

AlliedWare

How To | Create an X.509 Certificates VPN Between an Allied Telesis Router and a Windows XP Client

Introduction

In commonly deployed IPsec VPN solutions, ISAKMP (Internet Security and Key Management Protocol) is used to dynamically establish the Security Associations and provide key management for VPN encryption. Public key techniques or, alternatively, a pre-shared key, are used to mutually authenticate the communicating parties.

This solution uses X.509 certificates to provide a public key technique to seed the ISAKMP negotiation between the VPN access concentrator (AT router) and VPN remote host (XP Computer), thus providing a more secure authentication method than the alternate practice of using a pre-shared key. For security, the certificates must be signed by a trusted third party - the Certificate Authority. In addition, at the PPP level of this VPN solution, users are authenticated using CHAP authentication to a user database.

List of terms:

RSA Key Pair

A Key Pair are the encryption keys in an Asymmetric encryption algorithm. The pair contains a public and a private key. The special properties of the keys is that data which is encrypted with the public key can be decrypted with the private key. A device will distribute its public key to other devices, but keep its private key secret. Other devices will use the public key to encrypt data being sent to the holder of the private key. RSA is a popular asymmetric encryption algorithm.

Digital Certificate

A document that states who owns a given encryption key. The document contains the digital signature of a mutually trusted certificate authority.

Digital Signature

A number that can be appended to any electronic document. The number is an algorithmic hash of the document contents, that is then encrypted with a unique encryption key.

What information will you find in this document?

This How To Note begins with the following information:

- "Related How To notes" on page 2
- "Which products and software version does it apply to?" on page 2

Then it describes the configuration, in the following sections:

- "Solution setup" on page 5
- "Solution task details" on page 8
- "Caveat statement" on page 51
- "Appendix" on page 52

Related How To notes

VPN how to Allied Telesis offers How To Notes with a wide range of VPN solutions, from quick and simple solutions for connecting home and remote offices, to advanced multi-feature setups. Notes also describe how to create a VPN between an Allied Telesis router and equipment from a number of other vendors.

For a complete list of VPN How To Notes, see the Overview of VPN Solutions in How To Notes in the How To Library at www.alliedtelesis.com/resources/literature/howto.aspx.

Which products and software version does it apply to?

This Note applies to the following Allied Telesis routers and managed Layer 3 switches:

- AR415, AR440, AR441, AR442, and AR700 series routers.
- Rapier series switches
- Software versions: 291.19+

Solution overview

Hardware and software used in this solution

This solution was tested on an AR442 running software maintenance release 291-19. Also, Linux version 2.6.8.1-12mdk and OpenSSL version 0.9.7d were used.

The certificates required in this solution are for the following roles:

- I. Certificate Authority (CA) this is the trusted certificate
- 2. VPN access concentrator Allied Telesis router (validated by CA)
- 3. VPN remote host Windows XP client (validated by CA)

The **Certificate Authority** role can be provided by a Linux Server, a Windows Server, or a third party Certificate Authority paid service.

This solution uses a Linux Server as the Certificate Authority.



Security features

The security features in this solution include:

Encryption

Encryption provides data confidentiality, preventing interpretation of captured packets without the encryption key.

User and data origin authentication

- Public key certificates along with IPsec ESP provide a convenient, reliable method for verifying the identity of a sender, and provide per-packet data origin authentication.
- Centralized authentication and accounting can be provided with RADIUS.

L2TP/IPSec connections provide stronger authentication by requiring both computer-level authentication through certificates and user-level authentication through a PPP authentication protocol.

• Source Address Management.

Data integrity

Data integrity (proof that the data was not modified in transit).

Attack protection

- PPP authentication exchange is encrypted making off-line dictionary attacks much more difficult.
- Replay protection (prevention from resending a stream of captured packets).

Solution setup

The following paragraphs describe the process of setting up a certificate VPN solution. It is not possible to set up one device in it's entirety before moving to the next device. Some steps have pre-requisite steps on another device. Given that the sequential steps involve moving from one device to an other, each step has been **colour coded** to help you identify which device the step applies to.

Color coding The color codes for each device are as follows:

Certificate Authority (CA)	VPN access concentrator -	Windows XP - VPN remote	
	Router	host	

Solution tasks - sequential steps

Perform the tasks as listed in the tables below. Each task is described in detail at the end of this section in "Solution task details" on page 8.

On the CA		
Task A	Locate OpenSSL tool and set up directories.	
Task B	Generating the CA's Public /Private Key Pair and its own public X.509 certificate.	
Task C	Make a copy of certificate file with the file extension expected by the router. Transfer certificate files to a directory ready for transfer to router and XP host.	

On the Router				
Task D	sk D Creating a Security Officer user and enabling System Security mode.			
Task E	Adding the CA's public certificate into the PKI Certificate database and setting as trusted.			
Task F	Generating a RSA Public /Private Key Pair.			
Task G	Generating a Certificate Signing Request for the router's own certificate.			

On the CA		
Task H	Receiving a Certificate Signing Request from the router, which it will sign to produce the	
	router's public certificate.	

On the Router		
Task I	Adding the router's own certificate into the PKI Certificate database, and checking it is validated and trusted.	
Task J	Configuring the network and a VPN Server facility.	
Task K	Configure a firewall.	

On the \	On the VPN remote host		
Task L Set-up an MMC Certificates Console to manage your certificates.			
Task M	Download the CA's Certificate to the Windows XP - VPN remote host.		
Task N	Import the CA Certificate to the Trusted Root Certification Authority Store.		

On the CA		
Task O	Generating a Certificate Signing Request on behalf of the Windows XP - VPN remote host.	
Task P	Produce the Windows XP Public Certificate which the Windows XP - VPN remote host can import to its Certificate Registry.	
Task Q	Converting the Windows XP certificate to a form that includes a Private Key.	

On the VPN remote host		
Task R	Download and import the Windows XP-VPN remote host Certificate to the Certificate Registry.	
Task S	Setting Up the Windows XP Client VPN Network Connection.	

On the Router		
Task T	Verification of VPN Connection from Router viewpoint.	

Summary of trust relationship that the certificates create

Just for clarity, here is a brief overview of what is being done by the above tasks to get the right certificates in the right places, and how that enables the VPN access concentrator and the remote VPN client to trust each other's encryption keys.

- 1. Create a root CA certificate on the Certificate Authority server. (Task B)
- Load the root CA certificate into the Trusted Root CA certificate lists on both the VPN access concentrator and the remote VPN client, so they both agree that they trust this CA. (Task B and M)
- On the VPN access concentrator, create an RSA keypair, and then create an unsigned certificate to verify the VPN access concentrator's ownership of that RSA keypair. (Task F and G)
- 4. Upload the unsigned certificate to the CA server. The CA server signs the certificate, and the new, signed, version of the certificate is loaded back onto the VPN access concentrator. (Task H and I)

- 5. The VPN access concentrator now has a certificate, verifying its ownership of its RSA keypair, signed by a certificate authority that the remote VPN client also trusts.
- 6. On the CA server, create an RSA keypair, and a signed certificate for that keypair, on behalf of the remote VPN client. (Task O and P)
- 7. Combine the RSA keypair and the signed certificate into a single file, and load them onto the remote VPN client. (Task Q and R)
- 8. The remote VPN client now has its own RSA keypair, and a certificate verifying its ownership of that RSA keypair. The certificate is signed by a CA that the VPN access concentrator trusts.
- 9. Then, when the VPN access concentrator and remote VPN client want to exchange encrypted data, they will send their public encryption keys to each other. When each device sends data to the other, it will be expected to encrypt the data using the public key it received from that other device. The VPN access concentrator and remote VPN client each trust that the other device is the true owner of the public key that it sent, as they also send each other certificates that verify that they are the true owners of those RSA encryption keys. The VPN access concentrator and remote VPN client trust each others' certificates because the certificates are both signed by the CA server, and they have both loaded the CA server's certificate into their list of trusted CAs.

Solution task details

On the O	On the CA	
Task A	Locate OpenSSL tool and set up directories	
	At the Linux BASH prompt ensure you have access to the openssl tool:	
	"whereis openssl" or "locate openssl", after "updatedb"	
	This solution was documented using version 0.9.7a:	
	[root@localhost certificates]# openssl version	
	OpenSSL 0.9.7a Feb. 19 2003	
	If you cannot locate the openssl tool it may need to be installed on your system.	
	Once installed "man openssl" provides the manual describing usage of the openssl tool.	
	It is recommended that you create a directory for handling certificates, and another for handling the CA's certificates:	
	"mkdir certificates", "cd certificates", "mkdir ca"	

Task B Create the CA's Public /Private Key Pair and its Public X.509 certificate Once created, this certificate can be freely distributed to the VPN peers and any other security device (member entity) who trusts this CA and whose certificates will be signed by this CA. The CA's certificate contains the CA's public key. **Create the CA certificate:** Use the **OpenSSL tool**, (as described in Task A, change to the "certificates" directory with "ca" as the child directory). [root@multibox URLcerts]# openssl req -x509 -new -out ca/cacert.crt -keyout ca/cakey.key -days 9999 This will start a sequence of prompts, an example of which is given here: [root@multibox URLcerts]# openssl req -x509 -new -out ca/cacert.crt -keyout ca/cakey.key -days 9999 Generating a 1024 bit RSA private key + + + + + ++++++++ writing new private key to 'ca/cakey.key' Enter PEM pass phrase: Verifying - Enter PEM pass phrase: You are about to be asked to enter information that will be incorporated into your certificate request. What you are about to enter is what is called a Distinguished Name or a DN. There are quite a few fields but you can leave some blank For some fields there will be a default value, If you enter '.', the field will be left blank. Domain Component 1 (e.g. nz) [nz]: Domain Component 2 (e.g. co) [co]: Domain Component 3 (e.g. alliedtelesis) [alliedtelesis]: Country Name (2 letter code) [NZ]: State or Province Name (full name) [Canterbury]: Locality Name (eg, city) [Christchurch]: Organization Name (eg, company) [YourCompany]: Organizational Unit Name (eg, section) [OUN]:CSG Common Name (eg, YOUR name) [YourName]:CA-Cert Email Address []:. You will note the OpenSSL tool can be used to prompt for other Distinguished Name fields such as the Domain Component fields seen above. Your installation of OpenSSL might not be customised to prompt for these fields. You can make OpenSSL prompt these fields by adjusting the configuration file. Please see the appendix at the end of this document for an example of how to do that. Confirm that the certificate file has been created: [root@multibox URLcerts]# ls ca -lct total 8 -rw-r--r-- I root root 1444 May 21 14:21 cacert.crt -rw-r--r-- I root root 963 May 21 14:21 cakey.key Use OpenSSL to view the fingerprint for confirmation purposes: [root@multibox URLcerts] # openssl x509 -in ca/cacert.crt -SHA1 -

[rootemultibox ORLCerts]# openss1 x509 -in Ca/CaCert.Crt -SHAI fingerprint|more
SHA1
Fingerprint=75:DE:E3:C5:66:93:1D:35:6A:B1:C5:B2:A2:53:64:E3:2B:D9:9
7:73

Task C	Make a copy of certificate file with the file extension expected by the router. Transfer certificate files to a directory ready for transfer to router and XP host.
	On the router, the certificate file must have a .cer extension.
	 Make a copy of the file with the .cer extension.
	 Move or copy the file to the appropriate TFTP, FTP, or ZMODEM directory, ready for download to the router and to the Windows XP client: [root@multibox URLcerts]# cp ca/cacert.crt /root/cacert.cer
	The relevant cacert file can then be transferred to the Windows XP Computer, using a file transfer protocol such as TFTP, FTP, or ZMODEM.
	Examples of loading the certificate onto the router by ZMODEM and by TFTP are shown below in Task E - Add the CA's public certificate into the PKI Certificate database and set as trusted.

Task D	Create a Security Officer user and enable System Security mode.				
	Manager > add user=secoff pass=	secoff priv=sec	2		
	Manager > login secoff				
	SecOff > set sys name="Certific	ate VPN demo"			
	Info (1034003): Operation succe	sstul.			
	Secoli Certificate VPN demo> en	able system sec	curity		
	Secoli Certificate VPN demos se	t user securede	21ay=000		
Task E	Add the CA's public certificate into	the PKI Certifica	te database and	l set as	
	trusted.				
	 As mentioned above in Task C - "Make expected by the router", the CA's cert 	e a copy of certificat tificate needs to be	e file with the file transferred on the	extension e router.	
	 This step shows a choice of loading the server. 	e certificate file using	g ZMODEM or fr	om a TFTP	
	Loading by ZMODEM				
	SecOff Certificate VPN demo> load m	ethod=zmodem asyn	n=0		
	Router ready to begin ZMODEM file transfers B010000023be50				
	On terminal emulator, initiate ZMODEM send of file cacert.cer to the router				
	Info (1048293): ZMODEM, session ove	r.			
	Loading by TFTP				
	SecOff Certificate VPN demo> load fi=cacert.cer serv=10.33.26.11				
	Info (1048270): File transfer successfully completed.				
	Add the downloaded file to the PKI Certificate Database				
	SecOff Certificate VPN demo> add pki cert=cacert location=cacert.cer type=ca				
	Info (1095003): Operation successful.				
	SecOff Certificate VPN demo> set pki cert=cacert trusted=true				
	SecOff Certificate VPN demo> sh pki cert				
	Certificate Database: [ref.#: 14108-1412]				
	Name	State	MTrust Type	Source	
	cacert	TRUSTED	TRUE CA	- COMMAND	

Task E	View the certificate and the fingerprint for confirmation purposes.
continued	SecOff Certificate VPN demo> sh pki cert=cacert
	Certificate:
	manually trusted TRUE
	type CA
	source COMMAND
	version V3 serial number
	signature alg MD5 with RSA
	public key alg RSA
	not valid before 02:21:16 - 21-May-2009 (GMT)
	not valid after 02:21:16 - 05-Oct-2036 (GMT)
	<pre>subject cn=CA-Cert, ou=CSG, o=YourCompany,</pre>
	l=Christchurch, st=Canterbury, c=NZ, dc=alliedtelesis, dc=co, dc=nz
	l=Christchurch, st=Canterbury, c=NZ, dc=alliedtelesis, dc=co, dc=nz
	MD5 fingerprint c6a9 d973 cdda c5de a58d 427c bd50 0b72 SHA1 fingerprint 75de e3c5 6693 1d35 6ab1 c5b2 a253 64e3 2bd9
	9773
	Sace Key fingerprint 90e8 4fla 2ell 2063 b4/e 9c22 b800 /3bf e859
	key usage basic constraints subject type CA
	path length No constraint
	subject key ID ba5f4ace3993a8acb23dd6ec96d8bad9b301498c
	authority key ID ba5f4ace3993a8acb23dd6ec96d8bad9b301498c
	validation path [manually trusted, self-signed] Source Location:
	file cacert.cer
	This certificate is valid. The SHA fingerprint of the CA certificate loaded on the router's PKI database matches the fingerprint that we generated on Linux using OpenSSL.
	Optionally add the Certificate Revocation List file:

load file=ca_crl.crl server=10.33.26.11
add pki crl=ca_crl location=ca_crl.crl

Task F	Creating a RSA Public/Private Key Pair
	SecOff Certificate VPN demo> create enco key=1 type=rsa length=512
	Info (1073278): RSA Key Generation process started.
	Info (1073279): RSA Key generation process completed.
	SecOff Certificate VPN demo> sh enco key
	ID Type Length Digest Description Mod IP
	1 RSA-PRIVATE 512 739DAC6B

In Task F, we created an RSA public and private key. Now we need to request that the CA sign a certificate to validate the router's ownership of this RSA public/private key pair.

First it is necessary to set the distinguished name on the router to be the same as that used by the CA.

Create a Certificate	Signing Reque	st for the r	outer's own certif	ficate	
Certificate VPN de	mo> set syst	em dist="e	em=test@solutior	n.net,	
cn=router-ATI, ou=	CSG_Lab, o=A	llied Tele	esis, l=Christch	nurch,	
st=Canterbury, c=N	Ζ"				
Then create an enrolme	nt request for ke	ypair I (note	e that in Task F, the ID	D 'l' was specifie	ed
when creating the keys).					
SecOff Certificate	VPN demo> c:	reate pki			
enrollmentrequest=	rou_request 1	keypair=1	prot=manual typ	pe=pkcs10	
format=pem					
Info (1095265): PK	I Management	Request 1	rou_request Comp	pleted.	
The enrolment request i	s actually an unsi	igned certific	ate, that now needs	to be sent to th	he
CA to be signed.	,	•			
SecOff Certificate	VPN demo> s	h fi=*.cs:	<u>c</u>		
Filename	Device	Size	Created	Lock	s

On the CA

Task H	Receiving the Certificate Signing Request from the router, which it will sign to produce the router's public certificate
	 On the router, upload the signing request by TFTP.
	SecOff Certificate VPN demo> upload fi=rou_request.csr serv=10.33.26.11
	• On the CA, sign the certificate, based in the router's request.
	<pre>[root@multibox URLcerts]# openssl x509 -req -in rou_request.csr -CA ca/cacert.crt -CAkey ca/cakey.key -CAcreateserial -outform PEM -out rou_cert.cer -days 9999 Signature ok</pre>
	subject=/C=NZ/ST=Canterbury/L=Christchurch/O=Allied Telesis/ OU=CSG_Lab/CN=router-ATI/emailAddress=test@solution.net Getting CA Private Key
	Enter pass phrase for ca/cakey.key:
	<pre>[root@multibox URLcerts]# ls ca/ rou_cert.cer rou_request.csr</pre>
	• This certificate can now be loaded into the router's PKI Certificate database. First, move the certificate file to the appropriate file transfer directory, ready for download to the router.
	[root@multibox URLcerts]# cp rou_cert.cer /root

On the Router

Task IAdd the router's own certificate into the PKI Certificate database, and check it
is validated and trusted.

Now that the certificate has been signed by the CA, it can be loaded back into the router. SecOff Certificate VPN demo> load method=zmodem asyn=0

Router ready to begin ZMODEM file transfersB0100000023be50

In the terminal emulator, initiate the transfer of the signed certificate rou_cert.cer Info (1048293): ZMODEM, session over.

SecOff Certifi	lcate V	PN demo>	sh f	li=*.cer			
Filename		Device		Size	Created		Locks
cacert.cer	flash		1444	21-1	May-2009	14:31:05	0
rou_cert.cer	flash		924	21-1	May-2009	14:46:17	0

Add the file as a self-authenticating certificate. The router can validate that the certificate is signed by the trusted CA:

SecOff Certificate VPN demo> add pki cert=rou_cert
location=rou_cert.cer type=self

Info (1095003): Operation successful. SecOff Certificate VPN demo> sh pki cert

Certificate Database: [ref.#: 27116-1412] Name State MTrust Type

rou_cert	TRUSTED	FALSE	SELF	COMMAND
cacert	TRUSTED	TRUE	CA	COMMAND

Source

SecOff Certificate VPN demo> sh pki cert=rou_cert

Certificate:

name	rou cert
state	<u>-</u>
manually trugted	ENLOP
manually crusted	FALSE
type	SETL
source	COMMAND
version	V1
serial number	02
signature alg	MD5 with RSA
public key alg	RSA
not valid before	02:38:37 - 21-May-2009 (GMT)
not valid after	02:38:37 - 05-Oct-2036 (GMT)
subject	em=test@solution.net, cn=router-ATI,
ou=CSG_Lab, o=Alllied Te	lesis, l=Christchurch, st=Canterbury, c=NZ
issuer	cn=CA-Cert, ou=CSG, o=YourCompany,
1=Christchurch, st=Cante:	rbury, c=NZ, dc=alliedtelesis, dc=co, dc=nz
MD5 fingerprint	978f 6bc2 fb70 25dd 5534 0e65 b089 f895
CUAl fingerprint 3	20/3 $=100$ 8266 3555 $=022$ $9=64$ 8079 1674 $786f$
70fd	1045 albe 0200 5555 C422 9ald 0979 1074 7001
key fingerprint 4	e04 ci5i 60dc 2359 aac4 dc42 0540 /caa /400
748c	
key usage	
validation path	<- cacert[manually trusted, self-signed]
Source Location:	
file	rou cert.cer

On the 🤇	CA
Task I	The router's signed certificate which has now been downloaded and added to the router
continued	PKI register can be confirmed as correctly downloaded by comparing its fingerprint with the source certificate file on the Linux CA:
	[root@multibox URLcerts]# openssl x509 -in rou_cert.cer -SHA1 - fingerprint more
	SHA1Fingerprint=30:43:A1:9E:82:66:35:55:C4:22:9A:FD:89:79:16:74:78: 6F:70:FD
	This matches correctly with the SHAI fingerprint as previously seen on the router's copy of the certificate.

On the Router

Task J	Configuring the network and a VPN access concentrator facility.
	The VLAN configuration:
	create vlan="private" vid=2
	add vlan="2" port=2-5
	The IP configuration:
	enable ip
	# VLANI is the public side
	add ip int=viani ip=10.17.90.181 $Mask=255.255.255.0$
	add ip int=vlan2 ip=172.28.4.30
	add ip rou=0.0.0.0 mask=0.0.0.0 int=vlan1 next= <gateway></gateway>
	add ip dns prim=x.x.x.x
	create ip pool="12tpclient" ip=172.28.4.31-172.28.4.32
	Create the user for the L2TP/IPSec VPN remote host:
	add user=joe pass=friend lo=no telnet=no
	As an alternative, a RADIUS Server could be configured to handle user authentication
	requests.
	Create the PPP template:
	This defines the parameter values that will be set on the dynamic PPP interface that will be attached to the router's end of the L2TP tunnel.
	create ppp template=1
	echo=60 lqr=off
	The L2TP configuration:
	enable 12tp
	enable iztp server=both
	add l2tp ip=0.0.0.1-255.255.255.254 ppptemplate=1

Task J	The ISAKMP configuration:
continued	
	create isakmp pol="keys" pe=any enc=3desouter autht=rsasig gro=2 sendd=true sendn=true
	(You could also, optionally specify the parameters 'setc=true and natt=true on the
	above command)
	enable isakmp
	The IPSec configuration:
	Create several different SA specs, so that the policy can support different security
	association combinations offered by Windows VPN remote host:
	create ipsec sas=1 key=isakmp prot=esp enc=3desouter hasha=sha set ipsec sas=1 mod=transport
	create ipsec sas=2 key=isakmp prot=esp enc=3desouter hasha=md5 set ipsec sas=2 mod=transport
	create ipsec sas=3 key=isakmp prot=esp enc=des hasha=sha set ipsec sas=3 mod=transport
	create ipsec sas=4 key=isakmp prot=esp enc=des hasha=md5
	set ipsec sas=4 mod=transport
	create ipsec bundle=5 key=isakmp string="1 or 2 or 3 or 4"
	All policies below define local port, because we expect all tunnels to be externally initiated from clients - i.e.: incoming to this router.
	The IPSec policy to allow all ISAKMP negotiation and NAT-T traffic through to their appropriate modules:
	create ipsec pol="isakmp" int=vlan1 ac=permit
	set ipsec pol="isakmp" lp=500 tra=UDP create ipsec pol="natt udp" int=ulap1 ac-permit
	set ipsec pol="natt_udp" lp=4500 tra=UDP
	The IPSec policy for L2TP tunnel:
	create ipsec pol="l2tpVPN" int=vlan1 ac=ipsec key=isakmp bund=5 peer=ANY
	set ipsec pol="l2tpVPN" lp=1701 tra=UDP
	Add a final policy that allows all other traffic to pass through - so traffic from the LAN
	behind the router can access the general Internet. If you are allowing direct Internet access, then a firewall needs to be provisioned either on this router or elsewhere on the network:
	create ipsec pol="internet" int=vlan1 ac=permit enable ipsec

On the	Router
Task	Configure the firewall.
	enable fire
	create fire policy=main
	create fire policy=main dy=dynamic
	add fire policy=main dy=dynamic user=ANY
	add fire policy=main int=viani type=private
	Dynamic private interfaces are accepted from L21P, which are from IPSec only.
	add fire policy=main int=dyn-dynamic type=private
	The firewall allows for internally generated access to the internet through the following NAT definition.
	add fire policy=main nat=enhanced int=vlan1 gblinterface=eth0
	The following NAT definition allows Internet access for remote VPN users by providing address translation
	add fire policy-main nat-enhanced int-dyn-dynamic ghlinterface-eth
	Pules L and 2 allow for ISAKMP and the "port floated" IKE/ISAKMP that NATT uses
	add fire policy=main rule=1 int=eth0 action=allow protocol=udp ip= <office address="" internet=""> port=500 gblip=<office internet<br="">address> gblport=500</office></office>
	add fire policy=main rule=2 int=eth0 action=allow protocol=udp ip= <office address="" internet=""> port=4500 gblip=<office internet<br="">address> gblport=4500</office></office>
	Rule 3 becomes the L2TP tunnel allow rule. Additional security is provided by only allowing
	traffic from IPSec tunnels.
	add fire policy=main rule=3 int=eth0 action=allow prot=udp ip= <office address="" internet=""> port=1701 gblip=<office internet<br="">address> sbloart=1701 engapeipage</office></office>
	we recommend you use secure shell for remote management. Teinet should not be used
	to a secure gateway.
	<pre>enable ssn server serverkey=2 nostkey=3 expirytime=12 logintimeout=60 add ask user apacff parameted (seconff parameted)</pre>
	add ssn user=secoll password= <secoll password=""> 1paddress=<trusted< td=""></trusted<></secoll>

On the VPN remote host

Task L Set-up an MMC Certificates Console to manage your certificates.

• From the Windows **Start** menu, select **Run...**



• In the **Run** dialogue box type **MMC**. Click **OK**.

Run	? 🗙
1	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:	mmc
	Cancel Browse

• In the MMC Console, select File > Add /Remove Snap-in...

Action View Favori	es Window Helj:	p
Vew	Ctrl+N	
Open	Ctrl+O	
Save	Ctrl+S	
Save As		Name
Add/Remove Snap-ir	Ctrl+M	Nume
Options		
. certificates.msc		
C:\WINDOWS\\compmg	mt.msc	
8 Console1.msc		
4 C:\WINDOWS\\eventvv	r.msc	
Exit		

• In the Add /Remove Snap-in dialogue box, select Add...

Standalone	Extensions	
Use this pa	ge to add or remove a standalone Snap-in from the console.	
Snap-ins ad	Ided to: 🔄 Console Root	(n)
onap ine at		

Task L

continued

• Select Certificates from the list of Snap-ins, and click Add.

and ActiveX Control	Microsoft Corporation	
Certificates	Microsoft Corporation	
Component Services	Microsoft Corporation	
Scomputer Management	Microsoft Corporation	
🔜 Device Manager	Microsoft Corporation	
💕 Disk Defragmenter	Microsoft Corp, Executi	
🛱 Disk Management	Microsoft and VERITAS	
🔟 Event Viewer	Microsoft Corporation	
Eolder	Microsoft Corporation	
🔊 Group Policy	Microsoft Corporation	-
Image: Control of the second secon	Microsoft Corporation Microsoft Corporation Microsoft Corporation	

• Select My user account, then click Finish.

There are three types of **Certificate Snap-ins** available: User, Service, and Computer. We will add **two** of them.



• Back at the Add Standalone Snap-in window, select Certificates again, and click Add. This will allow you to snap-in another Certificate type.

Snap-in	Vendor	^
r≟ActiveX Control	Microsoft Corporation	
👹 Certificates	Microsoft Corporation	
🙆 Component Services	Microsoft Corporation	
🔜 Computer Management	Microsoft Corporation	
🚚 Device Manager	Microsoft Corporation	
💕 Disk Defragmenter	Microsoft Corp, Executi	
🗃 Disk Management	Microsoft and VERITAS	
🛄 Event Viewer	Microsoft Corporation	
🚞 Folder	Microsoft Corporation	
🔊 Group Policy	Microsoft Corporation	~
Description The Certificates snap-in allows you i certificate stores for yourself, a servi	to browse the contents of the ice, or a computer.	

Task L

continued • This time, select **Computer account**, then click **Next**.

Certificates snap-in	×
This snap-in will always manage certificates for:	
O My user account	
 Service account 	
 Computer account 	
	K Back Next Cancel

• Select Local computer, then click Finish.



• Confirm that the Add/Remove Snap-in window has the two certificate types listed, then click OK.

Add/Remove Snap-in	?×
Standalone Extensions	
Use this page to add or remove a standalone Snap-in from the console.	
Snap-ins added to: 🔄 Console Root 👻	
 Certificates - Current User Certificates (Local Computer) 	
- Description	
Add Remove About	Incel

Task L

continued

• At the **MMC Console** you should now have the two certificate Snap-ins available. As shown, you can open the hierarchy of certificates.

The Console1	
File Action View Favorites Window Help	
The Console Root	
Controls Book Controls Socie Controls Socie Controls Socie Controls Socie Controls Socie Controls Cont	Name ©Centroates - Current User ©Centroates (Local Computer)

To save and create a short-cut to this MMC Console snap-in arrangement, select File > Save.

Te Console1	
Action View Favorites Window	Help
Action Vew Pavorites Window New Cristel Seg Criste Seg Criste Self Ac., Additenove Snap-In Cortist Groom 1 certificates.nec 2 Cristel Ansc. 2 Cristel Ansc. 2 Cristel Ansc. 1 certificates.nec 2 Cristel Ansc. Exe 1 Teach Pavor Red Confliction Aufor 1 Teach Pavol 1 Teach Pavol 1 Teach Pavol 1 Teach Pavol 1 Certificate Proglet 1 Certificate Pr	Help Help Help Help Help Help Help Help
Save the current console.	

• Save the msc file under the Administrative Tools folder. i.e. C:/Documents and Settings/User/Start Menu/Programs/Administrative Tools.

PAS						28
Save in:	C Administrativ	ve Took:	*	000	• 🖃 •	
ty Recent sourcents	😭 Console I. ns	¢.				
Dealitop						
Documents						
31						
Lonputer		-				
	File native.	Configuration and				Save
	Save as type.	Microsoft Manage	ment Concole File	u("mic)		Cancel

 After saving, your Certificates MMC short-cut should be available from Start > All Programs > Administrative Tools

On the VPN remote host

Task M Download the CA's Certificate to the Windows XP Client.

 Use a file transfer method such as FTP. The CA Certificate was created in the earlier section in Task B, "Generating the CA's Public /Private Key Pair and its own public X.509 certificate." on page 5

Z FileZilla - Connec	cted to Linux Right (172.28.4.11)						L	
nie Luit Hansier Vi	📰 RìO. 🛯 🎽	D 9							
2002 G"L G"F NAK		N •							
Address:	User:	Passwor	d:	Port	Quick <u>c</u> onnect				
Response: Remote w Command: LIST Response: Sucessfull Status: Directory li Command: GET cace Response: Download Status: Download	orking directory is now /ro y received 4 items sting successful rt.ctr.C:\Documents and 9 ing /root/certificates/ca/o successful	ot/certificates/ca iettings\Shayle's T acert.crt to C:\Doc	est Bay\My Docur cuments and Settir	nents\cacert.crt igs\Shayle's Te	FALSE t Bay\My Documents	\cacert.crt			
Local Site: C:\Documen	ts and Settings\Shayle's 1	est Bay\My Docur	ments\ 🗸 🗸	Remote Site	/root/certificates/ca	3/			
💷 🗐 L	ocal Settings		^	Filename	L	Filesize	Filetype	Date	Time
	ly Documents IrintHood Lecent iendTo			Cacert.co	r L V	1367 1367 3 963	Security Ce Security Ce SRL File KEY File	03/05/2009 01/05/2009 04/05/2009 01/05/2009	21:22 17:35 11:39 17:35
Filename 🛆	Filesize Filet	ype La	ast Modified 🛛 🔺	ī l					
🛅 🛅 greig OSPF 🚵 My Music	File F File F	older 14	/03/2006 12:						
<			>	<					
4 folders and 30 files with	559515 bytes.			Selected 1 fil	e with 1367 bytes.				
Local Filename		Size Direction	Remote Filenam	e	Host	2	Status		
Ready		₿						Queue: 0 byt	es 🧔 🤇

On the VPN remote host

Task N Import the CA Certificate to the Trusted Root Certification Authority Store.

- In the MMC console, select: Certificates (Local Computer) > Trusted Root Certification Authorities > Certificates
- Right-click on Certificates and select: All Tasks > Import...

🚡 certificates - [Console Root\Certifica	tes (Local Computer)\Trusted Roo	t Certif
📸 File Action View Favorites Window	Help	
Console Root Certificates - Current User Certificates (Local Computer) Personal Certificates	Issued To A BABA.ECOM Root CA Autoridad Certificadora de la Asoci Autoridad Certificadora del Colegi	Issued B ABA.ECC Autorida Autorida
Certification Authorities Certification Authorities Certificate Certificate Certificate Certificate	Belgacom E-Trust Primary CA	Baltimoré Belgacon C&W HK
Intermediate View	W HKT Bocurentet CA Class B W HKT SecureNet CA Root W HKT SecureNet CA SGC Root	C&W HK C&W HK C&W HK
	1 rtiposte Classe A Personne rtiposte Serveur	CA 1 Certipost Certipost
	rtisign - Autoridade Certificador rtisign - Autoridade Certificador	Certisign Certisign Certisign
Constant of the second se	Certisign Autoridade Certificadora Class 1 Primary CA	Certisign Class 1 P

• This will start the Certificate Import Wizard. Click Next.



• To import the CA's certificate file, click **Browse...**

Specify the file you way	et to import.
Filenanes	
1	Browne
	and the termination of the
Note: More than one o	certificate can be stored in a single file in the following format
Personal Informatio	n Exchange- PKCS #12 (, PPX, P12)
Cryptographic Mess	age Syntax Standard- PKCS #7 Certificates (.P70)
Microsoft Serialized	Certificate Store (.551)

Task N					
continued	Select	your cac	ert file. Click O	pen.	
	Open				? 🗙
	Look in:	🕒 My Document	ts 💌	G 🏚 📂 🛄-	
	My Recent Documents Desktop My Documents My Documents My Computer	greig OSPF	ces		
	S	File name:	cacert.ort	×	Open
	My Network	Files of type:	X.509 Certificate (*.cer;*.crt)	v (Cancel

• The Wizard will automatically prompt a suitable store, in this case Trusted Root Certification Authorities. Click Next.



X.509 Certificate (*.cer;*.crt)

• Confirm the settings you have selected, click **Finish** to end the Wizard, then **OK** to complete.

Certificate Import Wizard		×	
	Completing the Certificate Impo Wizard You have successfully completed the Certificate Impor weard.		
	You have specified the following set	ings: Trusted Deet Certific	
	Certificate Store Selected by User Content File Name	Trusted Root Certific Certificate C:\Documents and Se	
		>	
	< Back F	inish Cancel	

Task N

- continued
- In the Certificate MMC Console, confirm that the certificate has been imported. The certificates are sorted by the Common Name they were issued to. In this case, the trusted CA certificate for the computer will be found as follows: Certificates (Local Computer) > Trusted Root Certification Authorities > Certificates Look in the Issued To list for the CA's Common Name.

Pile Action View Favorites Wi	ndow Help			X
◆ → 🖻 🖬 🗶 🚮 🕹	9 3			
Console Root	Issued To /	Issued By	Expiration Date	Intended Purp
Certificates - Current User	ABA.ECOM Root CA	ABA.ECOM Root CA	10/07/2009	Secure Email, :
Certificates (Local Computer)	Autoridad Certificadora de la Asoci	Autoridad Certificadora de la Asocia	29/06/2009	Secure Email, :
Personal	Autoridad Certificadora del Colegi	Autoridad Certificadora del Colegio	30/06/2009	Secure Email, :
Trusted Root Certification Authority	Baltimore EZ by DST	Baltimore EZ by DST	4/07/2009	Secure Email, :
Cerencates	Belgacom E-Trust Primary CA	Belgacom E-Trust Primary CA	22/01/2010	Secure Email, :
Enterprise trus:	C&W HKT SecureNet CA Class A	C&W HKT SecureNet CA Class A	16/10/2009	Secure Email, :
Touted & blobard	COW HKT SecureNet CA Class B	C&W HKT SecureNet CA Class B	16/10/2009	Secure Email, :
Inducted Publishers	Cow HKT SecureNet CA Root	CBW HKT SecureNet CA Root	16/10/2010	Secure Email, :
E Divid Party Boot Certification &	CBW HKT SecureNet CA SGC Root	C&W HKT SecureNet CA SGC Root	16/10/2009	Secure Email, :
Trusted People	CA 1	CA1	11/03/2019	Secure Email, :
Other People	E CA-Cert	CA-Cert	5/10/2036	<ab< td=""></ab<>
Certificate Enrolment Requests	Certiposte Classe & Personne	Certiposte Classe A Personne	24/06/2018	Secure Email, :
8- 🦲 SPC	Certiposte Serveur	Certiposte Serveur	24/06/2018	Secure Email, :
	Certisign - Autoridade Certificador	Certisign - Autoridade Certificadora	27/06/2018	Secure Email, :
	Certision - Autoridade Certificador	Certisign - Autoridade Certificadora	27/06/2018	Secure Email, :
	Certisign Autoridade Certificadora	Certisign Autoridade Certificadora A	27/06/2018	Secure Email, :
	Certisign Autoridade Certificadora	Certisign Autoridade Certificadora A	10/07/2018	Secure Email, :
	Class 1 Primary CA	Class 1 Primary CA	7/07/2020	Secure Email, :
	Class 1 Public Primary Certification	Class 1 Public Primary Certification A	2/08/2028	Secure Email, •
	Class 1 Public Primary Certification	Class 1 Public Primary Certification A	8/01/2020	Secure Email,
	Class 2 Primary CA	Class 2 Primary CA	7/07/2019	Secure Email, :
	Class 2 Public Primary Certification	Class 2 Public Primary Certification A	8,01,/2004	Secure Email,
	Class 2 Public Primary Certification	Class 2 Public Primary Certification A	2,108,12028	Secure Email, 👡
< > >	4			2

 Double-click on the certificate to display its detail. It should show as a valid certificate if it is not valid, an error message will be displayed.

Certificate	? 🗙
General Details Certification Path	
Certificate Information	
This certificate is intended for the following purpose(s): •Al issuance policies •Al application policies	-
Issued to: CA-Cert	-
Issued by: CA-Cert	
Valid from 21/05/2009 to 5/10/2036	
Issuer Statemer	nt
ОК	

• Verify that the **Subject** (Distinguished Name) details are correct.

now: <all></all>	*
Field	Value
- Subject	CA-Cert, CSG, YourCompany,
🗖 Public key 😽	R5A (1024 Bits)
💽 Subject Key Identifier	ba 5f 4a ce 39 93 a8 ac b2 3d
Authority Key Identifier	KeyID=ba 5f 4a ce 39 93 a8 a
Basic Constraints	Subject Type=CA, Path Lengt sha1
Thumbprint	75 de e3 c5 66 93 1d 35 6a b1

Task N

continued

• Verify that the certificate is valid through SHAI thumbprint. It should be the same value as in Task E (Adding the CA certificate to the router's PKI Database, on page 5), and Task B (Creating the CA's Public X.509 certificate, on page 5). In this example it ends with the numbers: 97 and 73.

Certificate	?		
General Details Certification	Path		
Show: <all></all>	~		
Field	Value 🔨		
Subject Public key Subject Key Identifier Authority Key Identifier Basic Constraints	CA-Cert, CSG, YourCompany, RSA (1024 Bits) ba 5F 4a ce 39 93 a8 ac b2 3d KeyID=ba 5F 4a ce 39 93 a8 a Subiect Type=CA. Path Lengt		
Thumbprint algorithm	sha1		
	/5 de e3 c5 66 93 10 35 68 D1		
75 de e3 c5 66 93 e3 2b d9 <mark>97 73</mark>	1d 35 6a b1 c5 b2 a2 53 64		
,	Edit Properties Copy to File		
	ОК		

On the CA

Task O Creating a certificate signing request on behalf of the Windows XP VPN remote host machine.

The next steps show the process used on the Linux CA Computer, to make a certificate request on behalf of the Windows XP Client, and then signing that request to produce the certificate.

Preparation points

• Be sure to use the correct common name for the Windows XP Client. The common name must be the computer's name (for example "ClientI")

System Properties			? 🛛				
System Restore	Automa	tic Updates	Remote				
General Com	puter Name	Hardware	Advanced				
Windows uses the following information to identify your computer on the network.							
Computer description:	csg						
	For example: "I Computer".	Kitchen Computer''	or "Mary's				
Full computer name:	Client1.						
Workgroup: K	SOLUTIONS						
To use the Network Identification Wizard to join a domain and create a local user account, click Network ID ID.							
To rename this computer or join a domain, click Change. Change							
	OK	Cance	Apply				

The OpenSSL command shown in the example below uses the file openssl.cnf. This file is normally installed automatically with an OpenSSL installation. In order for the openssl command to access it, this file may need to be copied into a system PATH directory or to the current directory.

Optional Note:

The file openssl.cnf may be used to specify other certificate fields such as domain name that are not prompted by the openssl command An example of this is shown in Appendix A. on page 52

$\label{eq:constraint} \mbox{Example using Linux OpenSSL tool to make Windows XP certificate request}$

Syntax:

```
openssl req -config openssl.cnf -out name.csr -pubkey -new -keyout nameKey.pem -outform PEM -nodes
```

Example:

[root@localhost certificates]# updatedb
[root@localhost certificates]# locate openssl.cnf

Task O	This certificate request shows an example of most available Distinguished Name fields being					
continued	<pre>set, these include the Domain Component (DC) needs and the email need. [root@multibox URLcerts]# openssl req -out WindowsXP.csr -pubkey - new -keyout WindowsXPKey.pem -outform PEM -nodes Generating a 1024 bit RSA private key .++++++</pre>					
	<pre>writing new private key to 'WindowsXPKey.pem'</pre>					
	You are about to be asked to enter information that will be incorporated into your certificate request. What you are about to enter is what is called a Distinguished Name or a DN. There are quite a few fields but you can leave some blank For some fields there will be a default value, If you enter '.', the field will be left blank. Domain Component 1 (e.g. nz) [nz]: Domain Component 2 (e.g. co) [co]: Domain Component 3 (e.g. alliedtelesis) [alliedtelesis]: Country Name (2 letter code) [NZ]: State or Province Name (full name) [Canterbury]: Locality Name (eg, city) [Christchurch]: Organization Name (eg, company) [YourCompany]: Organizational Unit Name (eg, section) [OUN]:csg Common Name (eg, YOUR name) [YourName]:Client1 Email Address []:test@solution.net Please enter the following 'extra' attributes to be sent with your certificate request A challenge password []:asdf An optional company name []: Now you should have a Certificate Request File (WindowsXP.csr) and a private key					
	(VVIndowsXFKey.pem): [root@multibox URLcerts]# ls ca/ rou_cert.cer rou_request.csr WindowsXP.csr WindowsXPKey.pem					

Task P Produce the Windows XP Public Certificate which the XP computer can import to its Certificate Registry.

Syntax:

openssl x509 -req -in name.csr -CA ca/cacert.crt -CAkey ca/cakey.key -CAcreateserial -outform PEM -out name.pem -days 9999

Example:

[root@multibox URLcerts]# openssl x509 -req -in WindowsXP.csr -CA ca/ cacert.crt -CAkey ca/cakey.key -CAcreateserial -outform PEM -out WindowsXP.pem -days 9999 Signature ok subject=/DC=nz/DC=co/DC=alliedtelesis/C=NZ/ST=Canterbury/ L=Christchurch/0=YourCompany/OU=csg/CN=Client1/ emailAddress=test@solution.net Getting CA Private Key Enter pass phrase for ca/cakey.key: [root@multibox URLcerts]#

Task P Now you should have a certificate (WindowsXP.pem) and a private key (WindowsXPKey.pem): continued Continued

```
[root@multibox URLcerts]# ls -lct |more
total 24
-rw-r--r- 1 root root 1099 May 22 12:24 WindowsXP.pem
-rw-r--r- 1 root root 1106 May 22 12:13 WindowsXP.csr
-rw-r--r- 1 root root 887 May 22 12:13 WindowsXPKey.pem
drwxr-xr-x 2 root root 4096 May 21 14:38 ca/
-rw-r--r- 1 root root 924 May 21 14:38 rou_cert.cer
-rw----- 1 root root 552 May 21 14:35 rou_request.csr
```

Verify the Windows certificate shal fingerprint:

```
[root@multibox URLcerts]# openssl x509-in WindowsXP.pem-SHA1-
fingerprint|more
SHA1Fingerprint=F8:38:E5:B3:26:13:15:7D:00:80:DC:9B:28:4D:17:23:85:
62:FF:32
```

Task Q Converting the Windows XP certificate to a form that includes a Private Key.

We need to combine the certificate and the private key value into a **pkcs l 2** format file, so that both the certificate and the private key that were created on behalf of Windows XP can be loaded onto Windows XP:

Note that you will be prompted for an export password. You can use any password you like, but make sure you remember this password, as you will need to enter it again when you import the certificate into the Windows PC.

Syntax:

openssl pkcs12 -export -in name.pem -inkey nameKey.pem -out name.p12 **Example:** [root@multibox URLcerts]# openssl pkcs12 -export -in WindowsXP.pem inkey WindowsXPKey.pem -out WindowsXP.p12 Enter Export Password: Verifying - Enter Export Password: [root@multibox URLcerts]# ls *.p12 WindowsXP.p12

On the VPN remote host

Task R Download the Windows XP Certificate to the Windows XP Client.

• Use a file transfer method such as FTP, to download the Windows XP Client certificate.p12 file.

	tsfer Yew Queue Se	rver Help									
🕵 - 📴	t, Q 📰 🗈 🥾	🛛 🕱 R	8								
Address:	Use	¢	Password		Port		Quickgonnect 👻				
ommand: C lesponse: P lonmand: L lesponse: S latus: D	D /hoot/certificates/ lemote working directory is JST successfully received 9 item hirectory listing successful	i now /root/cert	ficates								
lonmand: G lesponse: D	iET Windows/IP.p12 C:\D Jownloading /toot/certifica	ocuments and 5 tes/Windows/2	2 p12 to C: \Do	le's Test Bay/M ocuments and S	y Docur iettings\	shayle's Te	tows/P.p12 FALSI nit Bay/My Docum	ents\Winds	wskP.p12		
Local Site: 🖭	Documents and Settings\S	hagle's Test Ba	y/My Docume	ints'	Rer	note Site:	hoot/certificates/				-
Flename	NetHood PrintHood Recent SendTo Start Menu Taxeelahar Filesia	e Filetype	Lar	st Modified		a penssl.cnf ou_cert.ce ou_cert.pe ou_reques	r m t.csr	7569 851 851 502	File Folder SpeedDial Security Ce PEM File CSR File	04/05/2009 04/05/2009 04/05/2009 04/05/2009 04/05/2009	11:37 15:58 11:39 11:37 11:33
 My Music Wave LB rest 	n pras	File Folder	20/0	06/2005 14:		Windowsop Windowsop Windowsop	.p12 .pem	968 1669 936	Personal In PEM File	04/05/2009 04/05/2009 04/05/2009	16:01 16:14 16:11
folders and di	Her oak 207220 beter				<	Mindewcop	Ab 1660 between	887	DFM File	040512009	16:01
Local Filename	They will rough y bytes.	Sce	Direction	Repote Filepar	pane -		Host		2.ehus		_

Import the Windows XP certificate to the Personal Certificate Store

- In the MMC console, select: Certificates (Local Computer) > Personal > Certificates
- Right-click on Certificates and select: All Tasks > Import...

ъ	ertificates - [Console Root\Certifica	tes (Local Computer)\Personal\C	ertificates]		
30	File Action View Favorites Window	Help			@ ×
٠	- 🗈 🔟 🗈 🕞 😫				
	Control Root Controot Contro Control Root Control Root Control Roo	Sequent New Certificate	Issued By There are no kend to show in this view.	Expiration Date Int	inded Purposes
<		¢			>
Add	a certificate to a store				

- This will start the **Certificate Import Wizard**.
- Click Next.

On the \	On the VPN remote host				
Task R	• To import the CA's certificate file, click Bro	wse.			
continued					
	File to Import Specify the file you want to import. File name: I Browse Note: More than one certificate can be stored in a single file in the following formats: Personal Information Exchange- PKCS #12 (.PFX, P12) Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B) Microsoft Serialized Certificate Store (.SST)				

• Select your WindowsXP p12 file. Click **Open**.



• Type in the **password** of the private key, as used on Linux during the creation of this certificate in Task Q. Click **Next**.

rtificate lr	nport Wizard
Password To main	tain security, the private key was protected with a password.
Type th	e password for the private key.
Pass	*
E	nable strong private key protection. You will be prompted every time the rivate key is used by an application if you enable this option.
k	an cuis rey as exportable. This will allow you to back up or transport, your sys at a later time.
	< Back Next Cancel

On the VPN remote host

Task R• The Wizard will automatically prompt a suitable store, in this case it is the Personal
Certificate Store. Click Next.

ertificat	e Store
Certific	ate stores are system areas where certificates are kept.
Windo	ws can automatically select a certificate store, or you can specify a location for
0	Automatically select the certificate store based on the type of certificate
۲	Place all certificates in the following store
	Certificate store:
	Personal Browse

• Confirm the settings you have selected, then click **Finish**.



• Click **OK** to complete the import.



On the VPN remote host						
Task R	• In the Certificate MMC Console you can confirm that the certificate has been imported.					
continued	The certificates are sorted by the Common Name they were issued to. In this case, the					
	Personal Certificate for the computer will be found as follows: Certificates (Local					
	Computer) > Personal > Certificates.					
	Lock in list of contificator for the CA's Common Name					

Look in list of certificates for the CA's Common Name.



Double-click on the certificate and the certificate details will be displayed. It should show
as a valid certificate - if it is not valid, an error message will be displayed.

Certificate ?
General Details Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
Issued to: Client1
Issued by: CA-Cert
Valid from 22/05/2009 to 6/10/2036
\mathscr{P} You have a private key that corresponds to this certificate.
Issuer Statement

• The Certification Path tab, displays which CA issued (signed) this certificate.

Certification path	4			
Clent1				
		r		
			View Certific	ate
Certificate status:				
This certificate is O	К.			

On the VPN remote host

Task R • You can also validate the certificate by fingerprint value. It should match the fingerprint seen in Task P. In this example the value ends with FF 32: continued



This certificate will be used for negotiating the VPN link, and will dynamically be added to the router's PKI Database. When that happens you can also verify the fingerprint value of that dynamically added certificate, if desired, as a verification step.

On the V	/PN remote host	
Task S	Setting Up the Windows XP Client VPN Network Connection	

- Access The Network Connections Summary via Start > Control Panel > Network Connections.
- Select Create a new connection.



• The new connection wizard opens, click **Next**.



• Select **Connect to the network at my workplace**. This option supports VPN connections.





• The new connection wizard opens, click **Next**.



Select Connect to the network at my workplace. This option supports VPN connections.

etwork Connection Type What do you want to do?	
O Connect to the Internet	
Connect to the Internet so you	can browse the Web and read email.
Connect to the network at	mv workplace
Connect to a business network a field office, or another location	(using dial-up or VPN) so you can work from home, h.
○ Set up a home or small offi	ce network
Connect to an existing home or	small office network or set up a new one.
O Set up an advanced conne	ection
Connect directly to another com set up this computer so that oth	puter using your serial, parallel, or infrared port, or er computers can connect to it.
	< Back Next > Cano

On the V	On the VPN remote host									
Task S	Select Virtual Private Network connection. Click Next.									
continued										
	New Connection Wizard									
	Network Connection How do you want to connect to the network at your workplace?									
	Create the following connection:									
	Connect using a modem and a regular phone line or an Integrated Services Digital Network (ISDN) phone line.									
	Virtual Private Network connection Connect to the network using a virtual private network (VPN) connection over the Internet.									
	< Back Next >>> Cancel									

• Type in a **Company Name** for this connection. Click **Next**.



• Type a destination **IP for this VPN** connection. On our VPN router, this will be the address of the public interface that the IPsec policy is applied to. Click **Next**.

PN Server Selection What is the name or address of the	VPN server?
Type the host name or Internet Prot	ocol (IP) address of the computer to which you are
Host name or IP address (for examp	le, microsoft.com or 157.54.0.1):
10.17.90.181	
	C Bank Marks Can



• Other settings need to be adjusted. In the **Connection Solution** dialogue box, click **Properties**.



• In the Security tab choose Typical settings.

50l	Ition Properties (*
enei	al Options Security Networking Advanced
-Se	curity options
۲	Typical (recommended settings)
	Validate my identity as follows:
	Require secured password
	Automatically use my Windows logon name and password (and domain if any)
	Require data encryption (disconnect if none)
C	Advanced (custom settings)
Ĭ	Using these settings requires a knowledge Settings
	IPSec Settings
	OK Cance

On the VPN remote host

 Task S
 In the Networking tab, choose L2TP IPsec VPN from the Type of VPN drop-down box. Click OK.



• To test the connection, click **Connect**. For first use, you might choose to enable ISAKMP debugging on the receiving router to track connection progress. Use **enable ISAKMP debug**.



• A Verifying username and password dialogue box appears during the connection attempt.



• Once connected, an additional **connection icon** will appear in the system tray. You can double-click the icon for more information.



On the Router

```
Task T
       Verification of VPN Connection from Router viewpoint.
       On the router, the ISAKMP debug will show as follows for a successful connection.
       SecOff Certificate VPN demo> enable isakmp debug=all
       ISAKMP MAIN exchange 13: New State: IDLE
       ISAKMP MAIN: RESP: xchg 13: Started with peer 10.17.90.1
       ISAKMP Rx Message
                    56a8d065ba62eb36:0000000000000000
           Cookies:
           Xchg Type: IDPROT(2) Ver: 10 Flags: 00
           MessageID: 00000000 Total Length: 312
           Payload #: 0 Length: 200 Type: Security Association (SA)
             DOI: IPSEC(0) Situation: 00000001
               Proposal#: 1 Protocol: ISAKMP(1) #Trans: 5 SPI:
                 Transform#: 1
                  Transform Id ..... IKE(1)
                  Encryption Algorithm..... 3DESOUTER(5)
                  Authentication Algorithm..... SHA(2)
                  Authentication Method..... RSA SIGNATURE(3)
                  Group Description..... UNKNOWN (14)
                  Group Type..... MODP
                  Expiry Seconds..... 28800
                 Transform#: 2
                  Transform Id ..... IKE(1)
                  Encryption Algorithm..... 3DESOUTER(5)
                  Authentication Algorithm..... SHA(2)
                  Authentication Method..... RSA SIGNATURE(3)
                  Group Description..... 1024(2)
                  Group Type..... MODP
                  Expiry Seconds..... 28800
                 Transform#: 3
                  Transform Id ..... IKE(1)
                  Encryption Algorithm..... 3DESOUTER(5)
                  Authentication Algorithm..... MD5(1)
                  Authentication Method..... RSA SIGNATURE(3)
                  Group Description..... 1024(2)
                  Group Type..... MODP
                  Expiry Seconds..... 28800
                 Transform#: 4
                  Transform Id ..... IKE(1)
                  Encryption Algorithm..... DES(1)
                  Authentication Algorithm..... SHA(2)
                  Authentication Method..... RSA SIGNATURE(3)
                  Group Description..... 768(1)
                  Group Type..... MODP
                  Expiry Seconds..... 28800
                 Transform#: 5
                  Transform Id ..... IKE(1)
                  Encryption Algorithm..... DES(1)
                  Authentication Algorithm..... MD5(1)
                  Authentication Method..... RSA SIGNATURE(3)
                  Group Description..... 768(1)
                  Group Type..... MODP
                  Expiry Seconds..... 28800
            Payload #: 1 Length: 24 Type: Vendor ID (VID)
             string=UNKNOWN
             1e 2b 51 69 05 99 1c 7d 7c 96 fc bf b5 87 e4 61 00 00 00 04
            Payload #: 2 Length: 20 Type: Vendor ID (VID)
             string=Microsoft L2TP/IPsec VPN remote host
             40 48 b7 d5 6e bc e8 85 25 e7 de 7f 00 d6 c2 d3
```

```
On the Router
          Payload #: 3 Length: 20 Type: Vendor ID (VID)
debug cont.
               string=draft-ietf-ipsec-nat-t-ike-02\n
               90 cb 80 91 3e bb 69 6e 08 63 81 b5 ec 42 7b 1f
             Payload #: 4 Length: 20 Type: Vendor ID (VID)
               string=UNKNOWN
               26 24 4d 38 ed db 61 b3 17 2a 36 e3 d0 cf b8 19
        ISAKMP MAIN: RESP: xchg 13: Rx NAT-T version 2 vendor ID
        ISAKMP MAIN exchange 13: New State: SARECV
        ISAKMP DOI: IPSEC: Compare transform fail: groupDescription 1=2 r=14
        ISAKMP MAIN: RESP: xchg 13: Found matching policy = keys
        ISAKMP Tx Message
                      56a8d065ba62eb36:76d1cff59aa528c8
             Cookies:
             Xchg Type: IDPROT(2) Ver: 10 Flags: 00
             MessageID: 00000000 Total Length: 80
             Payload #: 0 Length: 52 Type: Security Association (SA)
              DOI: IPSEC(0) Situation: 00000001
                 Proposal#: 1 Protocol: ISAKMP(1) #Trans: 1 SPI:
                  Transform#: 2
                    Transform Id ..... IKE(1)
                    Encryption Algorithm..... 3DESOUTER(5)
                    Authentication Algorithm..... SHA(2)
                    Authentication Method..... RSA SIGNATURE(3)
                    Group Description..... 1024(2)
                    Group Type..... MODP
                    Expiry Seconds..... 28800
        ISAKMP MAIN exchange 13: New State: SASENT
        ISAKMP Rx Message
             Cookies: 56a8d065ba62eb36:76d1cff59aa528c8
             Xchg Type: IDPROT(2) Ver: 10 Flags: 00
             MessageID: 00000000
                                   Total Length: 184
             Payload #:
                        0 Length: 132 Type: Key Exchange (KE)
               ea 97 76 66 37 64 60 2d ef b0 d3 2a 72 2b 22 3c 94 64 64 26
               90 2d 77 cf e8 be 68 91 8a 5b b9 59 67 ff f3 39 6e fd 5e 39
               c9 d0 73 67 88 25 c0 ee 66 68 b7 96 82 6b 22 d7 8b 3c 92 2c
              b6 b9 8a e6 7c 99 b5 e3 c5 34 a3 b5 dd 80 87 4c 84 e1 52 f0
               f3 61 f4 be 85 53 a3 e6 23 15 5e 0e fc bc 44 0d 7e 0b 52 0f
               37 44 2e 9a c8 e2 a5 fc 8d b5 b4 c3 ca fa 6a 09 c2 6d d7 dd
              be 2c d0 55 87 45 77 50
             Payload #: 1 Length: 24 Type: Nonce (NONCE)
              cb c8 1a 6a dc 96 ec b6 a8 72 2f 9c ca 78 fd f3 a3 d1 22 84
        ISAKMP MAIN exchange 13: New State: KERECV
        ISAKMP MAIN: RESP: xchg 13: Ni 1=20
        v=cbc81a6adc96ecb6a8722f9cca78fdf3a3d12284
        ISAKMP MAIN: RESP: xchg 13: Nr 1=20
        v=b9a348d97ff2cffc2c341d1f01b723bf684690b4
        ISAKMP MAIN: RESP: xchg 13: COOKIE_I l=8 v=56a8d065ba62eb36
        ISAKMP MAIN: RESP: xchg 13: COOKIE_R l=8 v=76d1cff59aa528c8
        ISAKMP MAIN: RESP: xchg 13: EncKey 1=24
        v=7c7645dbf89df549448b7d2dd36a49fb7f93b9
        5d68305bc1
        ISAKMP MAIN: RESP: xchg 13: IV 1=8 v=184fcd78c56a0d50
        ISAKMP Tx Message
                      56a8d065ba62eb36:76d1cff59aa528c8
             Cookies:
             Xchg Type: IDPROT(2) Ver: 10 Flags: 00
             MessageID: 00000000 Total Length: 184
```

On the R	outer																			
debug cont.	Payload	#:	0	Leng	gth	: 1	32	Тур	pe:	Key	7 E2	xcha	ang	e (]	KE)					
0	ć	af 39	9 83	86	08	b4	38	0b	ae	c4	f8	d6	b3	7e	24	68	44	de	8f	17
	€	e4 f:	3 7 d	f4	80	7e	2a	7b	b4	0e	0b	be	16	96	29	d5	de	cf	26	37
	C	cd 3	5 d8	37	a7	56	a7	59	1d	7e	1f	7b	bc	72	1b	db	e2	70	5b	ed
		7ef	7 b0	f6	57	c0	6f	30	95	69	51	£4	e3	d4	de	32	d7	8a	44	76
	1	38 4	9 2c	16 Ea	b5	3C	da bo	4b	43	98	00	ea	03	2e	C7	0e	d6	5b	64	19
	1)3 C0 =5 2'	е за 7 ЛЛ	La 6f	00 81	7C	80. 87	ee 6e	ae	eı	60	28	09	80	að	90	28	63	υa	18
	Pay	-J 2 Zload	/ == 7 #•	1	Le	ona.	+h•	24	Ψ,	me	· No	once	- (1	NON	°E)					
	laj	59 a.	3 4 8	d9	7£	f2	cf.	fc	2c	34	1d	1f	01	b7	23	bf	68	46	90	b4
	ISAKMP N	IAIN	exc	hang	ge 1	13:	Nev	w St	tat	e: P	KESI	ENT								
	ISAKMP H	Rx Me	essa	ge	(dec	cry	pteo	d)												
	Cod	kie	5:	568	a8d(0651	ba62	2eb3	36:	76d1	lcf	£59a	aa5	28c8	8					
	Xcł	ng T	ype:	I	DPRO) ТС	2)	Ve	r: 1	10	Fla	ags	: 0	1						
	Mes	ssage	eID:	0	0000	000	0	Tot	tal	Ler	ıgtl	h: 1	L11:	3						
	Pay	load	1 #:	0	Le	eng	th:	120	5 !	Гуре	e: 1	Ider	nti	Eica	atio	on	(ID))		
	1	lype -	: DE	R_A	SN1_	_DN	P	roto	oco:	lId	: 0	РC	ort	: 0					_	<u> </u>
	Va	Lue:	cn=	CL1	ent	1,	ou=	Sal	es,	0=2	ATT:	led	Te.	lesi	LS,	T=C	hri:	stc	hur	ch,
	SL= Pay	rload	₹ #•	1	T.e	ana	th:	65	· ۲	Fvne	(Cert	if	icat	te -	(C)				
	()4 3	2 82	02	87	30	82	01	f0	02	01	03	30	0d	06	09	2a	86	48	86
	ł	E7 00	d 01	01	04	05	00	30	81	a3	31	0b	30	09	06	03	55	04	06	13
	()2 4	e 5a	31	13	30	11	06	03	55	04	08	13	0a	43	61	6e	74	65	72
	6	52 7	5 72	79	31	15	30	13	06	03	55	04	07	13	0c	43	68	72	69	73
	5	74 63	3 68	75	72	63	68	31	17	30	15	06	03	55	04	0a	13	0e	41	6c
	6	5c 6	9 65	64	20	54	65	6c	65	73	69	73	31	19	30	17	06	03	55	04
	()b 13	3 10	43	75	73	74	6f	6d	65	72	20	53	75	70	70	6f	72	74	31
	()f 3	0 0 d	06	03	55	04	03	13	06	43	53	47	2f	43	41	31	23	30	21
	(9 2a	86	48	86	±7	0d	01	09	01	16	14	65	./8	61	6d	.70	6C	65
	4	10 /. 25 20	36I 121	6C 20	/5 21	/4 21	69 21	6İ 22	6e	∠e 5p	6e	65 04	/4	30	1e	1/	0d	30	39	30
	-	יכ כי 1 א ^י))4 1 33	31	54 5a	30	74	31	0h	30	1 / 0 9	06	03	55	04	06	13	02	10 10	54 5a
		31 1	3 30	11	06	03	55	04	0.8	13	0a	43	61	6e	74	65	72	62	75	72
		79 3:	1 15	30	13	06	03	55	04	07	13	0c	43	68	72	69	73	74	63	68
	5	75 72	2 63	68	31	17	30	15	06	03	55	04	0a	13	0e	41	6c	6c	69	65
	6	54 2	54	65	6c	65	73	69	73	31	0e	30	0c	06	03	55	04	0b	13	05
	ŗ,	53 63	1 6c	65	73	31	10	30	0e	06	03	55	04	03	13	07	43	6c	69	65
	6	5e 7	4 31	30	81	9f	30	0d	06	09	2a	86	48	86	f7	0d	01	01	01	05
	(0 0	3 81	8d	00	30	81	89	02	81	81	00	d7	37	68	b1	e6	df	2a	6a
	-	13 3! Da 1a	9 ea	a2	C8	72	38	41	ec	-79	ia 21	12	75	12	22	01	ea	80	86	c2
	(5 7	2 2 2 1	00 50	14 06	5u	50 bo	40	LCI FO	04 09		e4	ee 50	40	9e f3	24 28	6D	13	ea ga	eo hg
	e	a a	5 5 5 F 9 1	49	e0 b5	b9	ca	4e	75	50	9a	68	07	91	62	43	db	16	7f	e8
	(a e	3 a9	1f	4a	74	00	d5	5d	b6	e5	4b	94	08	7a	40	be	c4	a6	41
	ć	a2 71	5 a6	05	с0	d5	7e	1b	56	e8	CC	7f	e1	dc	9e	31	f4	01	b7	f5
	(02 03	3 01	00	01	30	0d	06	09	2a	86	48	86	f7	0d	01	01	04	05	00
	()3 83	1 81	00	84	a2	90	£9	fa	40	9f	51	a1	06	68	fe	db	56	5a	93
	ł	0 22	2 cc	46	2c	c5	39	55	5e	3b	8c	7e	ff	a7	7f	с0	1b	64	75	c1
	C	14 8	5 7e	51	ec	b9	b2	0c	55	09	32	da	45	d6	13	с7	83	01	06	6e
	2	la c	3 72	8f	33	75	a5	64	bc	99	6d	8a	eb	46	86	bd	6e	25	26	63
	-)1 5a	a e8	fa	c7	cf	0a	4c	5f	9d	26	01	22	c5	e2	4b	c5	b9	de	ed
	0	10 ±1	J 30	48	31	C5	27 £2	90 af	6d	47	12	cd	/i	cd	31	6C	aa	6e	80	Ud
	e	= / 4(a eb	ΟŎ	uy	01	LΖ	uI	uδ	40	00	ze								

| On the R | outer | |
 | | |
 | |
 | | |
 | | | | |
 | | | | | |
|-------------|--------------------------|--
--
---|---|---|--
---	---
--	--
--	--
debug cont	Payload
 | 2 1 | Leng | gth
 | : 1 | 32
 | Тур | be: | Sig
 | gnat | ture | э (; | SIG |)
 | | | | | |
| debug cont. | | 7a | f1
 | 31 | f0 | e4
 | be | са
 | 8c | 93 | 48
 | 09 | 41 | 59 | 20 | 95
 | e1 | 96 | 7c | de | 67 |
| | | 72 | с8
 | 74 | 39 | 70
 | 8b | 2e
 | 65 | 7d | 24
 | 15 | 9c | 81 | 43 | a6
 | 21 | fd | 87 | 9d | e3 |
| | | 28 | 1e
 | 58 | d8 | 88
 | 84 | 0a
 | ab | 81 | 7e
 | fb | b8 | 30 | 4e | a9
 | 28 | 2d | e9 | d0 | 53 |
| | | 01 | 49
 | c4 | 85 | ba
 | 39 | 56
 | a2 | 91 | 2e
 | 0d | da | 29 | ad | ba
 | 2e | 8e | 37 | cd | 8f |
| | | 86 | e9
 | 53 | 8f | с1
 | fc | de
 | 32 | a8 | 99
 | a8 | 3a | 9a | 62 | 19
 | 00 | 79 | 7e | 71 | 28 |
| | | 33 | 33
 | cd | 2e | 94
 | a4 | 0f
 | 0a | 35 | 84
 | 80 | 96 | a4 | 94 | 89
 | 06 | 4d | b7 | b7 | £3 |
| | P | 87 | 2c
 | 85 | 7e | d8
 | d9 | 47
 | 51 | _ | | | |
 | | ~ 1 | | |
 | | | | ~ T \ | |
| | Pe | AAT(| 30
 | #:
Q1 | 2 | 上6
3.1
 | eng
0b | 30
 | T / 1 | 06 | U3
LÀDe
 | 3: (
55 | on a | 06 | 13 | Le i
02
 | keqi | Jesi
5a | 2 ((
21 | _R)
13 | 3.0 |
| | | 11 | 06
 | 03 | a5
55 | 01
 | 0.0 | 13
 | 09 | 13 | 61
 | 60 | 7/ | 65 | 13
72 | 62
 | 40
75 | 72 | 79 | 1J
21 | 15 |
| | | 30 | 13
 | 06 | 03 | 55
 | 04 | 07
 | 13 | 4.5
0.c | 43
 | 68 | 72 | 69 | 73 | 74
 | 63 | 68 | 75 | 72 | 63 |
| | | 68 | 31
 | 17 | 30 | 15
 | 06 | 03
 | 55 | 04 | 0a
 | 13 | 0e | 41 | 6c | 6c
 | 69 | 65 | 64 | 20 | 54 |
| | | 65 | 6c
 | 65 | 73 | 69
 | 73 | 31
 | 19 | 30 | 17
 | 06 | 03 | 55 | 04 | 0b
 | 13 | 10 | 43 | 75 | 73 |
| | | 74 | 6f
 | 6d | 65 | 72
 | 20 | 53
 | 75 | 70 | 70
 | 6f | 72 | 74 | 31 | 0f
 | 30 | 0d | 06 | 03 | 55 |
| | | 04 | 03
 | 13 | 06 | 43
 | 53 | 47
 | 2f | 43 | 41
 | 31 | 23 | 30 | 21 | 06
 | 09 | 2a | 86 | 48 | 86 |
| | | f7 | 0d
 | 01 | 09 | 01
 | 16 | 14
 | 65 | 78 | 61
 | 6d | 70 | 6c | 65 | 40
 | 73 | 6f | 6c | 75 | 74 |
| | | 69 | 6f
 | 6e | 2e | 6e
 | 65 | 74
 | | | | | |
 | | | | |
 | | | | | |
| | ISAKMP | MA | EN:
 | RE; | SP: | xcl
 | ng i | 13:
 | Cei | tif | Eica
 | ate | rec | cei | ved | and
 | l va | alid | late | eđ | |
| | ISAKMP | MA: | EN e
 | excl | hang | ge 1
 | 13: | Ne
 | wrSt
_ | tate | e: /
 | AUTI | HRE | CV | |
 | | | | | |
| | ISAKMP | MA: | LN:
 | RE | SP: | xci
 | ng : | 13:
 | Ren | note | EID=
 | =DN | :cn: | =C1: | len | τ1,
 | ou | =Sal | Les | ' | |
| | l=Chrie | st cl | 1916
 | cb. | s,
et: | _
 | |
 | | | | | |
 | | | | |
 | | | | | |
| | ISAKMP | MAI | EN:
 | RES | SP: | xcl
 | na i | 13:
 | Cei | tif | Eica
 | ate | sei | nt | |
 | | | | | |
| | ISAKMP | Тx | Mes
 | ssag | ge | | | |
|---|---|---|---|---|
 | | |
 | | | | |
 | | | | | |
| | Co | ook | ies
 | : | 56a | a8d(
 | 0651 | ba62
 | 2eb3 | 86:7 | 76d1
 | lcf | E59a | aa52 | 28c8 | 3
 | | | | | |
| | Xc | chg | Тур
 | pe: | II | DPR
 |) ТС | 2)
 | Vei | :: 1 | LO
 | Fla | ags | : 00 | C |
 | | | | | |
| | Me | essa | agei
 | ID: | 00 | 0000
 | 000 | 0
 | Tot | al | Ler
 | ngtl | n: 8 | 348 | | |
 | | | | | |
| | | |
 | | |
 | |
 | | | | | |
 | - | | | |
 | | | | | |
| | Pa | ayl o | bađ
 | #: | 0 | Le
 | engt | th:
 | 131 | . 1 | ſype
 | ••• | [dei | ntii | Eica | atio
 | on | (ID) |) | | |
| | Pa | yld
Typ | pad
pe:
 | #:
DEI | 0
R_A | Le
SN1_
 | eng
DN | th:
P:
 | 131
roto | | [ype
LId:
 | e: 1
: 0 | Ider
Po | ort | Eica
: O | atio
 | on | (ID) |) | | |
| | Pa
1=Chris | yld
Typ
Val | bad
pe:
Lue
 | #:
DEI
: CI | 0
R_A
n=ro | Le
SN1_
oute
 | engi
_DN
er-J | th:
P:
ATI
 | 131
roto
, ou | | fype
LId:
SG_I
 | : 0
Lab | Ider
Po
, O | ort
=A1 | Eica
: 0
Lied | atio
1 Te
 | on
ele: | (ID)
sis, | , | | |
| | Pa
l=Chris
Payload | yld
Typ
Val
stcl | bad
be:
Lue
huro
 | #:
DEI
: CI
ch,
1] | 0
R_A
n=ro
st:
Leno | Le
SN1_
oute
=
gth:
 | engi
_DN
er-2 | th:
P:
ATI,
93
 | 131
roto
, ou
Typ | ocol
1=C: | fype
LId:
SG_I
Cei
 | e: 1
: 0
Lab, | Eica | ntii
ort
=A1: | Eica
: 0
Lied
(C) | atio
1 Te
)
 | on
ele: | (ID)
sis, | , | | |
| | Pa
l=Chris
Payload | yld
Tyr
Val
stcl
1 #:
04 | bad
pe:
Lue
huro
30
 | #:
DEI
: CI
ch,
1 1
82 | 0
R_A
n=ro
st:
Leng
02 |
Le
SN1_
oute
=
gth:
48 | engt
_DN
er-2
: 5!
30 | th:
P:
ATI,
93
82
 | 131
roto
, ou
Typ
01 | b1 | Fype
LId:
SG_I
Cei
02
 | e: 1
: 0
Lab,
rti:
01 | Iden
Po
, O:
Eica
02 | ate | Eica
: 0
Lied
(C)
0d | atio
1 Te
06
 | on
ele:
09 | (ID)
sis,
2a | 86 | 48 | 86 |
| | Pa
l=Chris
Payload | yld
Tyn
Val
stcl
1 #:
04
f7 | bad
pe:
Lue
hur
30
0d
 | #:
DEI
: CI
ch,
1 I
82
01 | 0
R_As
n=ro
st:
Leng
02
01 |
Le
SN1_
Oute
=
gth:
48
04 | engt
_DN
er-2
: 5!
30
05 | th:
P:
ATI,
93
82
00
 | 131
roto
01
30 | b1
81 | Cen
D2
a3
 | : 0
Lab,
rti:
01
31 | Eica
02
0b | ate
30
30 | Eica
: 0
Lied
(C)
0d | atic
1 T
06
06
 | on
ele:
09
03 | (ID)
sis,
2a
55 | 86
04 | 48
06 | 86
13 |
| | Pa
l=Chris
Payload | yld
Tyr
Va
stcl
tcl
1
#
04
f7
02 | bad
be:
Lue
auro
30
0d
4e | #:
DEI
ch,
1 1
82
01
5a | 0
R_A:
n=rc
st:
Leng
02
01
31 | Le
SN1_
Oute
=
gth:
48
04
13 | - DN
- DN
 2
 | <pre>th:
P:
ATI,
93
82
00
11</pre> | 131
roto
Tyr
01
30
06 | b1
03 | fype
Id :
G _1
Cen
02
a3
55 | : 0
Lab,
01
31
04 | Eica
02
08 | ate
30
30
13 | Eica
: 0
Lied
(C)
0d
09
0a | atic
d Te
06
43 | on
ele:
09
03
61 | (ID)
sis,
2a
55
6e | 86
04
74 | 48
06
65 | 86
13
72 |
| | Pa
l=Chris
Payload | yla
Tyr
Va
stcl
1 #:
04
f7
02
62 | ad
a
i
a
i
a
i
a
b
a
b
a
b
a
b
a
b
a
b
a
b
a
b
a
b
a
b
a
b
b
c
c
c
c
c
c
c
c
c
c
 | #:
DEI
: CI
ch,
1 1
82
01
5a
72 | 0
R_As
n=rc
st:
Leng
02
01
31
79 |
Le
SN1_
Oute
=
gth:
48
04
13
31 | png
DN
sr -2
3 0
05
30
15 | <pre>th:
P:
ATI,
93
82
00
11
30</pre>
 | 131
rotc
Tyr
01
30
06
13 | b1
03
06 | Cen
02
a3
55
03
 | Cab ,
Cab ,
01
31
04
55 | Eica
02
0b
08
04 | ate
30
30
13
07 | Eica
: 0
lied
(C)
0d
09
0a
13 | atic
d Te
06
06
43
0c
 | 09
03
61
43 | (ID)
sis,
2a
55
6e
68 | 86
04
74
72 | 48
06
65
69 | 86
13
72
73 |
| | Pa
l=Chris
Payload | yld
Tyr
va:
stcl
stcl
1
#
04
f7
02
62
74 | ad
ue
30
0d
4e
75
63
 | #:
DEI
ch,
1 1
82
01
5a
72
68 | 0
R_A:
n=rc
st:
02
01
31
79
75 | Le
SN1_
Out
e
e
48
04
13
31
72 | DN
5
5
3 0
05
3 0
15
63 | P
ATI
93
82
00
11
30
68
 | 131
roto
Tyr
01
30
06
13
31 | b1
81
03
06
17 | Cen
02
a3
55
03
30
 | cti
Cab
rti
01
31
04
55
15 | Eica
02
0b
08
04
06 | ate
30
30
13
07
03 | Eica
: 0
Lied
(C)
0d
09
0a
13
55 | atic
1 T
06
06
43
0c
04
 | 09
03
61
43
0a | (ID)
sis,
2a
55
6e
68
13 | 86
04
74
72
0e | 48
06
65
69
41 | 86
13
72
73
6c |
| | Pa
l=Chris
Payload | yld
Tyr
va
stcl
1
#
04
f 7
02
62
74
6c | ad
a
a
a
a
a
b
a
b
a
b
a
b
a
b
a
b
a
b
a
b
a
b
a
b
a
b
a
b
a
b
b
a
b
b
c
b
c
c
c
c
c
c
c
c
c
c | #:
DEI
ch,
1 1
82
01
5a
72
68
65 | 0
R_A:
st:
Ceng
02
01
31
79
75
64 | Le
SN1_
Out e
=
48
04
13
31
72
20 | DN
5
3 0
3 0
1 5
6 3
5 4
5 4 | h:
P:
ATI
82
00
11
30
68
65 | 131
rot
Typ
01
30
06
13
31
6c | b1
81
03
06
17
65 | Cer
02
a3
55
03
30
73 | t in
t | Eica
02
0b
08
04
06
73 | ate
30
30
13
07
03
31 | Eica
: 0
(C)
0d
09
0a
13
55
19 | atic
1 Te
06
06
43
0c
04
30 | 09
03
61
43
0a
17 | (ID)
sis,
2a
55
6e
68
13
06 | 86
04
74
72
0e
03 | 48
06
65
41
55 | 86
13
72
73
6c
04 |
| | Pa
1=Chris
Payload | yld
Tyr
va
stcl
1
#
04
f7
02
62
74
6c
0b
0c | ad
a
a
a
a
a
b
a
b
a
b
a
b
a
b
a
b
a
b
a
b
a
b
a
b
a
b
a
b
b
c
c
c
c
c
c
c
c
c
c
 | #:
DEI
: CI
ch,
82
01
5a
72
68
65
10 | 0
R_A:
n=ro
st:
02
01
31
79
75
64
43
02 | Le
SN1_
Out
e
=
48
04
13
31
72
20
75 | DN
5
3 0
5
3 0
15
6 3
5 4
7 3
5 4 | P:
ATI
93
82
00
11
30
68
65
74
 | 131
Typ
01
30
06
13
31
6c
6f | b1
03
06
17
65
6d | Cer
Cer
Cer
02
a3
55
03
30
73
65
06
 | 5
1
1
1
1
1
1
1
1 | Eica
02
0b
08
04
06
73
20 | ate
30
30
13
07
03
31
53 | Eica
: 0
(C)
0d
09
0a
13
55
19
75 | atic
a T
a
a
b
a
b
a
b
a
b
b
b
b
c
c
c
c
c
d
d
d
d
d
d
d
d
 | 09
03
61
43
0a
17
70 | (ID)
sis,
2a
55
6e
68
13
06
6f | 86
04
74
72
0e
03
72 | 48
06
65
69
41
55
74 | 86
13
72
73
6c
04
31 |
| | Pa
l=Chris
Payload | ylc
Tyr
va:
stcl
1 #:
04
f7
02
62
74
6c
0b
0f | Dad De: Jue 30 0d 4e 75 63 69 13 30
 | #:
DEJ
ch,
1 1
82
01
5a
72
68
65
10
0d | 0
R_As
n=rc
st:
02
01
31
79
75
64
43
06 |
Le
SN1_
Dute
=
(1)
48
04
13
31
72
20
75
03 | DN
C
C
C
C
C
C
C
C | <pre>th: P: ATI 93 82 00 11 30 68 65 74 04 57</pre>
 | 131
Tyr
01
30
06
13
31
6c
6f
03
04 | 2000
1=C2
b1
81
03
06
17
65
6d
13 | Cen
02
a3
55
03
30
73
65
06
 | c i i i i i i i i i i | Eden
Pc
C
C
C
C
C
C
C
C
C
C | ate
30
30
13
07
03
31
53
47 | Eica
: 0
lie
(C)
0d
09
0a
13
55
19
75
2f | atic
1 Te
06
06
43
0c
04
30
70
43
70
 | 09
03
61
43
0a
17
70
41 | (ID)
2a
55
6e
68
13
06
6f
31 | 86
04
72
0e
03
72
23 | 48
06
65
69
41
55
74
30 | 86
13
72
73
6c
04
31
21 |
| | Pa
l=Chris
Payload | ylc
Tyr
va:
stcl
1 #;
04
f7
02
62
74
62
74
62
0b
0f
06 | Dad De: Jue 30 0d 4e 755 63 69 13 30 09 72
 | #:
DEI
: Ch,
1 1
82
01
5a
72
68
65
10
0d
2a | 0
R_A:
st:
Cleng
02
01
31
79
75
64
43
06
86 | La
SN1_
Out
of
a
48
04
13
31
72
20
75
03
48
75 | DN
DN
2
3
0
5
3
0
5
6
3
0
5
6
3
0
5
6
3
0
5
6
3
0
5
6
3
0
5
6
3
0
5
6
3
0
5
6
3
0
5
6
3
0
5
6
3
0
5
6
3
0
5
6
3
1
5
6
3
1
5
6
3
1
5
6
3
1
5
6
3
1
5
6
3
1
5
6
3
7
7
7
7
7
7
7
7 | <pre>th:
P:
P3
82
00
11
30
68
65
74
04
f7
60</pre>
 | 131
rotc
, ou
01
30
06
13
31
6c
6f
03
0d | b1
1=CS
b1
81
03
06
17
65
6d
13
01
65 | Cei
02
a3
55
03
30
73
65
06
09
 | <pre>clab,
clab,
01
31
04
55
15
69
72
43
01</pre> | Eden
P
C
C
C
C
C
C
C
C
C
C | ate
30
30
13
07
03
31
53
47
14
74 | Eica
: 0
lied
(C)
0d
09
0a
13
55
19
75
2f
65
20 | atic
1 Te
06
06
43
0c
04
30
70
43
78
10
 | 09
03
61
43
0a
17
70
41
61 | (ID)
sis,
2a
55
6e
68
13
06
6f
31
6d | 86
04
72
0e
03
72
23
70 | 48
06
65
69
41
55
74
30
6c | 86
13
72
73
6c
04
31
21
65
20 | | | | | | | | | | | | | | | | | |
| | Pa
l=Chris
Payload | Tyr
Val
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl
stcl | Dad pe: lue 30 0d 4e 75 63 69 13 30 09 73 30 | #:
DEI
: CI
ch,
1 1
82
01
5a
72
68
65
10
0d
2a
6f
33 | 0
R_A:
m=rc
st:
Leng
02
01
31
79
75
64
43
06
86
6c
32 | Le
SN1_
Out (
48
04
13
31
72
20
75
03
48
75
33 | b n n n n n n n n n n | <pre>th: P: ATI 93 82 00 11 30 68 65 74 f7 69 39</pre> | 131
rotc
, ot
01
30
06
13
31
6c
6f
03
0d
6f
30 | b 1
b 1 | Cen
Cen
02
a3
55
03
30
73
65
06
09
2e
5a | cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
c | Eden
Po
Po
C
C
C
C
C
C
C
C
C
C | ate
30
30
13
07
03
31
53
47
14
74
33 | Eica
: 0
lied
(C)
0d
09
0a
13
55
19
75
2f
65
30
36 | atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic | 09
03
61
43
0a
17
70
41
61
17
39 | (ID)
sis,
2a
55
6e
68
13
06
6f
31
6d
0d
31 | 86
04
72
0e
03
72
23
70
30
37 | 48
06
65
41
55
74
30
6c
39 | 86
13
72
73
6c
04
31
21
65
30
33 |
| | Pa
l=Chris
Payload | ylc
Tyr
va:
stch
1 #:
04
f7
02
62
74
62
02
62
74
62
06
06
40
35
33 | ad pe: lue 30 0d 4e 755 63 69 13 300 73 300 301 | #:
DEI
: CI
ch,
1 1
5a
72
68
65
10
0d
2a
6f
33
30 | 0
R_A:
st:
Leng
02
01
31
79
75
64
43
06
86
6c
32
36 | Le
SN1_
Out (
=
()
()
()
()
()
()
()
()
()
()
()
()
() | b ng
DN
5
5
5
5
6
3
0
5
6
3
0
5
6
3
0
5
6
3
0
5
6
3
0
5
6
3
0
5
6
3
0
5
6
3
0
5
6
3
0
5
5
6
3
0
5
5
6
3
0
5
5
8
6
7
3
8
6
7
3
8
6
7
3
1
5
5
8
6
7
3
1
5
5
8
6
7
1
5
5
8
6
7
1
5
5
8
6
7
1
5
5
8
6
7
4
3
3
3
1
5
5
5
5
5
5
5
5 | <pre>th:
P:
ATI
82
00
11
30
68
65
74
67
69
39
79</pre> | 131
rotc
, ot
01
30
06
13
31
6c
6f
03
0d
6f
30
31 | b 1
b 1 | Cen
Cen
02
a3
55
03
30
73
65
06
09
2e
5a
30 | cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
c | Eden
Po
Po
C
C
C
C
C
C
C
C
C
C | ate
30
30
13
07
03
31
53
47
14
74
33
03 | Eica
: 0
(C)
0d
09
0a
13
55
19
75
2f
65
30
36
55 | atic
a Te
0 6
0 6
4 3
0 c
0 4
3 0
7 0
4 3
7 8
1 e
3 0
0 4 | 09
03
61
43
0a
17
70
41
61
17
39
06 | (ID)
sis,
2a
55
6e
68
13
06
6f
31
6d
0d
31
13 | 86
04
74
72
0e
03
72
23
70
30
30
37 | 48
06
69
41
55
74
30
6c
39
32
4e | 86
13
72
73
6c
04
31
21
65
30
33
5a |
| | Pa
l=Chris
Payload | Tyr
val
it ch
it ch | ad pe: lue 30 0d 4e 75 63 69 13 300 73 300 310 320 330 300 133 300 133 300 133 300 301 302 303 303 304 305 306 307 308 309 313 | #:
DEJ
: CT
Ch,
1 1
82
01
5a
72
68
65
10
0d
2a
6f
33
30
30 | 0
R_As
n=rc
st:
Censor
02
02
01
31
79
75
64
43
06
86
6c
32
36
11 | Le
SN1_
Out of
a
48
04
13
31
72
20
75
03
48
75
33
5a
06 | <pre>provide state /pre> | <pre>th: P:
P3
82
00
11
30
68
65
74
04
f7
69
39
79
55</pre> | 131
rotc
01
30
06
13
31
6c
6f
03
0d
6f
30
31
04 | 1
1
1
1
1
1
1
1 | Cel
3 G_I
02
a3
55
03
30
73
65
06
09
2e
5a
30
13 | c c c c c c c c c c | Efica 02 0b 08 04 06 73 20 53 16 65 0d 06 43 | ate
30
30
13
07
03
31
53
47
14
74
33
03
61 | Eica
: 0
(C)
0d
09
0a
13
55
19
75
2f
65
30
36
55
6e | atic
1 Te
06
06
43
0c
04
30
70
43
70
43
1e
30
04
74 | 09
03
61
43
0a
17
70
41
61
17
39
06
65 | (ID)
2a
55
6e
68
13
06
6f
31
6d
0d
31
13
72 | 86
04
74
72
0e
03
72
23
70
30
37
02
62 | 48
06
65
41
55
74
30
6c
39
32
4e
75 | 86
13
72
73
6c
04
31
21
65
30
33
5a
72 |
| | Pa
l=Chris
Payload | ylc
Tyr
va:
stcl
f7
02
62
74
6c
0b
0f
06
40
35
33
31
79 | ad ye: 30 0d 4e 75 63 69 13 300 73 300 31
 | #:
DE1
: CT
Ch,
1 1
82
01
5a
72
68
65
10
0d
2a
65
10
0d
2a
6f
33
30
30
15 | 0
R_As
n=rc
st:
Const
02
01
31
79
75
64
43
06
86
6c
32
36
11
30 | Le
SN1_
Out
of
48
04
13
31
72
20
75
03
48
75
33
5a
06
13 | <pre>provide state /pre> | <pre>th: P: P: ATI 93 82 00 11 30 68 65 74 04 f7 69 39 79 55 03</pre>
 | 131
Type
01
30
06
13
31
6c
6f
03
0d
6f
30
31
04
55 | 2000
1=CS
b1
81
03
06
17
65
6d
13
01
6e
36
0b
08
04 | Central
Central
Central
Central
Central
Central
Central
Central
Central
Central
Central
Central
Central
Central
Central
Central
Central
Central
Central
Central
Central
Central
Central
Central
Central
Central
Central
Central
Central
Central
Central
Central
Central
Central
Central
Central
Central
Central
Central
Central
Central
Central
Central
Central
Central
Central
Central
Central
Central
Central
Central
Central
Central
Central
Central
Central
Central
Central
Contral
Central
Contral
Central
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contral
Contr
 | cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
cti
c | Iden Pc Pc 02 02 0b 08 04 06 73 20 53 16 65 0d 06 43 0c | ate
30
30
13
07
03
31
53
47
14
74
33
03
61
43 | fica
: 0
(C)
0d
03
13
55
19
75
2f
65
30
36
55
6e
68 | atic
1 Te
06
06
43
0c
04
30
70
43
78
1e
30
04
74
72 | 09
03
61
43
0a
17
70
41
61
17
39
06
65
69 | (ID)
2a
55
6e
68
13
06
6f
31
6d
0d
31
13
72
73
 | 86
04
74
72
0e
03
72
23
70
30
37
02
62
74 | 48
06
65
69
41
55
74
30
6c
39
32
4e
75
63 | 86
13
72
73
6c
04
31
21
65
30
33
5a
72
68 |
| | Pa
l=Chris
Payload | ylc
Tyn
va:
stcl
1 #:
04
f7
02
62
74
6c
0b
0f
06
40
35
33
31
79
75 | ad ye: 30 0d 4e 75 63 69 13 300 73 30 13 30 31 72 | #:
DEI
Ch,
1 1
82
01
5a
72
68
65
10
0d
2a
65
10
0d
2a
6f
33
30
30
15
63 | 0
R_As
n=r
st:
Cenc
02
01
31
79
75
64
43
06
86
62
32
36
11
30
68 | Lee
SN1_
Out of
a 48
04
13
31
72
20
75
03
48
75
33
5a
06
13
31 | <pre>>ngt
_DN
30
05
30
15
63
54
73
55
86
74
33
30
03
06
17</pre> | b :
P :
 | 131
TYT
01
30
06
13
31
6c
6f
30
31
6f
30
31
04
55
15 | 2000
1=CS
b1
81
03
06
17
65
6d
13
01
6e
36
0b
08
04
06 | Cen
Cen
Cen
02
a3
55
03
30
73
65
06
09
2e
5a
30
13
07
03 | c
c
c
c
c
c
c
c | Idea Pc 02 02 02 08 04 06 73 20 53 16 65 0d 06 43 0c 04 | ate 30 30 30 30 31 53 47 14 74 33 61 43 0a | fica
: 0
(C)
0d
09
0a
13
55
19
75
2f
65
30
36
55
6e
68
13 | atic
1 Te
06
06
43
0c
04
30
70
43
78
1e
30
04
74
72
0e | 09
03
61
43
0a
17
70
41
61
17
39
06
65
69
41 | (ID)
sis,
2a
55
6e
68
13
06
6f
31
6d
31
13
72
73
6c | 86
04
72
0e
03
72
23
70
30
37
02
62
74
6c | 48
06
65
41
55
74
30
6c
39
32
4e
75
63
69 | 86
13
72
73
6c
04
31
21
65
30
33
5a
72
68
65 |
| | Pa
l=Chris
Payload | ylc
Tyn
va:
stch
1 #:
04
f7
02
62
74
6c
0b
0f
06
40
35
33
31
79
75
64 | ad pe: lue 30 0d 4e 75 63 69 13 300 73 300 31 72 20
 | #:
DEI
Ch,
1 1
82
01
5a
72
68
65
10
0d
2a
65
10
0d
2a
6f
33
30
30
15
63
54 | 0
R_A:
st:
5
5
6
1
1
3
0
6
4
3
0
6
4
3
0
6
4
3
0
6
4
3
0
6
4
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
1
1
1
1
1
1
1
1
1
1
1
1 | Lecond Control
 | <pre>>ngt
_DN
30
05
30
15
63
54
73
55
86
74
33
30
03
06
17
65</pre> | b
b
c
c
c
c
c
c
c
c
 | 131
TYT
01
30
06
13
31
6c
6f
30
31
6f
30
31
04
55
69 | 2000
1=CS
b1
81
03
06
17
65
6d
13
01
6e
36
0b
08
04
06
73 | Cen
Cen
02
a3
55
03
30
73
65
06
09
2e
5a
30
13
07
03
31
 | 5
1
1
1
1
1
1
1
1 | Idea Pc 02 02 08 04 06 73 20 53 16 65 0d 06 43 0c 04 30 | ate
30
30
13
07
03
31
53
47
14
74
33
03
61
43
0a
0e | Eica
: 0
(C)
0d
09
0a
13
55
19
75
2f
65
30
36
55
6e
8
13
06 | atic
1 Te
06
06
43
0c
04
30
70
43
78
1e
30
04
74
72
0e
03 | 09
03
61
43
0a
17
70
41
61
17
39
06
65
69
41
55 | (ID)
sis,
2a
55
6e
68
13
06
6f
31
6d
0d
31
13
72
73
6c
04
 | 86
04
72
0e
03
72
23
70
30
37
02
62
74
6c
0b | 48
06
65
41
55
74
30
6c
39
32
4e
75
63
9
13 | 86
13
72
73
6c
04
31
21
65
30
33
5a
72
68
65
07 |
| | Pa
l=Chris
Payload | Y
Ty
va
i
t
i
i
i
i
i
i
i
i | ad ye: 30 0d 4e 75 63 69 13 300 73 30 73 30 73 31 72 20 53
 | #:
DEJ
Ch,
1
5a
72
68
65
10
0d
2a
65
10
0d
2a
65
10
0d
2a
65
10
0d
2a
65
5
10
0d
2a
65
5
4
30
30
30
47 | 0
R_As
st:
5
5
6
1
7
9
7
5
6
4
3
0
6
4
3
0
6
2
3
6
4
3
0
6
2
3
1
3
1
7
9
7
5
6
4
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
3
1
1
1
1
1
1
1
1
1
1
1
1
1 |
Le
SN1_
Out
48
04
13
31
72
20
75
03
48
75
03
48
75
33
5a
06
13
31
6c
4c | DN
3 0
05
30
15
63
54
73
55
86
74
33
06
17
65
61 | <pre>ch:
P:
ATI
30
68
65
74
69
39
79
55
03
30
73
62</pre>
 | 131
Tyr
01
30
06
13
31
6c
6f
03
0d
6f
30
0d
6f
31
04
55
15
69
31 | 5
1
1
1
1
1
1
1
1 | Cen
Cen
02
a3
55
03
30
73
65
06
09
2e
5a
30
13
07
03
31
30
 | rti
01
31
04
55
15
69
72
43
01
6e
17
09
0a
13
55
10
11 | Idea Pc 02 02 08 04 06 73 20 53 16 65 0d 0c 43 0c 04 30 06 | ati
ate
30
30
13
07
03
31
53
47
14
74
33
03
61
43
0a
0e
03 | Eica
: 0
(C)
0
0
0
0
0
0
0
0
0
0
0
0
0 | atic
1 Te
06
06
43
0c
04
30
70
43
70
43
78
1e
30
04
72
0e
03
04
 | 09
03
61
43
0a
17
70
41
61
17
39
06
65
69
41
55
03 | (ID)
sis,
2a
55
6e
68
13
06
6f
31
6d
0d
31
13
72
73
6c
04
13 | 86
04
72
0e
03
72
23
70
30
37
23
70
30
37
22
62
74
6c
0b
0a | 48
06
65
69
41
55
74
30
6c
39
32
4e
75
63
69
13
72 | 86
13
72
73
6c
31
21
65
30
33
5a
72
68
65
07
6f |
| | Pa
l=Chris
Payload | y
Ty
va
i
t
i
i
i
i
i
i
i
i | Dad Jae 30 0d 4e 75 63 69 13 300 73 30 73 31 72 20 53 74
 | #:
DEJ
ch,
1
5
a
72
68
65
10
0d
2a
65
10
0d
2a
6f
330
30
15
63
54
47
65 | 0
R_As
parts
st:
Construction
02
01
31
79
75
64
43
06
86
6c
32
36
11
30
68
65
5f
72 | Le
SN1_
SN1_
Out
of
SN1_
SN1_
Out of
SN1_
Out of
SN1_
SN1_
Out of
SN1_
SN1_
Out of
SN1_
Out of
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_SN1_
SN1_SN1_SN1_SN1_SN1_SN1_SN1_SN1_SN1_SN1_ | DN
3 0
05
30
15
63
54
73
55
86
74
33
00
03
06
17
65
61
41 | <pre>ch:
P:
ATI
93
82
00
11
30
68
65
74
69
39
79
55
03
30
73
62
54</pre>
 | 131
Tyr
01
30
06
13
31
6c
6f
03
0d
6f
30
31
04
55
15
69
31
49 | 5
5
5
5
5
5
5
5 | Cen
Cen
02
a3
55
03
30
73
65
06
09
2e
5a
30
13
07
03
31
30
5c
 | <pre>class : : : : : : : : : : : : : : : : : :</pre> | Idea Pc 02 02 08 04 06 73 20 53 16 65 0d 06 43 0c 04 30 06 04 | ati
ate
30
30
13
07
03
31
53
47
14
74
33
61
43
0a
0e
03
06 | Eica
: 0
(C)
0
0
0
0
0
0
0
0
0
0
0
0
0 | 1 Te
06
06
43
0c
04
30
70
43
70
43
70
43
70
43
70
43
72
0e
03
04
2a | 09
03
61
43
0a
17
70
41
61
17
39
06
65
69
41
55
03
86
 | (ID)
sis,
2a
55
6e
68
13
06
6f
31
6d
0d
31
13
72
73
6c
04
13
48 | 86
04
74
72
0e
03
72
23
70
30
37
02
62
74
6c
0b
0a
86 | 48
06
65
69
41
55
74
30
6c
39
32
4e
75
63
69
13
72
f7 | 86
13
72
73
6c
04
31
21
65
30
33
5a
72
68
65
07
6f
0d |
| | Pa
l=Chris
Payload | Y
Ty
val
t
t
t
t
t
t
t
t | ad lue 30 0d 4e 75 63 69 13 300 73 30 73 30 73 31 72 20 53 74 01
 | #:
DEJ
ch,
1
5a
72
68
65
10
0d
2a
6f
33
30
30
30
15
63
54
47
65
01 | 0
R_As
parts
5
5
6
1
1
3
0
2
0
2
0
2
0
2
0
2
0
2
0
2
0
2
0
2
0
2
0
2
0
2
0
2
0
2
0
2
0
2
0
2
0
2
0
2
0
2
0
2
0
2
0
2
0
2
0
2
0
2
0
2
0
2
0
2
0
2
0
2
0
2
0
2
0
2
0
2
0
2
0
2
0
2
0
2
0
2
0
2
0
0
2
0
6
4
3
0
6
2
2
3
0
6
2
2
3
6
2
2
3
0
6
2
2
3
0
6
2
2
3
0
6
2
2
3
6
2
2
3
6
2
2
3
6
2
2
3
6
2
2
3
6
2
2
3
6
2
2
3
6
5
5
5
7
2
2
3
6
2
3
6
5
5
5
7
2
2
3
6
5
5
5
7
2
2
0
5
5
5
7
2
0
5
5
5
7
2
0
5
5
5
5
5
5
5
5
5
5
5
5
5 |
Le
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_SN1_SN1_SN1_SN1_SN1_SN1_SN1_SN1_SN1_ | DN
3 0
05
30
15
63
54
73
55
86
74
33
00
03
00
17
65
61
41
03 | <pre>ch:
P:
ATI
93
82
00
11
30
68
65
74
04
f7
69
39
79
55
03
30
73
62
54
4b</pre>
 | 131
Tyr
01
30
06
13
31
6c
6f
03
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
31
04
55
15
69
31
49
00 | T b1 81 03 06 17 65 6d 13 01 6e 36 04 06 73 30 30 |
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen | <pre>class : : : : : : : : : : : : : : : : : :</pre> | Idea Pc 02 02 08 04 06 73 20 53 16 65 0d 06 43 0c 04 30 06 04 30 06 04 30 04 | ate
30
30
13
07
03
31
53
47
14
74
33
03
61
43
0a
0e
03
06
00 | Eica
: 0
(C)
0
0
0
0
0
0
0
0
0
0
0
0
0 |
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic
atic | 09
03
61
43
0a
17
70
41
61
17
39
06
65
69
41
55
03
86
ba | (ID)
sis,
2a
55
6e
68
13
06
6f
31
6d
0d
31
13
72
73
6c
04
13
48
ef | 86
04
74
72
0e
03
72
23
70
30
37
02
62
74
6c
0b
0a
86
ef | 48
06
65
69
41
55
74
30
62
32
4e
75
63
913
72
f7
96 | 86
13
72
73
6c
04
31
21
65
30
33
5a
72
68
65
07
6f
0d
01 |
| | Pa
l=Chris
Payload | Y
Tyr
val
i
i
i
i
i
i
i
i | ad Jue 30 0d 4e 75 63 69 13 300 73 300 73 30 13 30 13 30 13 31 72 20 53 74 01 fc
 | #:
DEJ
Ch, J
82
01
5a
72
68
65
10
0d
2a
6f
33
30
30
15
63
30
30
15
63
447
65
01
ac | 0
R_AS
D=rc
st:
Leng
02
01
31
79
75
64
43
06
86
6c
32
36
11
30
68
65
5f
72
05
80 |
Le
SN1_
SN1_
STA
48
04
13
31
72
20
75
03
48
75
33
5a
06
13
31
6c
4c
2d
00
fe | DN
5
5
3 0
05
3 0
15
6 3
5 4
73
5 5
86
74
3 3
06
17
6 5
61
41
03
c7 | <pre>ch:
P:
ATI
93
82
00
11
30
68
65
74
04
f7
69
39
79
55
03
30
73
62
54
4b
0b</pre>
 | 131
TYT
01
30
06
13
31
6c
6f
03
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
55
56
6f
9
31
0d
6f
55
69
31
0d
6f
6f
6f
6f
6f
6f
6f
6f
6f
6f | 1
1
1
1
1
1
1
1 |
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen | <pre>class : : : : : : : : : : : : : : : : : :</pre> | Idea Pc 02 02 08 04 06 73 20 53 16 65 0d 06 30 0c 04 30 0d 41 64 | ate
30
30
13
07
03
31
53
47
14
74
33
03
61
43
03
61
43
03
06
00
b4 | Eica
(C)
0d
09
0a
13
55
19
75
2f
65
30
36
55
6e
68
13
06
55
09
dc
96 |
1 Te
06
06
43
0c
04
30
70
43
78
1e
30
04
72
0e
03
04
2a
bf
90 | 09
03
61
43
0a
17
70
41
61
17
39
06
65
69
41
55
03
86
ba
7b | (ID)
sis,
2a
55
6e
68
13
06
6f
31
6d
0d
31
13
72
73
6c
04
13
48
ef
21 | 86
04
74
72
0e
03
72
23
70
30
37
23
70
30
37
02
62
74
6c
0b
86
ef
98 | 48
06
65
69
41
55
74
30
62
32
4e
75
63
91
3
72
f7
96
4 | 86
13
72
73
6c
04
31
21
65
30
33
5a
72
68
65
07
6f
01
e2 |
| | Pa
l=Chris
Payload | Tyr
val
t
t
t
t
t
t
t
t | Dad Jae 30 0d 4e 75 63 69 13 300 73 30 73 30 73 30 73 31 72 20 53 74 01 fc e | #: DEI
: ch , :
8
2
1
1
1
2
2
4
3
3
1
5
1
1
1
1
1
1
1
1
1
1 | 0
R_AS
D=rc
st:
Leng
02
01
31
79
75
64
43
06
86
62
32
36
11
30
68
65
5f
72
05
80
42
06
80
80
80
80
80
80
80
80
80
80 | Le
SN1_
SN1_
Control = 1
(1)
(1)
(1)
(1)
(1)
(1)
(1)
(1 | DN
5
5
3 0
05
3 0
15
6 3
5 4
73
5 5
8 6
74
3 3
003
06
17
6 5
6 1
03
c 7
e 2
c 7
e 2
c 7
c 7 | <pre>ch:
p3
82
00
11
30
68
65
74
69
39
79
55
03
30
73
62
40
00
73
62
54
40
00
73</pre> | 131
TYT
01
30
06
13
31
6c
6f
03
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
6f
6d
6f
6d
6d
6d
6d
6d
6d
6d
6d
6d
6d | T b1 81 03 06 17 65 6d 13 01 6e 36 04 06 73 30 24 | Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
CenCen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
Cen
CenCenCenCenCenCenCenCen | cti
i
o
i
o
i
o
i
o
i
o
i
o
i
o
i
o
i
o
i
o
i
o
i
o
i
o
i
o
i
o
i
o
i
o
i
o
i
o
i
o
i
o
i
o
i
o
i
o
i
o
i
o
i
o
i
o
i
o
i
o
i
o
i
i
o
i
o
i
o
i
o
i
o
i
i
i
i
i
i
i
i
i
i | Idea Pc 02 08 04 06 73 20 53 16 65 0d 06 30 0c 04 30 0c 04 30 0c 04 30 0cd 41 64 9c | ate
30
30
13
07
03
31
53
47
14
74
33
03
61
43
03
61
43
0a
06
00
b4
cf | Eica
: 0
0
0
0
0
0
0
0
0
0
0
0
0
0 | atic
a Te
b
c
c
c
c
c
c
c
c | 09
03
61
43
0a
17
70
41
61
17
39
06
65
69
41
55
03
86
ba
7b
78 | (ID)
sis,
2a
55
6e
68
13
06
6f
31
6d
0d
31
13
72
73
6c
04
13
8ef
21
44 | 86
04
72
0e
03
72
23
70
30
23
70
30
37
22
30
37
62
74
60
0a
86
f
98
56 | 48
06
59
41
55
74
30
62
32
40
53
40
53
22
57
63
63
72
75
63
72
79
64
10
60
50
57
50
50
50
50
50
50
50
50
50
50
50
50
50 | 86
13
72
73
6c
04
31
65
30
33
5a
65
07
6f
01
e2
61 |
| | Pa
l=Chris
Payload | Tyr Tyr val f7 02 62 74 62 74 60b 06 05 06 33 75 64 375 64 01 82 01 82 | ad 30 4e 75 63 69 13 300 73 30 73 30 73 30 73 30 73 30 73 30 73 30 73 30 73 30 73 30 73 30 74 01 69 42 42 42 42 42 42 42 42 42 42 42 42 43 44 45 46 47 47 48 </th <th>#: DEI
: Ch
: Ch
: Ch
: Ch
: : Ch
: : Ch
: : Ch
: : Ch
: : Ch
: : : Ch
: : : : : : : : : :</th> <th>0
R_As
n=rc
st:
Constant
02
01
31
79
75
64
43
06
86
6c
32
36
11
30
68
65
5f
72
05
80
4d
65
5f
72
05
80
4d
65
5f
72
05
80
60
60
75
75
80
75
75
80
75
75
80
75
75
80
75
75
80
75
75
80
75
75
80
75
75
80
75
75
80
75
75
80
75
75
80
75
75
80
75
75
80
75
75
80
75
75
80
75
75
80
75
75
80
75
75
80
75
75
80
75
75
80
80
80
80
80
72
75
80
80
80
80
72
75
80
80
80
80
80
80
80
80
80
80</th> <th>Le
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_SN1_
SN1_SN1_
SN1_SN1_SN1_SN1_SN1_SN1_SN1_SN1_SN1_SN1_</th> <th>DN
5
5
30
05
30
15
63
54
73
55
86
74
33
03
06
17
65
61
03
c7
2
80
2
2
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
17
1</th> <th><pre>ch:
P:
ATI
93
82
00
11
30
68
65
74
69
39
79
55
03
30
73
62
54
0b
74
25
4
24
0b
73</pre></th> <th>131
Tyr
01
30
06
13
31
6c
6f
03
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
6g
31
0d
6f
6g
30
0d
6f
6g
30
0d
6f
6g
30
0d
6f
6g
30
0d
6f
6g
8d
6g
8d
6g
8d
6g
8d
6g
8d
6d
6d
6d
6d
6d
6d
6d
6d
6d
6</th> <th>Topological De: bl 81 03 06 17 65 6d 13 01 6e 0b 08 04 06 73 30 243 243</th> <th>Cen
36
11
36
11
36
13
30
73
30
73
30
73
65
06
09
2e
5a
30
13
07
31
30
5c
48
fd
a
2
2
48
fd
1
30
5
5
5
5
5
5
5
5
5
5</th> <th>cti
i
i
i
i
b
i
i
i
i
i
i
i
i
i
i</th> <th>Idea Pc Fica 02 0b 08 04 06 73 20 53 16 65 0d 06 43 0c 04 30 0d 41 9cd</th> <th>ation 30 30 30 30 30 31 53 47 33 61 43 03 61 43 0a 0ce 03 06 00 b4 cff 61</th> <th>Eica
(C)
0d
09
0a
13
55
19
75
2f
65
30
55
6e
81
30
65
50
9d
b5
72
13
75
2f
55
0d
95
75
75
75
75
75
75
75
75
75
7</th> <th>atic
a Te
b
c
c
c
c
c
c
c
c</th> <th>09
03
61
43
0a
17
70
41
61
17
39
06
65
69
41
55
03
86
ba
70
86
ba
70
86</th> <th>(ID)
sis,
2a
55
6e
68
13
06
6f
31
6d
0d
31
13
72
73
6c
04
13
48
ef
21
44
50
6c
6c
6c
6c
6c
6c
6c
6c
6c
6c</th> <th>86
04
72
0e
03
72
23
70
30
23
70
30
23
70
30
23
70
23
70
23
70
23
70
23
70
26
2
74
6
6
27
4
6
6
20
8
6
98
6
02
20
20
20
20
20
20
20
20
20
20
20
20</th> <th>48
06
59
41
55
74
30
62
32
40
53
63
13
72
57
96
41
03</th> <th>86
13
72
73
6c
04
31
21
65
30
33
5a
72
68
65
07
6f
01
e2
61
01</th> | #: DEI
: Ch
: Ch
: Ch
: Ch
: : Ch
: : Ch
: : Ch
: : Ch
: : Ch
: : : Ch
: : : : : : : : : : | 0
R_As
n=rc
st:
Constant
02
01
31
79
75
64
43
06
86
6c
32
36
11
30
68
65
5f
72
05
80
4d
65
5f
72
05
80
4d
65
5f
72
05
80
60
60
75
75
80
75
75
80
75
75
80
75
75
80
75
75
80
75
75
80
75
75
80
75
75
80
75
75
80
75
75
80
75
75
80
75
75
80
75
75
80
75
75
80
75
75
80
75
75
80
75
75
80
75
75
80
75
75
80
75
75
80
80
80
80
80
72
75
80
80
80
80
72
75
80
80
80
80
80
80
80
80
80
80 | Le
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_
SN1_SN1_
SN1_SN1_
SN1_SN1_SN1_SN1_SN1_SN1_SN1_SN1_SN1_SN1_ | DN
5
5
3 0
05
3 0
15
6 3
5 4
73
5 5
8 6
74
3 3
03
06
17
6 5
6 1
03
c 7
2
8 0
2
2
1 7
1 | <pre>ch:
P:
ATI
93
82
00
11
30
68
65
74
69
39
79
55
03
30
73
62
54
0b
74
25
4
24
0b
73</pre> | 131
Tyr
01
30
06
13
31
6c
6f
03
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
6f
30
0d
6f
30
0d
6f
30
0d
6f
30
0d
6f
6g
31
0d
6f
6g
30
0d
6f
6g
30
0d
6f
6g
30
0d
6f
6g
30
0d
6f
6g
8d
6g
8d
6g
8d
6g
8d
6g
8d
6d
6d
6d
6d
6d
6d
6d
6d
6d
6 | Topological De: bl 81 03 06 17 65 6d 13 01 6e 0b 08 04 06 73 30 243 243 | Cen
36
11
36
11
36
13
30
73
30
73
30
73
65
06
09
2e
5a
30
13
07
31
30
5c
48
fd
a
2
2
48
fd
1
30
5
5
5
5
5
5
5
5
5
5 | cti
i
i
i
i
b
i
i
i
i
i
i
i
i
i
i | Idea Pc Fica 02 0b 08 04 06 73 20 53 16 65 0d 06 43 0c 04 30 0d 41 9cd | ation 30 30 30 30 30 31 53 47 33 61 43 03 61 43 0a 0ce 03 06 00 b4 cff 61 | Eica
(C)
0d
09
0a
13
55
19
75
2f
65
30
55
6e
81
30
65
50
9d
b5
72
13
75
2f
55
0d
95
75
75
75
75
75
75
75
75
75
7 | atic
a Te
b
c
c
c
c
c
c
c
c | 09
03
61
43
0a
17
70
41
61
17
39
06
65
69
41
55
03
86
ba
70
86
ba
70
86 | (ID)
sis,
2a
55
6e
68
13
06
6f
31
6d
0d
31
13
72
73
6c
04
13
48
ef
21
44
50
6c
6c
6c
6c
6c
6c
6c
6c
6c
6c | 86
04
72
0e
03
72
23
70
30
23
70
30
23
70
30
23
70
23
70
23
70
23
70
23
70
26
2
74
6
6
27
4
6
6
20
8
6
98
6
02
20
20
20
20
20
20
20
20
20
20
20
20 | 48
06
59
41
55
74
30
62
32
40
53
63
13
72
57
96
41
03 | 86
13
72
73
6c
04
31
21
65
30
33
5a
72
68
65
07
6f
01
e2
61
01 |

On the R	outer
debug cont.	00 1a ff ee 51 01 e7 dd 5d 16 dd d3 8d 37 de ac 64 ba 87 c2
	72 ca 23 ce 6c f9 3f 20 88 99 46 65 85 0e 55 a8 ac a7 ad 6b
	31 7f 72 b4 97 fb 4b b8 8b 96 eb fb a5 11 4f 37 98 d6 e7 06
	ac ce 1e 4f 46 79 e3 19 b9 af 98 7e 9c 1f ab a4 ba 3e ef fe
	92 ec f8 40 84 78 ec ac 0d 6a 71 b5 e7 d5 75 97 e1 76 e1 20
	1a 8b 53 53 1a 0a 49 0f ce c9 ad 38 08 ca 0a 37 c3 0c 84 3a
	ae 81 21 /C 34 80 50 23 2a Developed $\#_{1}$ 2 Longth, 60 $\#_{2}$ manage Gignature (CIC)
	Paytoad #: 2 Length: 00 Type: Signature (SiG) c^{7} 76 cf 72 ch ba 5d db co 39 48 at 7a 63 9f b7 cf d8 14 f4
	C_{1} 70 C1 72 CD ba 50 00 Ee 59 40 a4 7a 65 91 b7 C1 00 14 14 8a aa 9d 4a 67 b4 b4 c8 74 ea 46 9c 3e 5d 85 72 6d 6f 35 fd
	47 fd 50 6b 72 09 3c d9 61 e1 d8 07 01 1c e6 74 f5 f3 be f2
	0b a4 d9 29
	Payload #: 3 Length: 28 Type: Notification (N)
	00 00 00 01 01 10 60 02 56 a8 d0 65 ba 62 eb 36 76 d1 cf f5
	9a a5 28 c8
	ISAKMP MAIN exchange 13: New State: AUTHSENT
	ISAKMP MAIN exchange 13: New State: UP
	ISAKMP CORE: Exchange 13 done
	-
	ISAKMP QUICK: RESP: xchg 14: Started with peer 10.17.90.1
	ISAKMP QUICK exchange 14: New State: WAIT_HASH_SA_NONCE
	ISAKMP QUICK: RESP: xchg 14: COOKIE_I 1=8 v=56a8d065ba62eb36
	ISAKMP QUICK: RESP: xchg 14: COOKIE_R 1=8 v=76d1cff59aa528c8
	ISAKMP QUICK: RESP: xchg 14: MessageID=03836676
	ISAKMP QUICK: RESP: xchg 14: IV 1=8 v=1fb53490b31bba20
	ISAMP KX Message (decrypted)
	Yoha Type, OIICK(32) Ver, 10 Flags, 01
	MessageID: 03836c7b Total Length: 1112
	Pavload #: 0 Length: 24 Type: Hash (HASH)
	c2 73 ae c3 09 6c 54 aa 1b b6 c7 6f 3e 19 4a 00 0c 0e 14 b9
	Payload #: 1 Length: 1012 Type: Security Association (SA)
	DOI: IPSEC(0) Situation: 00000001
	Proposal#: 1 Protocol: ESP(3) #Trans: 2 SPI: b4736c0e
	Transform#: 1
	Transform Id 3DESOUTER(3)
	Group Description MODP768(1)
	Encapsulation Mode TRANSPORT(2)
	Authentication Algorithm MD5(1)
	Expiry KBytes 250000
	Expiry Seconds
	Transform Id 2DECOMPER(2)
	Group Description MODD768(1)
	Encapsulation Mode $TRANSPORT(2)$
	Authentication Algorithm SHA(2)
	Expiry KBytes
	Expiry Seconds

On the R	outer
debug cont	Proposal#: 2 Protocol: AH(2) #Trans: 1 SPI: b4736c0e
debug cont.	Transform#: 1
	Transform Id SHA(3)
	Group Description MODP768(1)
	Encapsulation Mode TRANSPORT(2)
	Authentication Algorithm SHA(2)
	Expiry KBytes 250000
	Expiry Seconds 3600
	<pre>Proposal#: 2 Protocol: ESP(3) #Trans: 1 SPI: 6cbf9d3d</pre>
	Transform#: 1
	Transform Id 3DESOUTER(3)
	Group Description MODP768(1)
	Encapsulation Mode TRANSPORT(2)
	Authentication Algorithm NULL(0)
	Expiry KBytes 250000
	Expiry Seconds 3600
	Proposal#: 3 Protocol: AH(2) #Trans: 1 SPI: D4/36CUe
	Transform Id MD5(2)
	Group Description MODP768(1)
	Encapsulation Mode TRANSPORT(2)
	Authentication Algorithm MD5(1)
	Expiry KBytes 250000
	Expiry Seconds
	Proposal#: 3 Protocol: ESP(3) #Trans: 1 SPI: 6cbf9d3d
	Transform#: 1
	Transform Id 3DESOUTER(3)
	Group Description MODP768(1)
	Encapsulation Mode TRANSPORT(2)
	Authentication Algorithm NULL(0)
	Expiry KBytes 250000
	Expiry Seconds 3600
	Proposal#: 4 Protocol: AH(2) #Trans: 1 SPI: b4736c0e
	Transform#: 1
	Transform Id SHA(3)
	Group Description MODP768(1)
	Encapsulation Mode TRANSPORT(2)
	Authentication Algorithm SHA(2)
	Expiry RBytes 250000
	Expiry Seconds
	mranaform#, 1
	$\frac{112}{2} \text{ Transform Id} \qquad 3 \text{ DESOUTER}(3)$
	Group Description MODP768(1)
	Encapsulation Mode
	Authentication Algorithm SHA(2)
	Expirv KBvtes 250000
	Expiry Seconds 3600
	Proposal#: 5 Protocol: AH(2) #Trans: 1 SPI: b4736c0e
	Transform#: 1
	Transform Id MD5(2)
	Group Description MODP768(1)
	Encapsulation Mode TRANSPORT(2)
	Authentication Algorithm MD5(1)
	Expiry KBytes 250000
	Expiry Seconds 3600

debug cont.	
	Proposal#: 6 Protocol: ESP(3) #Trans: 2 SPI: b4736c0e Transform#: 1
	Transform Id DES(2)
	Group Description MODP768(1)
	Encapsulation Mode TRANSPORT(2)
	Authentication Algorithm MD5(1)
	Evolvy KByteg 250000
	Expiry Coconda 2600
	Transform#: 2
	Transform Id DES(2)
	Group Description MODP/68(1)
	Encapsulation Mode TRANSPORT(2)
	Authentication Algorithm SHA(2)
	Expiry KBytes 250000
	Expiry Seconds 3600
	Proposal#: 7 Protocol: AH(2) #Trans: 1 SPI: b4736c0e Transform#: 1
	Transform Id SHA(3)
	Group Description MODP768(1)
	Encansulation Mode TRANSPORT(2)
	Authentication Algorithm SHA(2)
	Every KPut og
	Expiry Cocords
	Expiry Seconds 5000
	Transform#: 1
	Transform Id DES(2)
	Group Description MODP768(1)
	Encapsulation Mode TRANSPORT(2)
	Authentication Algorithm NULL(0)
	Expiry KBytes 250000
	Expiry Seconds
	Proposal#: 8 Protocol: AH(2) #Trans: 1 SPI: b4736c0e
	Transform#: 1
	Transform Id MD5(2)
	Group Description MODP768(1)
	Encapsulation Mode TRANSPORT(2)
	Authentication Algorithm MD5(1)
	Expiry KBytes 250000
	Expiry Seconds 3600
	Proposal#: 8 Protocol: ESP(3) #Trans: 1 SPI: 6cbf9d3d Transform#: 1
	Transform Id DES(2)
	Group Description
	Encapsulation Mode $TRANSPORT(2)$
	Authorization Algorithm NULL(0)
	Emiry KButes
	Expiry Abyces 250000
	Proposal#: 9 Protocol: AH(2) #Trans: 1 SPI: b4/36CUe Transform#: 1
	Transform Id SHA(3)
	Group Description MODP768(1)
	Encapsulation Mode TRANSPORT(2)
	Authentication Algorithm SHA(2)
	Expire KBytes 250000
	Expiry Seconds 3600
	Expiry Seconds

On the R	outer
debug cont.	Proposal#: 9 Protocol: ESP(3) #Trans: 1 SPI: 6cbf9d3d
	Transform#: 1
	Transform Id DES(2)
	Group Description MODP768(1)
	Encapsulation Mode TRANSPORT(2)
	Authentication Algorithm SHA(2)
	Expiry KBytes 250000
	Expiry Seconds 3600
	Proposal#: 10 Protocol: AH(2) #Trans: 1 SPI: b4/36cue
	Transform Id
	Crown Description MODP768(1)
	Encapsulation Mode TRANSPORT(2)
	Authentication Algorithm MD5(1)
	Expire KBytes 250000
	Expiry Seconds
	Proposal#: 10 Protocol: ESP(3) #Trans: 1 SPI: 6cbf9d3d
	Transform#: 1
	Transform Id DES(2)
	Group Description MODP768(1)
	Encapsulation Mode TRANSPORT(2)
	Authentication Algorithm MD5(1)
	Expiry KBytes 250000
	Expiry Seconds 3600
	Payload #: 2 Length: 24 Type: Nonce (NONCE)
	ae 00 08 37 7f ef 4a 65 33 27 2d 7f 3c 3e fe b1 b6 fb 1f cf
	Payload #: 3 Length: 12 Type: Identification (ID)
	Type: IPV4_ADDR ProtocolId: 17 Port: 1701
	Value: 10.17.90.1
	Payload #: 4 Length: 12 Type: Identification (ID)
	Type: IPV4_ADDK Protocolld: 1/ Port: 1/01
	Value. 10.17.90.101
	ISAKMP OUICK: RESP: xchg 14: rx msg 1: rec PROP 0: # 1, protid 3,
	outspi b4736c0e
	ISAKMP QUICK: RESP: xchg 14: rx msg 1: PROP 0 transforms good
	ISAKMP QUICK: RESP: xchg 14: rx msg 1: rec PROP 1: # 2, protid 2,
	outspi b4736c0e
	ISAKMP QUICK: RESP: xchg 14: rx msg 1: PROP 1 transforms good
	ISAKMP QUICK: RESP: xchg 14: rx msg 1: rec PROP 2: # 2, protid 3,
	outspi 6cbf9d3d
	ISAKMP QUICK: RESP: xchg 14: rx msg 1: PROP 2 transforms good
	ISAKMP QUICK: RESP: xchg 14: rx msg 1: rec PROP 3: # 3, protid 2,
	outspi b4736c0e
	ISAKMP QUICK: RESP: xchg 14: rx msg 1: PROP 3 transforms good
	ISAKMP QUICK: RESP: xchg 14: rx msg 1: rec PROP 4: # 3, protid 3,
	outspi 6cbf9d3d
	ISAKMP QUICK: RESP: xchg 14: rx msg 1: PROP 4 transforms good
	ISAKMP QUICK: RESP: xchg 14: rx msg 1: rec PROP 5: # 4, protid 2,
	ULSPI D4/30CUE
	ISAMMP QUICK: RESP: XCHQ 14: IX MSG 1: PROP 5 TRANSFORMS GOOD
	outeni 6abf9d3d
	TSAKMP OUTCK, RESP, yohg 1/, ry mag 1, DROD 6 transforms good
	Total gover, here, any 11, 14 may 1, 1601 0 cranstorms good

On the R	outer						
	ISAKMP	QUICK: RESP:	xchg	14:	rx msg	1:	rec PROP 7: # 5, protid 2,
debug conta	outspi	b4736c0e					
	ISAKMP	QUICK: RESP:	xchg	14:	rx msg	1:	PROP 7 transforms good
	ISAKMP	QUICK: RESP:	xchg	14:	rx msg	1:	rec PROP 8: # 5, protid 3,
	outspi	6cbf9d3d					
	ISAKMP	QUICK: RESP:	xchg	14:	rx msg	1:	PROP 8 transforms good
	ISAKMP	QUICK: RESP:	xchg	14:	rx msg	1:	rec PROP 9: # 6, protid 3,
	outspi	b4736c0e					
	ISAKMP	QUICK: RESP:	xchg	14:	rx msg	1:	PROP 9 transforms good
	ISAKMP	QUICK: RESP:	xchg	14:	rx msg	1:	rec PROP 10: # 7, protid 2,
	outspi	b4736c0e					
	ISAKMP	QUICK: RESP:	xchg	14:	rx msg	1:	PROP 10 transforms good
	ISAKMP	QUICK: RESP:	xchg	14:	rx msg	1:	rec PROP 11: # 7, protid 3,
	outspi	6cbf9d3d					
	ISAKMP	QUICK: RESP:	xchg	14:	rx msg	1:	PROP 11 transforms good
	ISAKMP	QUICK: RESP:	xchg	14:	rx msg	1:	rec PROP 12: # 8, protid 2,
	outspi	b4736c0e					
	ISAKMP	QUICK: RESP:	xchg	14:	rx msg	1:	PROP 12 transforms good
	ISAKMP	QUICK: RESP:	xchg	14:	rx msg	1:	rec PROP 13: # 8, protid 3,
	outspi			1 4		1	
	ISAKMP	QUICK: RESP:	xcng	14: 14:	rx msg	⊥: 1.	red DDOD 14. # 0 protid 2
	ISAMP	DUICK: RESP:	xcng	14:	IX MSG	т:	iec PROP 14: # 9, protid 2,
	TCARMD	OUTCK, PEGD.	vaha	11.	ry mca	1.	PPOP 14 transforms good
	TCAKMD	QUICK: RESP:	xchq	11.	ry mea	1.	rec PROP 15, # 9 protid 3
	outeni	6chf9d3d	ACTIG	TTT .	IN MBY	±•	iee ikoi is. # 5, piotid 5,
	TSAKMP	OUTCK · RESP	xcha	14.	rx msa	1.	PROP 15 transforms good
	ISAKMP	OUICK: RESP:	xchq	14:	rx msq	1:	rec PROP 16: # 10, protid 2,
	outspi	b4736c0e	5		5		
	ISAKMP	OUICK: RESP:	xchq	14:	rx msq	1:	PROP 16 transforms good
	ISAKMP	OUICK: RESP:	xchq	14:	rx msq	1:	rec PROP 17: # 10, protid 3,
	outspi	6cbf9d3d	- 5				
	ISAKMP	QUICK: RESP:	xchg	14:	rx msg	1:	PROP 17 transforms good
	ISAKMP	QUICK: RESP:	xchg	14:	rx msg	1:	SA proposals good
	ISAKMP	QUICK: RESP:	xchg	14:	rx msg	1:	payloads good:
	ISAKMP	QUICK: RESP:	xchg	14:	rx msg	1:	good

```
On the Router
        ISAKMP DOI: IPSEC: resp match pol:
debug cont.
           peerIP=10.17.90.1
           filtEnableFlag=00000075
           filtOpaqueFlag=0000000
           selectorsFromPktFlag=00000000
           lAddr=10.17.90.181
           1Mask=255.255.255.255
           lAddrLow=0.0.0.0
           lAddrHigh=0.0.0.0
           rAddr=10.17.90.1
           rMask=255.255.255.255
           rAddrLow=0.0.0.0
           rAddrHigh=0.0.0.0
           1Port=1701
           rPort=1701
           lName=
           rName=
           1AddrVer=4
           rAddrVer=4
        ISAKMP QUICK: RESP: xchg 14: Match Pol: 2 Local (prot 1) found - 0
        ISAKMP QUICK: RESP: xchg 14: Match Pol: 2 Remote (prot 1) found - 0
        ISAKMP QUICK: RESP: xchg 14: Match Pol: prop match try: 1
        00000000000000007d36d
        5c r 00000000000000007d2fb9c
        ISAKMP QUICK: RESP: xchg 14: Match Pol: matching (prot 2) props 1
        ISAKMP QUICK: RESP: xchg 14: Match Pol: (prot 2) tran match try: loc
        0 - \text{rem } 0
        ISAKMP DOI: IPSEC: ATTR match fail: authAlg 2 1
        ISAKMP QUICK: RESP: xchg 14: Match Tran: match fail
        ISAKMP QUICK: RESP: xchg 14: Match Pol: (prot 2) tran match try: loc
        0 - rem 1
        ISAKMP QUICK: RESP: xchg 14: Match Tran: match good
        ISAKMP QUICK: RESP: xchg 14: Match Pol: matched
        ISAKMP QUICK: RESP: xchg 14: proc 1: done good
        ISAKMP QUICK exchange 14: New State: SENDING_HASH_SA_NONCE
        ISAKMP Tx Message
             Cookies: 56a8d065ba62eb36:76d1cff59aa528c8
             Xchg Type: QUICK(32) Ver: 10 Flags: 00
             MessageID: 03836c7b Total Length: 164
             Payload #: 0 Length: 24 Type: Hash (HASH)
               fc b3 6e 08 fd 5b e6 58 d3 fa 0f 9b ed 71 e6 dd e4 53 1d 1f
             Payload #: 1 Length: 64 Type: Security Association (SA)
               DOI: IPSEC(0) Situation: 00000001
                 Proposal#: 1 Protocol: ESP(3) #Trans: 1 SPI: 9a764608
                   Transform#: 2
                    Transform Id ..... 3DESOUTER(3)
                    Group Description ..... MODP768(1)
                    Encapsulation Mode ..... TRANSPORT(2)
                    Authentication Algorithm ..... SHA(2)
                     Expiry KBytes ..... 250000
                     Expiry Seconds ..... 3600
```

	Payload #: 2 Length: 24 Type: Nonce (NONCE)
debug cont.	67 32 93 00 b6 3e da 1c e7 ca bf 2d 76 f3 e4 9f 70 45 02 b6
	Payload #: 3 Length: 12 Type: Identification (ID)
	Type: IPV4_ADDR ProtocolId: 17 Port: 1701
	Value: 10.17.90.1
	Payload #: 4 Length: 12 Type: Identification (ID)
	Type: IPV4_ADDR ProtocolId: 17 Port: 1701
	Value: 10.17.90.181
	ISAKMP Rx Message (decrypted)
	Cookies: 56a8d065ba62eb36:76d1cff59aa528c8
	Xchg Type: QUICK(32) Ver: 10 Flags: 01
	MessageID: 03836c7b Total Length: 52
	Payload #: 0 Length: 24 Type: Hash (HASH)
	10 28 f6 a5 73 07 0b 0c dd 33 6d d1 1e 6a 71 24 ab 88 33 87
	ISAKMP QUICK: RESP: xchg 14: rx msg 1: start
	ISAKMP QUICK exchange 14: New State: RECEIVING_MESSAGE
	ISAKMP QUICK: RESP: xchg 14: rx msg 2: payloads good:
	ISAKMP QUICK: RESP: xchg 14: rx msg 2: good
	ISAKMP CORE: Exchange 14 done
	TRAKME ONICK evaluates 14. New State, DONE

	Other confirmation commands.										
H V rc so	Here are commands to verify that both the ISAKMP and IPsec Security Associations of the VPN are established, that the PPP link crossing the VPN is open, and that a host specific route to the VPN remote host has been added over the VPN PPP link: Secoff Certificate VPN demo> sh isa sa										
Si	A Id	PeerAdd	ress	Expi: En	ry Lim cA. H	its - 1 ashA. I	hard/s Bytes	oft/used	Ē	Seco	nds
4	4 10.17.90.1 3DES SHA -/-/- 28800/27360/6										860/68
S	SA Id Policy Bundle State Protocol OutSPI										
I	nSPI	101109			Duii		acc	110000		JUCDII	
S	3] ecOff	L2tpVPN Certif	icate N	VPN d	5 emo> s	Valid h ppp	ESF	302	7463182	2591	.44244(
	Name		Enabl	led :	ifInde	x Over			CP		State
	 *ppp0		YE:	 S	 10				IPCP	() PENED
						tnl-383	326		LCP	()PENED
II De Ac	ecOff P Rou estin	Certif tes ation	icate V Mask	7PN d	emo> s	tnl-383 h ip ro NextHop	326 ou o	Flags	LCP s Inter	rface	DPENED
II De Di Di Pi	ecOff P Rou estin ge LCI/C ref	Certif tes ation irc.	icate V Mask Type	7 PN đ	emo> s 	h ip ro NextHop Proto	326 54 57 57 50 50	Flags	LCP s Inter Met:	rface rics)PENED
	ecOff P Rou estin ge LCI/C ref .0.0.	Certif tes ation irc.	icate N Mask Type 0.0.	7 PN d F	emo> s Policy	tnl-383 h ip r NextHop Proto 172.23	226 5u col 8.0.1	Flags Tag	LCP s Inter Met: vl	rface rics)PENED
	ecOff P Rou estin ge LCI/C ref .0.0. 69447 0.17. 69447	Certif tes ation irc. 0 90.0	icate N Mask Type 0.0. direct 255.	7PN d F 0.0 255.2	emo> s Policy 	tnl-383 h ip ro NextHop Proto 172.23 tatic 0.0.4	226 5u col 8.0.1 	Flags Tag	LCP 5 Inter Met: vl 1 vl	rface rics an2	360
II: 	ecOff P Rou estin ge LCI/C ref .0.0. 69447 0.17. 69447 72.28 69447	Certif tes ation irc. 0 90.0 .0.0	icate N Mask Type 0.0. direct 255. direct 255.	7PN d E 0.0 255.2 0 255.0	emo> s Policy 255.0 in 0.0	tnl-383 h ip ro NextHop Proto 172.23 tatic 0.0.0	226 Du 20 col 8.0.1 0.0 20 20 20 20 20 20 20 20 20 2	Flags Tag 	LCP 5 Inter Met: vl 1 vl 1 vl	rface rics an2 Lan1)PENED 360 0
 S: DD DD P: 0 0 0 10 10 10 10 10 	ecOff P Rou estin ge LCI/C ref .0.0. 69447 0.17. 69447 72.28 69447	Certif tes ation irc. 90.0 .0.0 .4.31	icate N Mask Type 0.0. direct 255. direct 255.	7PN d F 0.0 255.2 0 255.2	emo> s Policy 255.0 in 0.0 in 55.255	tnl-383 h ip ro NextHop Protoc 172.23 tatic 0.0.0 hterfac 0.0.0	226 Du 20 col 8.0.1 - 0.0 2e - 0.0 2e - 0.0	Flags Tag 	LCP 5 Inter Met: vl 1 vl 1 1 vl 1 vl	rface rics an2 Lan1 .an2	DPENED 360 0 0

Caveat statement

This How To document uses Allied Telesis routers, Windows XP, and the OpenSSL Open Source toolkit (also called OpenSSL tool), to demonstrate an X.509 Certificate VPN solution. The certificates used contain many fields of information, and to achieve this the solution also shows how to modify the OpenSSL tool's configuration file to support the Domain Component (DC) fields.

Usually certificates do not utilise all the fields of information that could be used in a certificate, but if you intend to use many fields please be aware of the following limitation.

OpenSSL tool limitation

Because of a suspected limitation of the OpenSSL tool we need to limit the length of the Certificate Signing Request file that the router creates. The string that you configure as **System Distinguished Name** needs to be limited to a string less than around **136** characters. This will ensure we create a Certificate Signing Request (CSR) file that an OpenSSL tool, acting as Certificate Authority, can sign.

Note that 136 characters is an ample amount for most certificate requirements.

Appendix

OpenSSL configuration file - adjustment to support additional fields

This How To document uses the OpenSSL tool to create certificates which contain many fields of information, including the additional Domain Component or DC fields. In order to support the use of the additional fields, the OpenSSL configuration file (.cnf) may need some changes. This appendix provides an extract from a modified configuration file:

[root@localhost URL_certs]# more /usr/local/ssl/openssl.cnf

... Search forward in the configuration file to find this section of the document, and alter as per example below...

```
< cut >
# For the CA policy
[ policy_match ]
countryName
                      = match
stateOrProvinceName = match
organizationName = match
organizationalUnitName = optional
commonName = supplied
                      = optional
emailAddress
domainComponent = optional
# For the 'anything' policy
# At this point in time, you must list all acceptable 'object'
# types.
[ policy_anything ]
localityName = optional
organizationName = optional
organizationalUnitName = optional
commonName = supplied
emailAddress
                      = optional
domainComponent
                      = optional
*****
[req]
default_bits = 1024
default_keyfile = privkey.pem
distinguished_name = req_distinguished_name
= req_attributes
x509_extensions = v3_ca # The extentions to add to the self signed cert
# Passwords for private keys if not present they will be prompted for
# input_password = secret
# output_password = secret
# This sets a mask for permitted string types. There are several options.
# default: PrintableString, T61String, BMPString.
# pkix : PrintableString, BMPString.
# utf8only: only UTF8Strings.
# nombstr : PrintableString, T61String (no BMPStrings or UTF8Strings).
# MASK:XXXX a literal mask value.
# WARNING: current versions of Netscape crash on BMPStrings or UTF8Strings
```

```
# so use this option with caution!
string_mask = nombstr
# req_extensions = v3_reg # The extensions to add to a certificate request
[ req_distinguished_name ]
0.domainComponent
                               = Domain Component 1 (e.g. nz)
0.domainComponent_default
                               = nz
                               = Domain Component 2 (e.g. co)
1.domainComponent
1.domainComponent_default
                               = co
                               = Domain Component 3 (e.g. alliedtelesis)
2.domainComponent
2.domainComponent_default
                               = alliedtelesis
countryName
                               = Country Name (2 letter code)
countryName_default
                               = NZ
                               = 2
countryName_min
countryName_max
                               = 2
stateOrProvinceName
                              = State or Province Name (full name)
stateOrProvinceName_default
                              = Canterbury
localityName
                               = Locality Name (eg, city)
                               = Christchurch
localityName_default
                               = Organization Name (eg, company)
0.organizationName
0.organizationName_default
                               = Your Organization
# we can do this but it is not needed normally :-)
#1.organizationName
                               = Second Organization Name (eg, company)
#1.organizationName_default
                               = World Wide Web Pty Ltd
                               = Organizational Unit Name (eg, section)
organizationalUnitName
organizationalUnitName_default = SW AW Sustaining
commonName
                               = Common Name (eg, YOUR name)
                               = Your Name
commonName_default
commonName_max
                               = 64
emailAddress
                               = Email Address
emailAddress_max
                               = 64
# SET-ex3
                               = SET extension number 3
[ req_attributes ]
challengePassword
                               = A challenge password
challengePassword_min
                               = 4
challengePassword_max
                               = 20
unstructuredName
                               = An optional company name
<cut>
```

USA Headquarters | 19800 North Creek Parkway | Suite 100 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895 European Headquarters | Via Motta 24 | 6830 Chiasso | Switzerland | T: +41 91 69769.00 | F: +41 91 69769.11 Asia-Pacific Headquarters | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830 www.alliedtelesis.com

© 2009 Allied Telesis, Inc. All rights reserved. Information in this document is subject to change without notice. Allied Telesis is a trademark or registered trademark of Allied Telesis, Inc. in the United States and other countries. All company names, logos, and product designs that are trademarks or registered trademarks are the property of their respective owners.

C613-16144-00 REV A

Connecting The IP World

