Firewall and Proxy Server considerations when using Netop’s WebConnect /WebConnect 3.0 communicatio

Article Number: 182 | Last Updated: Fri, Oct 20, 2017 9:29 AM

Â When configuring Netop Remote Control (or Netop OnDemand) to use the WebConnect /WebConnect 3.0 commu
instances when access must be allowed through a company's proxy server and/or firewall. **Netop Hosted WebConn**

Data traffic protocols must be allowed outbound through a firewall to the Connection Manager and Connect
communication to the WebConnect Connection Manager is HTTP:80 and/or HTTPS:443.Â Outbound commu
WebConnect Connection Servers is TCP:6502 and/or HTTP(TCP encapsulated):80.

Rules or exceptions may need to be created that allow communication through a proxy server to communic
Connection Manager and Connection Server modules.

Netop's hosted WebConnect environment offers three separate environments.Â Connection Manager URL i
based on their region.Â Here is a list of I.P. addresses that you may refer to if you need to created firewall o
WebConnection communication.

For the European (EU) WebConnect service, the following communication needs to be allowed: Outbound H
HTTP:80 to the Connection Manager (webconnect01eu.netop.com), having the public IP 54.246.197.203 Outbou
HTTP(TCP encapsulated):80 to the first Connection Server, having the public IP 54.246.236.65 Outbound TCP:6502
encapsulated):80 to the second Connection Server, having the public IP 46.51.206.56 For the North American (US)
following communication needs to be allowed: Outbound HTTPS:443 and/or HTTP:80 to the Connection Manager (w
.netop.com), having the public IP 54.200.219.230 Outbound TCP:6502 and/or HTTP(TCP encapsulated):80 to the fir
having the public IP 54.200.190.121 Outbound TCP:6502 and/or HTTP(TCP encapsulated):80 to the second Connec
public IP 52.24.214.0 **Netop Hosted WebConnect 3.0** Data traffic protocols must be allowed outbound through a fi
Manager and Connection Server.Â Outbound communication to the WebConnect 3.0 Connection Manager is HTTP
communication to the WebConnect 3.0 Connection Servers is TCP:6502 and/or HTTP(TCP encapsulated):80.

Rules or exceptions may need to be created that allow communication through a proxy server to communicate with
Connection Manager and Connection Server modules.

Netop's hosted WebConnect 3.0 environment offers three separate environments.Â Connection Manager URL is as
their region.Â Here is a list of I.P. addresses that you may refer to if you need to created firewall or proxy rules to all
communication.

For the European (EU) WebConnect 3.0 service, the following communication needs to be allowed: Outbound HTT
Manager (webconnect3**eu**.netop.com), having the public IP 52.208.116.223 Outbound TCP:443 to the first Connecti
public IP 52.48.144.190 Outbound TCP:443 to the second Connection Server, having the public IP 52.51.33.226 Fo
WebConnect 3.0 service, the following communication needs to be allowed: Outbound HTTPS:443 to the Connectio
us.netop.com), having the public IP 52.24.48.84 Outbound TCP:443 to the first Connection Server, having the public
Outbound TCP:443 to the second Connection Server, having the public IP 52.41.220.110

Posted - Thu, Nov 17, 2011 9:03 PM.
Online URL:
https://kb.netop.com/article/firewall-and-proxy-server-considerations-when-using-netop-s-webconnect-webconnect-3