!rtr/ocole!sp
UKJ-260D	KLDAP0001M1100	2011-04-03 01:07:50	2011-04-03 500								500	vn!es!skmp	vn!es!skmp vn!es!sec!s!skmp!main_model!ev_exchange_message_vpn!re_4_vpn!es!skmp_cone...
UKJ-260D	KLDAP0001M1100	2011-04-03 01:09:53	2011-04-03 0 0								0	vn!esp	vn!esp nac/vpn!rtr/ocole!sp
UKJ-260D	KLDAP0001M1100	2011-04-03 01:12:53	2011-04-03 0 0								0	vn!esp	vn!en nac/vpn!rtr/ocole!sp
UKJ-260D	KLDAP0001M1100	2011-04-03 01:15:53	2011-04-03 0 0								0	vn!esp	vn!esp nac/vpn!rtr/ocole!sp
UKJ-260D	KI DAP0001M1100	2011-04-03 01:18:53	2011-04-03 0 0								0	vn!esp	vn!en nac/vpn!rtr/ocole!sp
UKJ-260D	KLDAP0001M1100	2011-04-03 01:21:53	2011-04-03 0 0								0	vn!esp	vn!esp nac/vpn!rtr/ocole!sp
UKJ-260D	KLDAP0001M1100	2011-04-03 01:24:53	2011-04-03 0 0								0	vn!esp	vn!esp nac/vpn!rtr/ocole!sp
UKJ-260D	KLDAP0001M1100	2011-04-03 01:30:53	2011-04-03 0 0								0	vn!esp	vn!esp nac/vpn!rtr/ocole!sp
UKJ-260D	KLDAP0001M1100	2011-04-03 01:33:53	2011-04-03 0 0								0	vn!esp	vn!esp nac/vpn!rtr/ocole!sp
UKJ-260D	KI DAP0001M1100	2011-04-03 01:36:53	2011-04-03 0 0								0	vn!esp	vn!en nac/vpn!rtr/ocole!sp
UKJ-260D	KLDAP0001M1100	2011-04-03 01:39:53	2011-04-03 0 0								0	vn!esp	vn!esp nac/vpn!rtr/ocole!sp
UKJ-260D	KI DAP0001M1100	2011-04-03 01:42:53	2011-04-03 0 0								0	vn!esp	vn!en nac/vpn!rtr/ocole!sp
UKJ-260D	KLDAP0001M1100	2011-04-03 01:45:53	2011-04-03 0 0								0	vn!esp	vn!esp nac/vpn!rtr/ocole!sp

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

job_58922_089756700130826380_1

This system is added for ...551218 and Human's Profile Account: hvc

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

XK Metaviewer: CREAKSTILE_HW_PK - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.kxscore.com

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

XK Results XK Metaviewer: CREAKSTILE... Query Results

This system is locked for _5012 19 and Huma Rights Act compliance
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

XKEYSCORE Welcome new! Warning: your password has expired! Log Out

Home Search Workload Centre Results Fingerprints Stategies Map My Account XK Forum

Navigation Filter

Search Wizard

- CNE
- Classic
- MultiSearch
- Classic AM
 - Alert
 - BlackBerry
 - Call Logs
 - Category DNI
 - Cellular DNI
 - Cisco Passwords
 - Client
 - DNS
 - Document Metadata
 - Document Tagging
 - Email Addresses
 - Extracted Files
 - Full Log DNI
 - Geo Info
 - HTTP Activity
 - IKE Parser
 - Keylogger
 - Logins and Password
 - Machine Info
 - Microplugin Metadata
 - Obfuscation/Munged
- Classic NZ
 - Network Information
 - Network Logs
 - PILBEAM
 - PPF VoIP Metadata
 - Passports from Image
 - Phone Number Extract
 - RBCAN
 - RTP
 - Radius Logs
 - Registry
 - SIP
 - SSH Parser
 - SSL Parser
 - Shellcode
 - TDI
 - TIP/Off Collection
 - Topic / Tech Strings
 - User Activity
 - User Activity (NewExp)

Histogram Grid

Page 1 of 1 Clear Selection Expon

Filter	Fm IP	To IP	Count
			22
			22
			63
			28

CREAKSTILE_HW_PK

Help Actions Reports View Map View FILTERS: [X] [Y] [Z]

Id	State	D	Classification	Sigad	Case notation	Datetime	Fm Port	Fm City (IP)	Fm Co	Fm IP	To IP	To Cou	To City (IP)	To Port	Application	AppID (+Fingerprints)
1		271	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I, UKC-302A	PKCSE030A000HD0		2011-04-01 00:41:04	500							500	vpn/isakmp	vpn/isakmp vpn/isakmp_content/vpn/isakmp_content
2		263	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I, UKC-302A	PKCSE030A000HD0		2011-04-01 00:41:04	500							500	vpn/isakmp	vpn/isakmp vpn/isakmp_chase1_policy
3		264	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I, UKC-302A	PKCSE030A000HD0		2011-04-01 00:41:04	500							500	vpn/isakmp	vpn/isakmp vpn/isakmp_chase1_policy
4		254	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I, UKC-302A	PKCSE030A000HD0		2011-04-01 00:41:04	500							500	vpn/isakmp	vpn/isakmp vpn/isakmp_content/vpn/isakmp_content
5		261	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I, UKC-302A	PKCSE030A000HD0		2011-04-01 00:46:33	500							500	vpn/isakmp	vpn/isakmp vpn/isakmp_content
6		262	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I, UKC-302A	PKCSE030A000HD0		2011-04-01 00:46:33	500							500	vpn/isakmp	vpn/isakmp vpn/isakmp_content
7		259	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I, UKC-302A	PKCSE030A000HD0		2011-04-01 00:49:00	500							500	vpn/isakmp	vpn/isakmp vpn/isakmp_content
8		260	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I, UKC-302A	PKCSE030A000HD0		2011-04-01 00:49:00	500							500	vpn/isakmp	vpn/isakmp vpn/isakmp_content
9		265	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I, UKC-302A	PKCSE030A000HD0		2011-04-01 01:45:31	500							500	vpn/isakmp	vpn/isakmp vpn/isakmp_content
10		266	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I, UKC-302A	PKCSE030A000HD0		2011-04-01 01:45:31	500							500	vpn/isakmp	vpn/isakmp vpn/isakmp_content
11		267	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I, UKC-302A	PKCSE030A000HD0		2011-04-01 02:42:40	500							500	vpn/isakmp	vpn/isakmp vpn/isakmp_content
12		260	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I, UKC-302A	PKCSE030A000HD0		2011-04-01 02:42:40	500							500	vpn/isakmp	vpn/isakmp vpn/isakmp_content
13		162	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I, UKC-302A	PKCSE007A000HD0		2011-04-01 03:27:00	500							500	vpn/isakmp	vpn/isakmp vpn/device/ipsec/vpn/isakmp_chase
14		237	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I, UKC-302A	PKCSE007A000HD0		2011-04-01 03:27:00	500							500	vpn/isakmp	vpn/isakmp vpn/device/ipsec/vpn/isakmp_chase
15		271	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I, UKC-302A	PKCSE007A000HD0		2011-04-01 03:27:30	500							500	vpn/isakmp	vpn/isakmp vpn/isakmp_content/vpn/isakmp_content
16		272	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I, UKC-302A	PKCSE007A000HD0		2011-04-01 03:27:30	500							500	vpn/isakmp	vpn/isakmp vpn/isakmp_content/vpn/isakmp_content
17		163	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I, UKC-302A	PKCSE030A000HD0		2011-04-01 03:34:32	500							500	vpn/isakmp	vpn/isakmp vpn/isakmp_content
18		226	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I, UKC-302A	PKCSE030A000HD0		2011-04-01 03:34:32	500							500	vpn/isakmp	vpn/isakmp vpn/isakmp_content
19		1	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I, UKC-302A	PKCSE007A000HD0		2011-04-01 03:38:52	500							500	vpn/isakmp	vpn/isakmp vpn/isakmp_content
20		2	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I, UKC-302A	PKCSE007A000HD0		2011-04-01 03:38:52	500							500	vpn/isakmp	vpn/isakmp vpn/isakmp_content
21		11	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I, UKC-302A	PKCSE030A000HD0		2011-04-01 07:15:29	500							500	vpn/isakmp	vpn/isakmp vpn/isakmp_content
22		247	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I, UKC-302A	PKCSE030A000HD0		2011-04-01 07:15:29	500							500	vpn/isakmp	vpn/isakmp vpn/isakmp_content
23		175	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I, UKC-302A	PKCSE030A000HD0		2011-04-01 08:24:36	500							500	vpn/isakmp	vpn/isakmp vpn/isakmp_content
24		220	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I, UKC-302A	PKCSE030A000HD0		2011-04-01 08:24:36	500							500	vpn/isakmp	vpn/isakmp vpn/isakmp_content
25		3	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I, UKC-302A	PKCSE030A000HD0		2011-04-01 08:24:38	500							500	vpn/isakmp	vpn/isakmp vpn/isakmp_content

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

Displaying 1 - 50 of 296

jh_50122_006624000130394635_1

This system is locked for _5012 19 and Huma Rights Act compliance
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

https://xks-cep/tral.com.nsa/.../meta/metadata/list?toipurlid=h_50122_00966240001303946355_1#

(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'

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

NKB Disco Route - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://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 it man test tag in results. Query History:

collapse Results by: stamefalged

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 1.2.3.4/24 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 B - BGP D - Show CDP G - GPRS H - TAO 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

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

Session ID:

Clear Panel

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

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	Source IP	S Count	S City	Session	Quality	SPort	DPort	B
CW_SMS		20091229	huawei	USD-1031TE	MNDAQ						4432	18	00023	12480	
CW_SMS		20091215	huawei	USD-1031TE	MNDAQ						25956	20	00023	13320	
CW_SMS		20091215	huawei	USD-1031TE	MNDAQ						25956	20	00023	13320	
		20091119	cisco	USD-1031TE	MNDAQ						98	9	00023	13429	
A6VPN		20091022	huawei	USF-790	SCDVS000001MWC	M					23955	51	00023	01327	
A6VPN		20091022	huawei	USF-790	SCDVS000001MWC	R					17894	55	00023	01327	
A6VPN		20091013	huawei	USF-790	SCDVS000001MWC	R					8503	47	00023	01059	
		20091002	huawei	USD-1031TE	MNDAQ						57299	1	23	13332	
		20090910	huawei	USD-1031TE	MNDAQ						4210	1	23	15973	
		20090910	huawei	USD-1031TE	MNDAQ						4955	1	23	15941	
		20090615	huawei	USF-790	SCDVS000001MWC						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 - 30

Keyword: XVL Summary Vac Query Parameters Open a New Window

```
password cipher 2S {S1EA, 3S, 4#C3YB01!}
service-type telnet terminal
level 2 .I .L
#
ike proposal 10
 encryption-algorithm 3des-cbc
 dh group21 .H .
#
ike peer peer-nq
 exchange-mode aggressive
 pre-shared-key Key4C.ba-A6
 id-type name
 remote-address [REDACTED]
 nat traversal
 peer multi-sunset.I.V..
!
ipsec proposal proposal_gh2
 esp authentication-algorithm sha
```

Powered by the SIGDEV Lab
Version Number: 2.14 New!
Last Modified Date: March 14, 2011
Last Reviewed Date: March 14, 2011
Content Steward: [REDACTED] SSG21, 989-1341
Page Publisher: [REDACTED] COM: SSG21, 989-0342

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

Find: [] Prev Next Highlight all Match case

Done

DiscoRoute Combined Query

Submit | CSV | Tips: This is the new DISCOURTE webserver. Update any bookmarks to bring you here. | Query History:

Text Query: U'AAAI

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

Vendor: Cisco Huawei Infinet Juniper Mikrotik Tenorswitch

IP Address: | IP Address Search: Interfaces - Subnet Static Route IP Access Lists Routing Protocol IP Exact IP Search IP Header FROMTO Interfaces - Exact Anywhere else in the XML

Manifest Cisco Only: A - EQUANT I - Show Interfaces V - Voip K - Crypto Keys H - Show Run D - Show CDP M - Multihop T - Tacacs G - GPRS N - Tgt Nat Service V - Show Versions H - TAC Pop O - OSPF

Detailed Combined Command Results

Hostname	Model	DOI	Vendor	Serial	Date	Manifest	IOS Image	Source IP	S Count	S City	Session	Qualif	S Port	D Port
VPND1-UNAMI-B		2003-06-08T	cisco	UKC-125W	G2B70D0001MWC	_____K__P_R_____				RESERVED	109450	78	23	61470
GILAT-HRT5826	c2900	2003-10-15T	cisco	UKC-125W	G2B82D0001MWC	_____D__K__R_T_____	c2900-advs			RESERVED	134422	75	00023	03019
GILAT-HRT5826	c2900	2003-10-31T	cisco	UKC-125W	G2B82D0001MWC	_____D__K__R_____	c2900-advs			RESERVED	36202	75	00023	02012
kuw-hub		2003-10-15T	cisco	UKC-125W	G2B6900001MWC	_____D__K__R_____				RESERVED	32973	74	00023	50534
kuw-hub		2003-10-15T	cisco	UKC-125W	G2B6900001MWC	_____D__K__R_____				RESERVED	32973	74	00023	50534
kuw-hub		2003-10-15T	cisco	UKC-125W	G2B73D0001MWC	_____D__K__R_____				RESERVED	30000	74	00023	50534
VPND2-UNAMI-K		2003-03-10T	cisco	UKC-125W	G2B82D0001MWC	_____D__K__R_____	c2800nm-ad			RESERVED	59380	73	23	3408
fundam-k-kuw-hub		2003-01-16T	cisco	UKC-125W	G2B6900001MWC	_____D__K__R_____				RESERVED	26342	71	23	59228
ISP02-UNAMI-LAP		2003-07-23T	cisco	US-957J	1A4-116337454200	_____B__K__O_P_R_____				DUBAI	29572	71	23	27714
ldr01-unami-klr		2003-08-07T	cisco	UKC-125W	G2B70D0001MWC	_____K__P_R_____				DUBAI	23927	89	23	64278
ldr01-unami-mc	c2800nm	2010-05-22T	cisco	UKC-125W	G2B67D0001MWC	_____K__N__P_R_____	c2800nm-ad			RESERVED	40254	88	00023	44038

Powered by the SIGDEV Lab

```
*****
*
*          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
*
g(
*
* FEAT.RES
```

Powered by the SIGDEV Lab
Version Number: 2.14 New
Last Modified Date: March 10, 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

AUS, CAN, GBR, NZL

AUS, CAN, GBR, NZL

(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]