NETOP™ RemoteControl Secure Remote Management and Support

Secure tunnel for remote application port access and control



Contents

1	Introduction	. 1
2	Illustration of workflow	. 2
3	Technical requirements and recommendations	. 3
4	Set up a system with a secure Tunnel	.4
5	Connect using the Tunnel	. 5

1 Introduction

To extend the support and management capabilities within the Netop Remote Control solution, a new Tunnel function has been implemented. The Tunnel establishes a secure connection between the Guest and Host and allows application ports to be redirected from the Host to the Guest through the Tunnel.

This allows the Guest to run local applications while interacting with the connected Host and without having to remote control the Host machine.

While not exclusive to such environments, the Tunnel is ideally suited to environments where no traditional desktop is available for use with standard remote control (screen, keyboard and mouse control); however support and system administrative tasks can still be carried out remotely while conforming to industry regulatory standards such as PCI-DSS, HIPAA and FIPS.

Examples of such environments include embedded Linux systems where operating machinery and hardware contains a streamlined version of a Linux operating system, for example, fuel dispensers and retail systems. In addition, enterprises can also take advantage of the Tunnel for managing and supporting their Linux Desktops and Servers using common applications and services such as Shell clients, HTTP and SFTP.



The Guest's ability to use the Tunnel along with the associated ports can be governed by the central Netop Security Server solution. This allows organizations to apply granular access privileges. Even when remote systems have a desktop, it may not be required to give Guest users full remote control access on certain machines but limit their ability to use certain application ports through the Netop Tunnel.

Any traffic sent through the established Tunnel can be secured with up to 256-bit AES encryption.

Identity management can be centrally governed using Directory Services, RSA SecurID, Smartcards, RADIUS or Netop proprietary authentication.

Granular access permissions controlled centrally using Netop Security Server.

A full audit trail can be maintained centrally, including physical session recordings.

This technical paper lists the technical requirements, describes how to set up the Tunnel and how to establish a Tunnel session. For basic information about the Netop Remote Control solution, please refer to Netop Remote Control User's Guide <add link> and Netop Remote Control Administrator's Guide <add link>

2 Illustration of workflow

Step 1 Guest initiates Secure Tunnel to any Windows, Linux or Mac machine running the Host



Data within the Netop Tunnel is secured with 256-bit AES encryption for **confidentiality**, **integrity** checking using 256-bit SHA HMAC and **authenticity** using key exchanges via a combination of 2048-bit Diffie-Hellman, 256-bit AES and 512-bit SHA.

Step 2 Host authenticates Guest using Security Server



When using the Security Server, the Guest can be validated against a variety of authentication

Methods including Directory Services, Windows Security Management, Netop proprietary, Smart Cards and RSA SecurID.

Step 3 After successful authentication and appropriate permissions assigned, the Guest can use applications through the Secure Tunnel



After the Guest is authenticated, the Security Server dictates which local ports on the Host machine can be redirected to the Guest through the Tunnel. For each port redirected from the Host, a random available local port is assigned to the Guest.

Step 4 Guest sessions are auditable through log events and physical recordings using Security Server



The Netop applications can log audit data to multiple locations including local log files or centrally including the Security Server. Optional physical recordings are created by the Guest and stored in a pre-define location for later playback.

3 Technical requirements and recommendations

Netop Remote Control Guest	The Tunnel functionality is available in the Windows, Linux and Mac Guest.
Netop Remote Control Host	The Guest can establish a Tunnel with a Host running on Windows, Linux and Mac.
Communication profiles	The Tunnel can be established using WebConnect, TCP and UDP.
Netop Security Server	While the Tunnel session functionality is available in the basic Host for Linux and Mac, we highly recommend using Netop Security Server for centralized identity management, audit trails and granular control over port assignments.
	The Security Server is also a pre-requisite when using the Tunnel with Hosts running in a Windows environment

4 Set up a system with a secure Tunnel

In Netop Security Manager, create a role with the appropriate permissions.

Name Linux A	dministrators		
Description Membe	s from the Linux Ad	min team	
Permissions Confirm Access			
		Allow	Deny
Remote control (View)			
Use keyboard and mou	е		
Lock keyboard and mo	se		
Blank the screen			
Transfer the clipboard			
Execute command (Restar)		
Request chat			
Request audio chat			
Request video			
Send files to host			
Receive files from host			
Run programs			
Redirect print			
Remote manage			
Retrieve inventory			
Demonstrate			
Send message			
Join multi Guest session			
Act as multi Guest session.	dministrator		
Tunnel		v	
Allowed Ports	6501,80,20-22		
Blocked Ports	2000-2500		

Select the **Tunnel** option to enable the port fields.

Only the **Allowed Ports** field is mandatory. Type one or more individual ports separated by comma or a range of ports with a hyphen.

These are the ports that the Guest user will be allowed to control through a secure tunnel. By default any other ports are not allowed.

If you specify a wide range or ports, say 2000-2500, you can use the **Blocked Ports** to specify exceptions to the allowed ports list. For example, you could specify 2300-2350 to indicate that these ports cannot be controlled.

Next make the role assignment and identify Guest computer, Host computer and role.

Retop Security Manager - Logged on	to ODBC data source "Net	Op_Security_Evaluation"		
File Records Edit View Options H	Help			
🕷 🚓 🤼 🛰 🧖 🌡 😚 🖆 🛍	₽ <u>_</u> :- ::: !!!			
Where LIKE	▼ A%	-		
🖃 🐺 Netop Security Management	Guest	Host	Role	Enabled
😑 🍓 Security Settings	Cn=domain admins	🙈 LINUX HOSTS 📖	Full Control	1
Role Assignments	cn=1st level support.	REDHAT HOST	Linux Administrators	
🖓 Roles				•
Security Policies				
E Logging				
Security Log				
Netop Log				
Active Sessions				
G Scheduling				
Scheduled Jobs				
Guert IDc				
Guest ID Groups				
Host IDs				
Host ID Groups				
Netop Properties				
📄 🖳 Directory Services Definitions				
🔄 🥳 Users				
Groups				
Directory Services				
🔄 Organizational Units	•			Þ
r Ready			NU	M

Note For general information on Netop Security Server and Netop Security Manager, refer to Netop Remote Control Administrator's Guide, section 2 <add link>

5 Connect using the Tunnel

Select the Host you want to connect to and click the **Tunnel** icon on the toolbar:



Once the Guest has been authenticated, the Tunnel console will appear confirming which remote ports are available (as set up in the Security Manager) and what randomly assigned local ports can be used by the Guest:

Time	Description	
15:28:55	Tunnel created:	
15:28:55	local port 52304 - remote port 20	
15:28:55	local port 52305 - remote port 21	
15:28:55	local port 52306 - remote port 22	
15:28:55	local port 52307 - remote port 80	
15:28:55	local port 52308 - remote port 6501	

If ports 80 or 6501 are allowed when connecting to a Linux Host, the Tunnel console will display shortcut buttons to the Guest's default web browser and the built-it Netop Shell client (SSH), for example:

192.168.1.7	72 - Netop Shell			
Skipping s > Runnir > Packa > Packa > Packa > Finish Dependenci	ecurity plug ng transactio nge gtk2.i386 nge perl.i386 nge sos.noarc ned Dependenc Les Resolved	in, no data in check 0:2.10.4-21.el5_7.7 set 4:5.8.8-32.el5_7.6 set in 0:1.7-9.54.el5_7.1 set y Resolution	to be updated to be updated to be updated	•
Package	Arch	Version	Repository	Size
Updating: gtk2 perl sos Transactio	i386 i386 noarch on Summary	2.10.4-21.e15_7.7 4:5.8.8-32.e15_7.6 1.7-9.54.e15_7.1	rhel-i386-client-5 rhel-i386-client-5 rhel-i386-client-5	6.5 M 12 M 151 k
Install Upgrade Total dowr Is this ok	0 Packag 3 Packag nload size: 1 c [y/N]:]	ре (з) ре (з) 8 М		E

Third-party Shell access is still available when port 22 is redirected through the Tunnel. For example, the above connection also allows a local Shell client, i.e. Putty, to be used to administer the Host machine through the local port 52306:

Reputry Configuration		×
Puttry Configuration Category: Session Logging Terminal Rell Features Window Pelarance Behaviour Translation Selection Colours Data	Basic options for your PuTTY so Specify the destination you want to connect Host Name (or IP address) localhost Connection type: Raw Telnet Rlogin SS Load, save or delete a stored session Saved Sessions Default Settings	ect to Port 52306 H O Serial Load Save Delete
About	Always Never Only on C	Clean exit

The Tunnel console will continue to update with any processes or applications that are using ports through the active Tunnel session:

Time	Description	
15:28:55	Tunnel created:	
15:28:55	local port 52304 - remote port 20	
15:28:55	local port 52305 - remote port 21	
15:28:55	local port 52306 - remote port 22	
15:28:55	local port 52307 - remote port 80	
15:28:55	local port 52308 - remote port 6501	
15:30:46	Connection accepted - process name: putty.exe, local port: 52306	

Netop Tunnel activity is logged to the previous locations including the Security Server for centralized management. When using the Tunnel with the Recording feature enabled on the Guest, the Guest will capture a full screen recording and store this in the location defined by the Guest settings.