Where do you Install Cyber Predator on your Network so you can collect all the data packets?

The purpose of this document is to demonstrate to a new or existing Cyber Predator user where in a network the system must be installed so that it works properly.

The document contains pictures of various sample network diagrams and shows you where to install the software. It also shows any other changes that you may need to make.

Table of contents:

Introduction 2
Cyber Predator installed on a small LAN which has one or more switched Hubs 4
Cyber Predator installed to monitor a small part of a bigger network (Workgroup) 5
Cyber Predator installed to monitor a small part of a bigger network (Workgroup) that has switched hubs 6
Cyber Predator installed to monitor one site of a multi-site network 7
Cyber Predator installed to monitor many sites of a multi-site network (Option 1) 8
Cyber Predator installed to monitor many sites of a multi-site network (Option 2) 9
Cyber Predator installed to monitor many sites of a multi-site network that has switched hubs (Option 1) 10
Cyber Predator installed to monitor many sites of a multi-site network that has switched hubs (Option 2) 11
Cyber Predator installed to monitor all sites of a multi-site network 12
Cyber Predator installed to monitor all sites of a multi-site network that has switched hubs 13
Cyber Predator installed to monitor many sites of a multi-site network that has separate internet access for each site 14
Cyber Predator installed to monitor many sites of a multi-site network that has separate internet access for each site and switched hubs 15

Introduction

Cyber Predator has two main components, the Data Collector (DC) and the Management Console (MC). The DC collects all the data and writes it to the database. The MC provides a user-friendly graphical interface for the system owner to perform configuration and reporting tasks.

The DC acts like a network sniffer, passively listening to the traffic on the LAN. In order to collect the data you want it to collect, that data has to be present on the part of the LAN the DC machine is listening to.

Switched hubs reduce overall traffic on a network by only sending the data to the port(s) it needs to go to, whereas NON-switched hubs send the data to all ports. For this reason switched hubs cause a problem for network sniffers and Cyber Predator because they don't send the data to all ports, therefore the DC doesn't see it and cannot collect it.

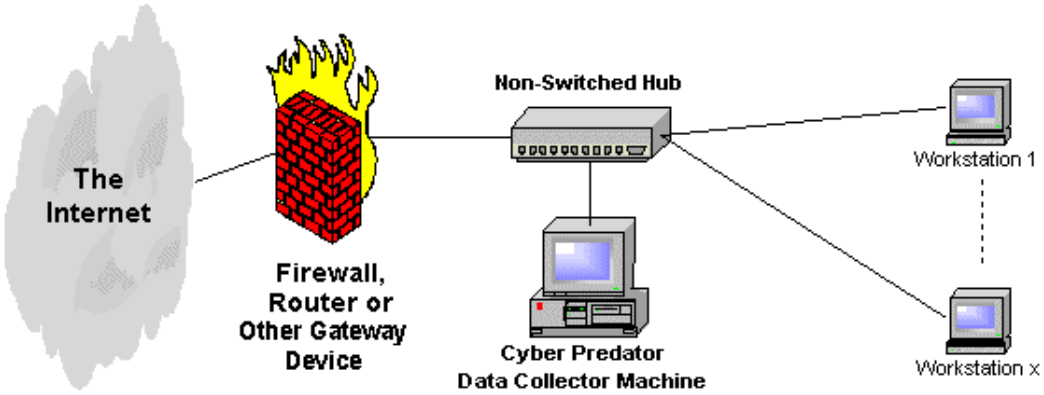
To overcome this problem, the basic principal is to install the DC onto a machine that is plugged into a NON-switched hub, and insert that hub into the network where all the Internet traffic will be. This is always the egress or access point that is usually a router or a firewall.

The network diagrams below show various network scenarios and provide guidance as to where to install the DC and NON-switched hub.

If you have a network topology that isn't covered by any of these, and are having difficulty collecting all your data, please forward a copy of your network including internet access point details and we will be happy to advise you.

Network Routers have been removed from some of the diagrams below to simplify them; in a real world situation they would of course be required.

Cyber Predator installed on a small LAN that has one or more NON-switched Hubs

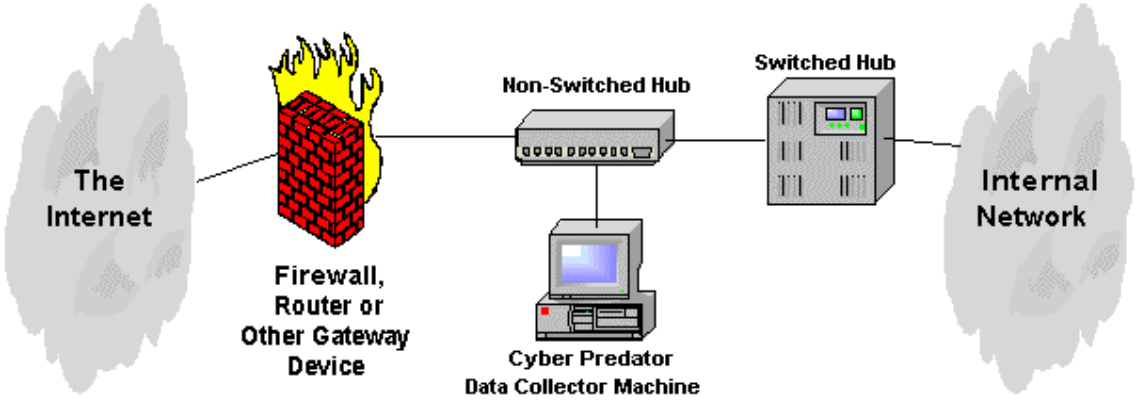


In this situation the Cyber Predator Data Collector Software could be installed onto any machine in the network, this is possible because the network isn't switched, therefore the location of the DC could be anywhere and would probably be on the sysadmin/managers PC.

All the traffic from workstations 1…x would be visible to the DC machine via the NON-switched hub.

The Cyber Predator Management Console Software would most probably be installed onto the same machine as the Data Collector but it could be installed on any machine on the network that has TCP/IP connectivity to the DC machine.

Cyber Predator installed on a small LAN which has one or more switched Hubs



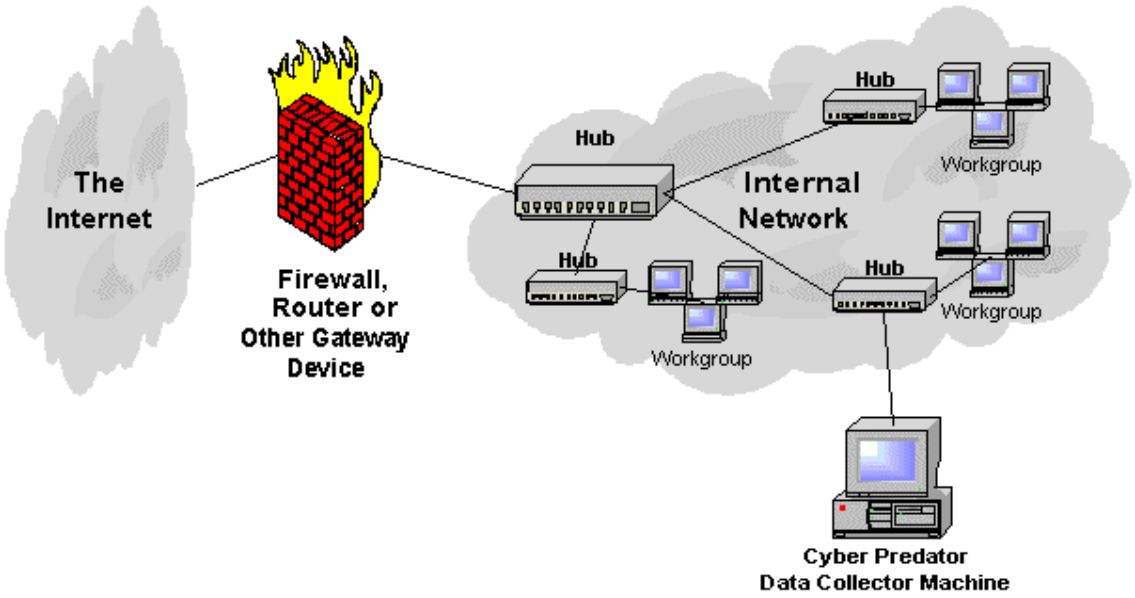
Because switched hubs do such a good job at hiding the traffic from the remaining switch ports, it is necessary to place a NON-Switched hub between the main network and your Internet access device. In this situation the Cyber Predator Data Collector Software would be installed onto a machine connected to that NON-switched hub and all the traffic from the internal workstations would be visible to the DC machine via the NON-switched hub.

The Cyber Predator Management Console Software could be installed onto any other machine that has TCP/IP connectivity to the DC machine.

Alternatively you could install the MC onto the same machine as the Data Collector, and remotely manage the machine via remote control software such as Windows 2000 Terminal Services, Windows XP Remote Desktop, Funk Proxy, PC Anywhere, VNC or other.

All the traffic from workstations on the internal network to the Internet would have to go via the NON-switched hub to access the Internet and therefore would be visible to the DC machine via the NON-switched hub.

Cyber Predator installed to monitor a small part of a bigger network (Workgroup)

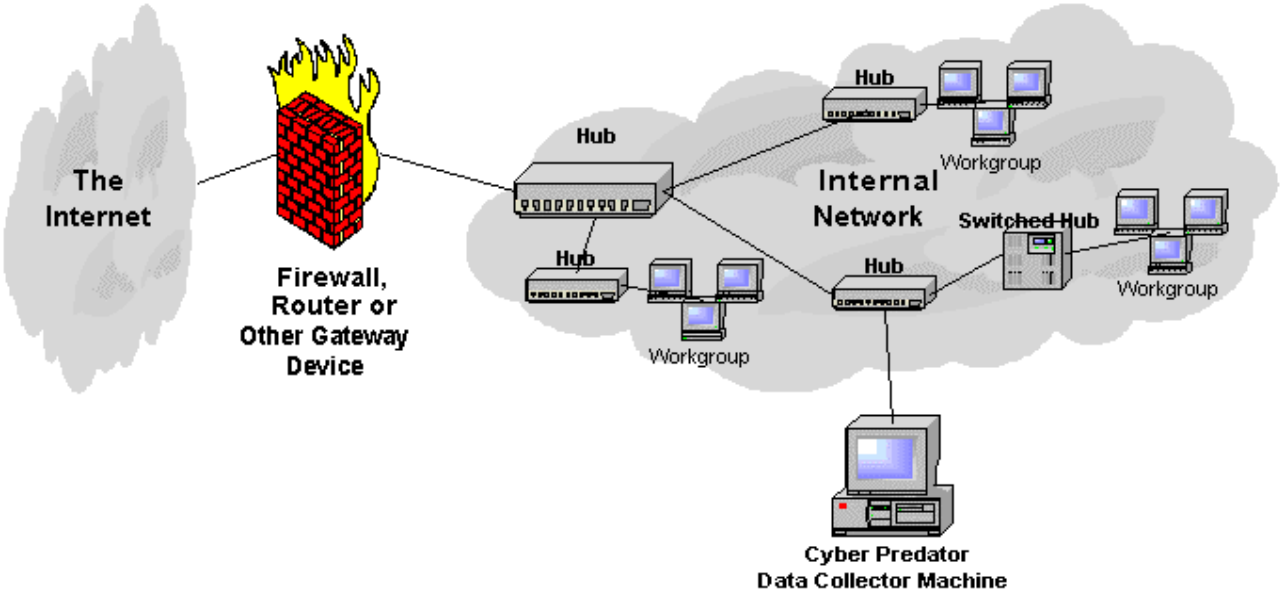


In this situation the Cyber Predator Management Console Software could be installed onto any other machine that has TCP/IP connectivity to the DC machine. Alternatively you could install the MC onto the same machine as the Data Collector, and remotely manage the machine via remote control software such as Windows 2000 Terminal Services, Windows XP Remote Desktop, Funk Proxy, PC Anywhere, VNC or other.

Here the Data Collector is placed in between the PCs that need monitoring and the Internet access device. The hub that the DC plugs into must be NON-Switched, because switched hubs do such a good job at hiding the traffic from the remaining switch ports. It is necessary to place a NON-Switched hub between the network to be monitored and the route to your Internet access device.

All the traffic from the required workgroup workstations would be visible to the DC machine via the NON-switched hub.

Cyber Predator installed to monitor a small part of a bigger network (Workgroup) that has switched hubs

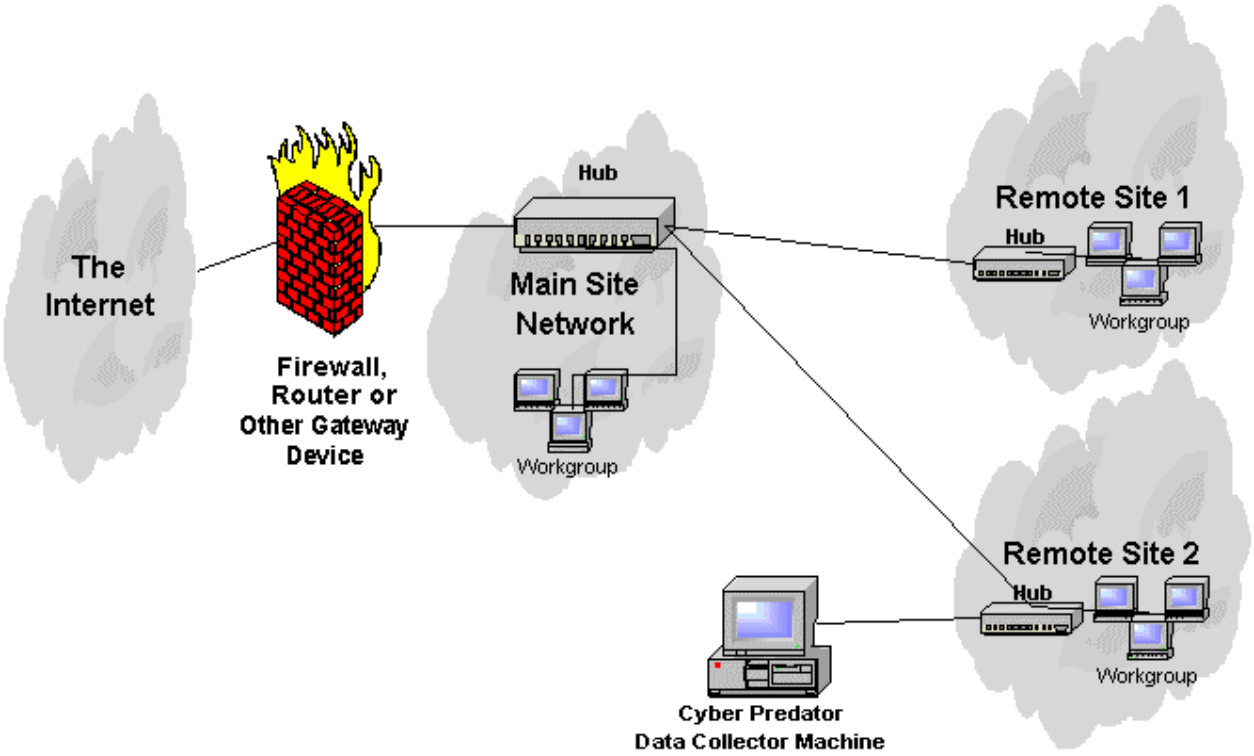


In this situation the Cyber Predator Management Console Software could be installed onto any other machine that has TCP/IP connectivity to the DC machine. Alternatively you could install the MC onto the same machine as the Data Collector, and remotely manage the machine via remote control software such as Windows 2000 Terminal Services, Windows XP Remote Desktop, Funk Proxy, PC Anywhere, VNC or other.

Here the Data Collector is placed in between the PCs that need monitoring and the Internet access device. The hub that the DC plugs into must be NON-Switched, because switched hubs do such a good job at hiding the traffic from the remaining switch ports. It is necessary to place a NON-Switched hub between the network to be monitored and the route to your Internet access device.

All the traffic from the required workgroup workstations would be visible to the DC machine via the NON-switched hub.

Cyber Predator installed to monitor one site of a multi-site network

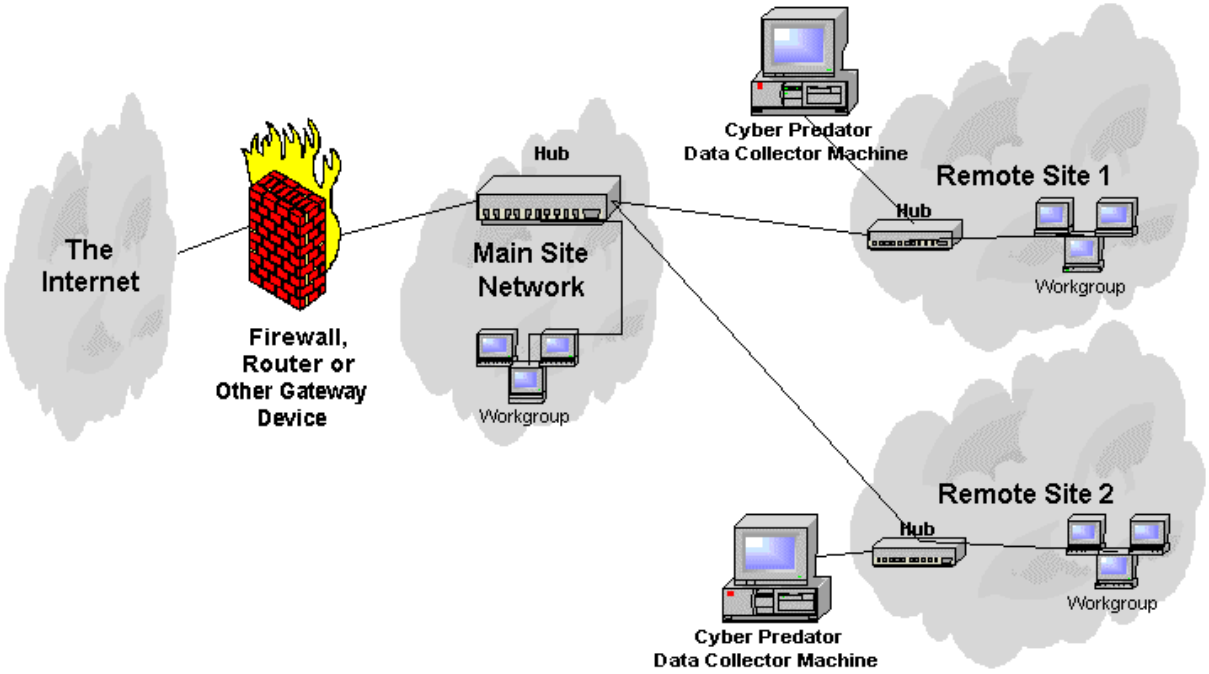


In this situation the Cyber Predator Management Console Software could be installed onto any other machine that has TCP/IP connectivity to the DC machine. Alternatively you could install the MC onto the same machine as the Data Collector, and remotely manage the machine via remote control software such as Windows 2000 Terminal Services, Windows XP Remote Desktop, Funk Proxy, PC Anywhere, VNC or other.

Here the Data Collector is placed in between the PCs that need monitoring and the Internet access device. The hub that the DC plugs into must be NON-Switched, because switched hubs do such a good job at hiding the traffic from the remaining switch ports. It is necessary to place a NON-Switched hub between the network to be monitored and the route to your Internet access device.

All the traffic from the required workgroup workstations would be visible to the DC machine via the NON-switched hub.

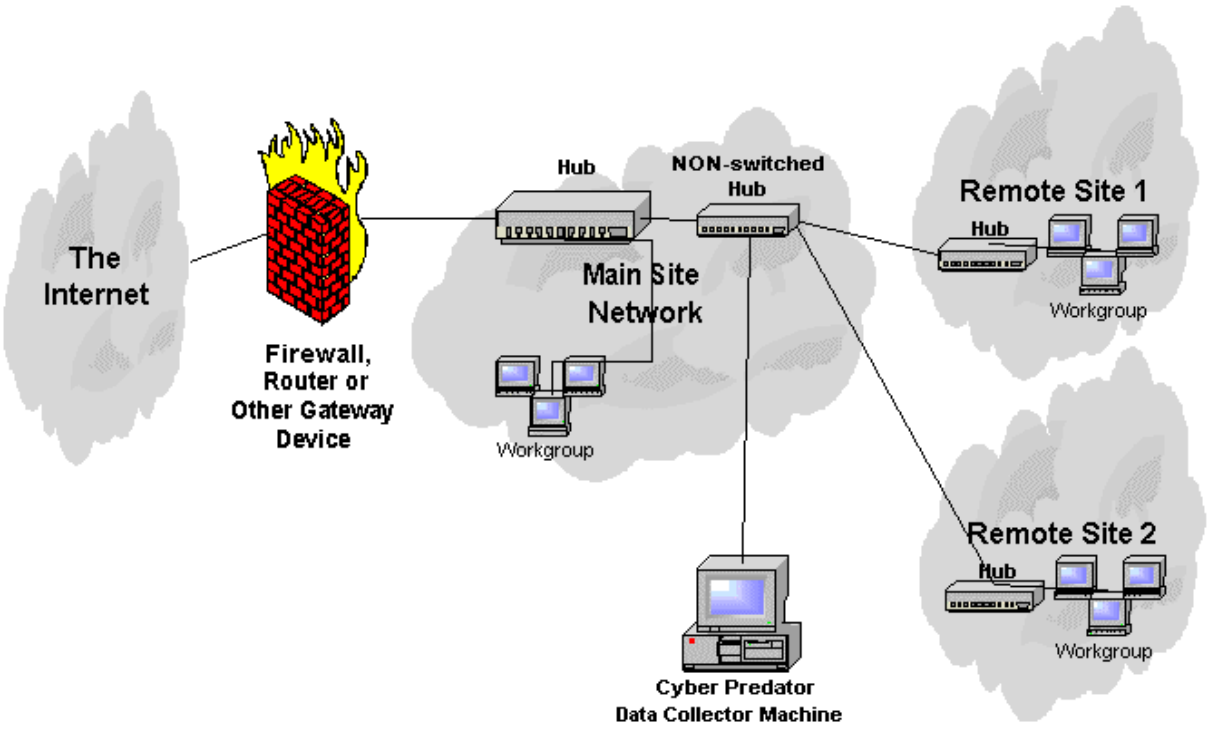
Cyber Predator installed to monitor many sites of a multi-site network (Option 1)



If you only wanted to monitor the remote sites 1 and 2 but not the main site, you would require two Cyber Predator installations, one at each remote site and a NON-switched hub placed between the network and the link to the main site.

All the traffic from the required remote site workstations would be visible to the DC machine via the NON-switched hub.

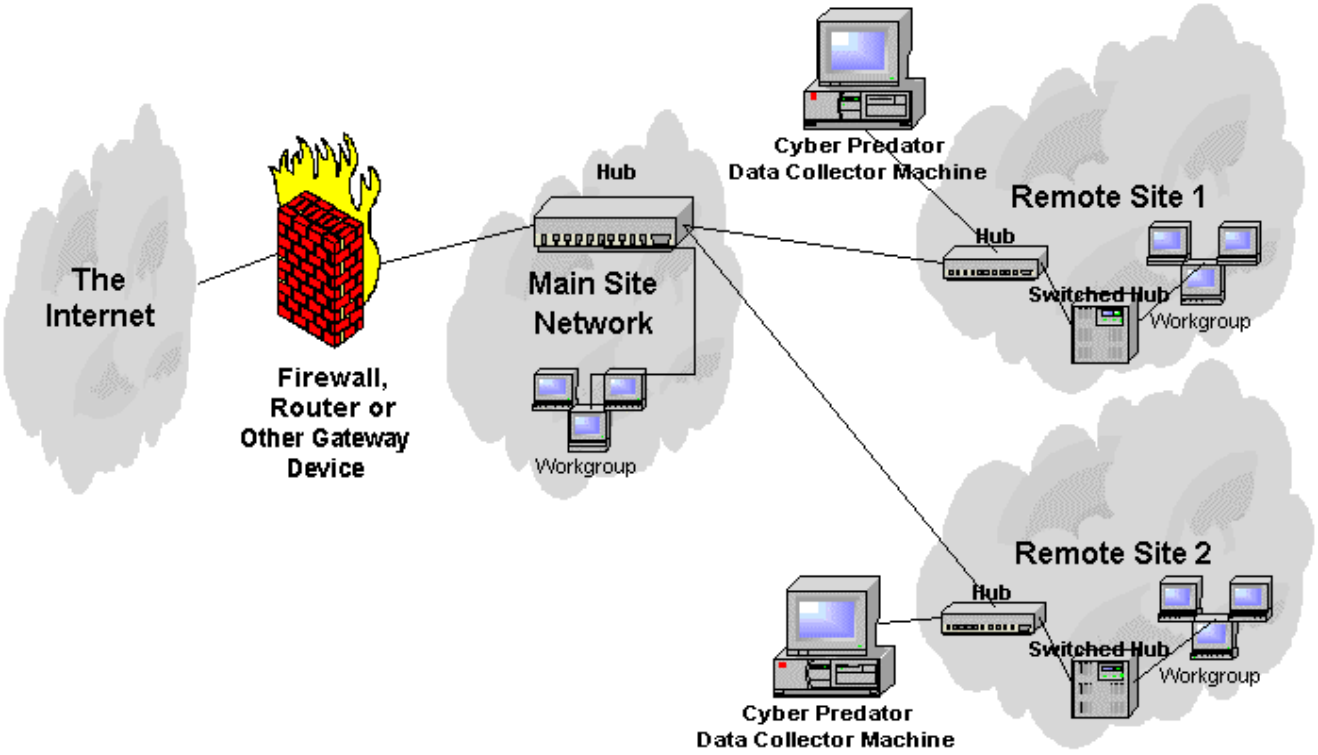
Cyber Predator installed to monitor many sites of a multi-site network (Option 2)



If you only wanted to monitor the remote sites 1 and 2 but not the main site, then this scenario requires one Cyber Predator installation. This would be achieved by placing a NON-switched hub between the main site network and the links to the remote sites and by installing the DC on a machine at the main site.

All the traffic from the required remote site workstations would be visible to the DC machine via the NON-switched hub at the Main Site.

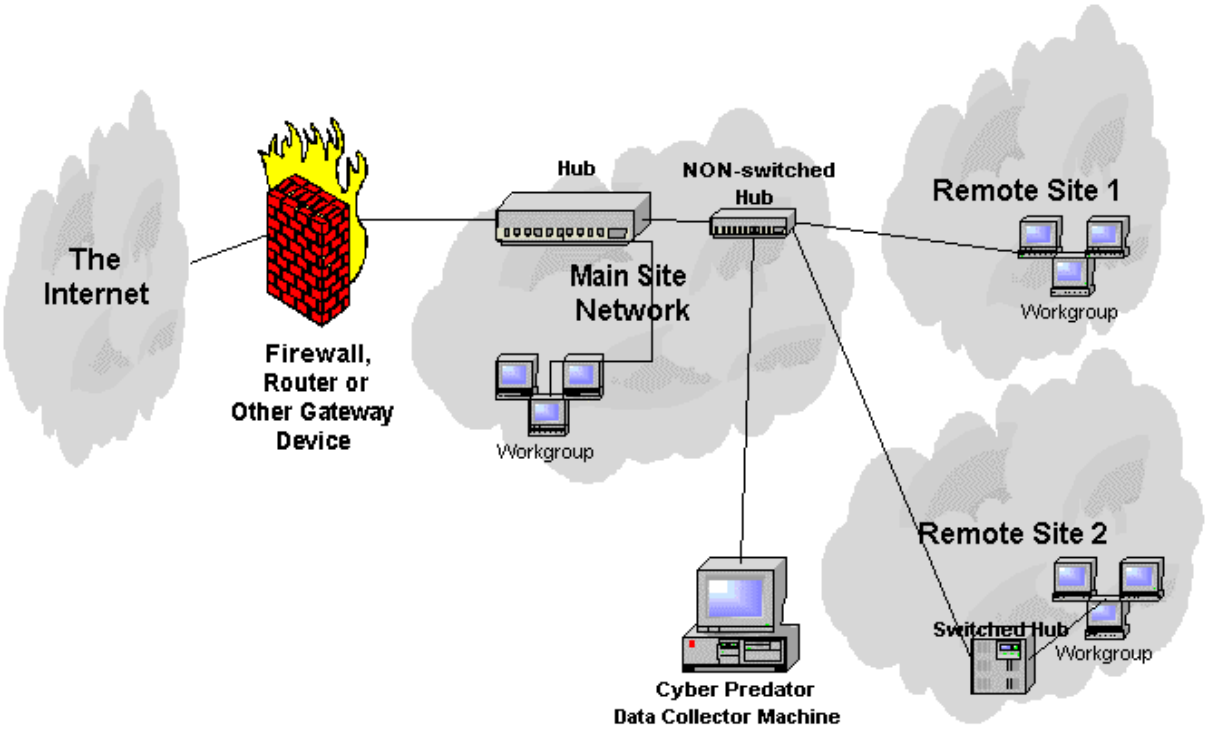
Cyber Predator installed to monitor many sites of a multi-site network that has switched hubs (Option 1)



If you only wanted to monitor the remote sites 1 and 2 but not the main site, you would require two Cyber Predator installations, one at each remote site and a NON-switched hub placed between the switched hub at the remote site and the network link to the main site.

All the traffic from the required remote site workstations would be visible to the DC machine via the NON-switched hub.

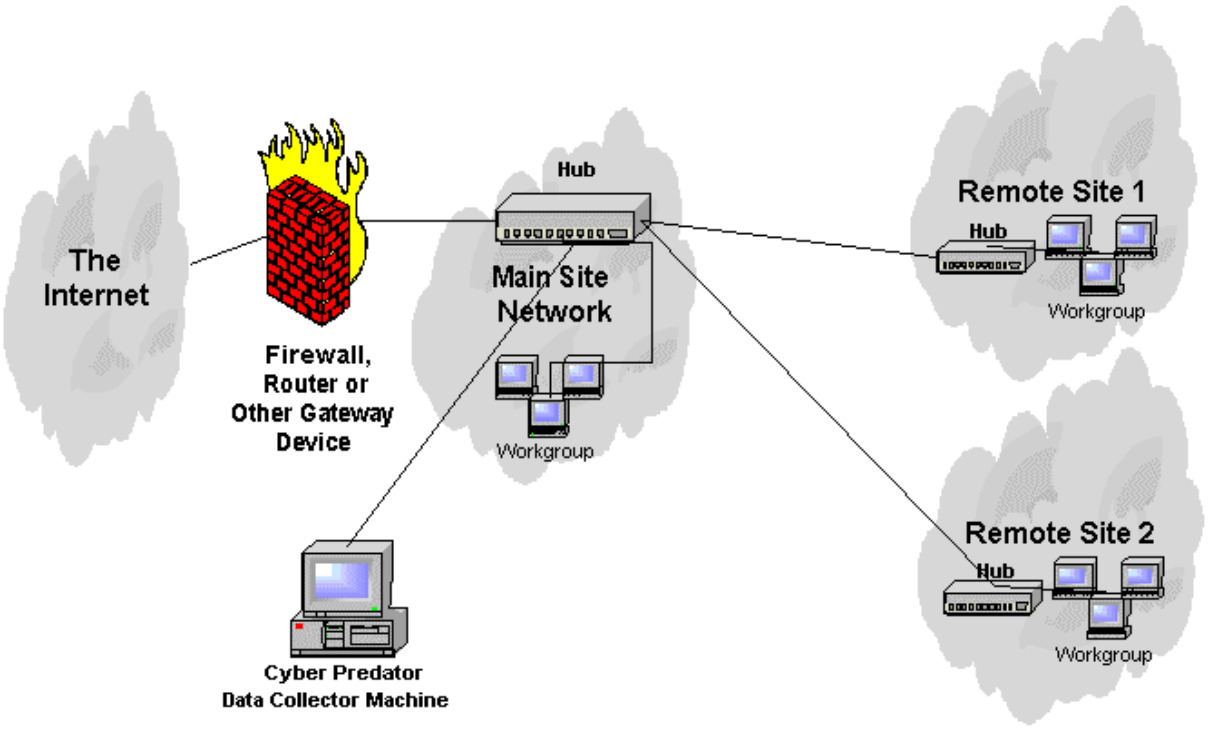
Cyber Predator installed to monitor many sites of a multi-site network that has switched hubs (Option 2)



If you only wanted to monitor the remote sites 1 and 2 but not the main site, this scenario requires one Cyber Predator installation. This is achieved by placing a NON-switched hub between the main site network and the links to the remote sites and by installing the DC on a machine at the main site.

All the traffic from the required remote site workstations would be visible to the DC machine via the NON-switched hub at the Main Site.

Cyber Predator installed to monitor all sites of a multi-site network

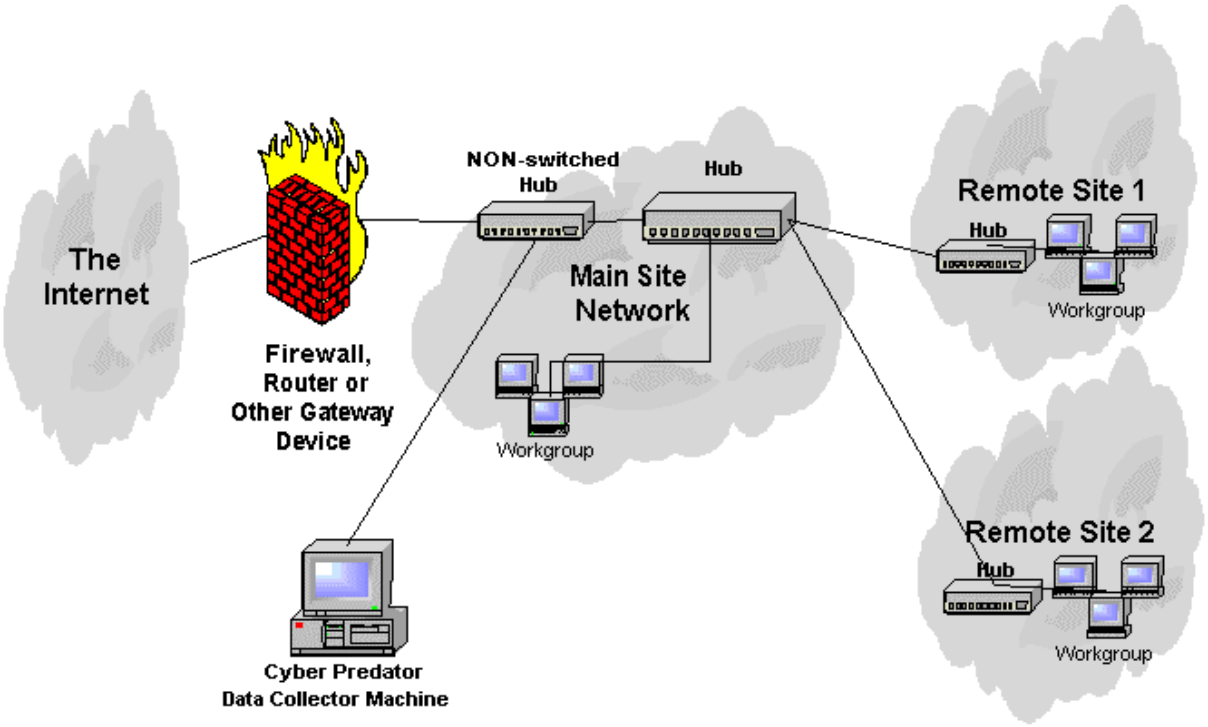


In this situation the Cyber Predator Management Console Software could be installed onto any other machine that has TCP/IP connectivity to the DC machine. Alternatively you could install the MC onto the same machine as the Data Collector and remotely manage the machine via remote control software such as Windows 2000 Terminal Services, Windows XP Remote Desktop, Funk Proxy, PC Anywhere, VNC or other.

Here the Data Collector is connected to a NON-Switched hub at the Main Site.

All the traffic from the main site and the remote sites would be visible to the DC machine via the NON-switched hub.

Cyber Predator installed to monitor all sites of a multi-site network that has switched hubs

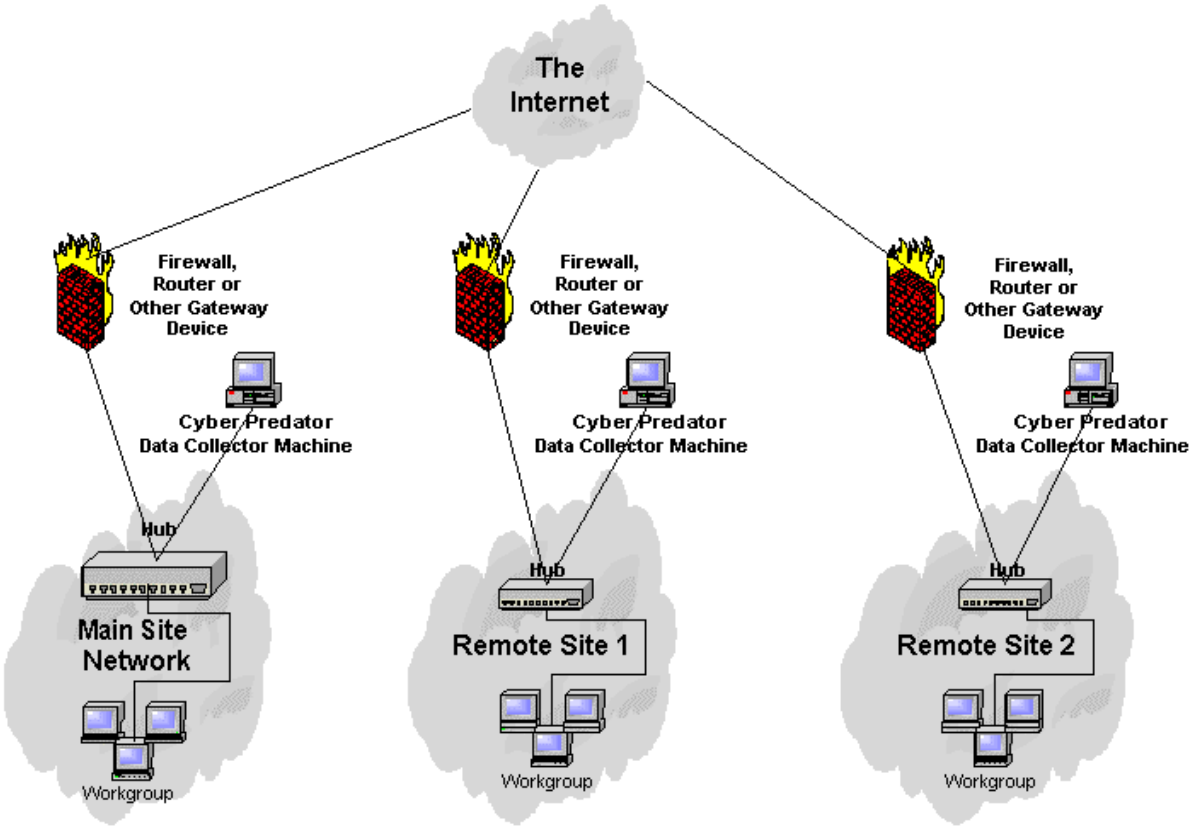


In this situation the Cyber Predator Management Console Software could be installed onto any other machine that has TCP/IP connectivity to the DC machine. Alternatively you could install the MC onto the same machine as the Data Collector and remotely manage the machine via remote control software such as Windows 2000 Terminal Services, Windows XP Remote Desktop, Funk Proxy, PC Anywhere, VNC or other.

Here the Data Collector to a NON-Switched hub at the main site that has been inserted between the main network and its switched hubs and the Internet access point.

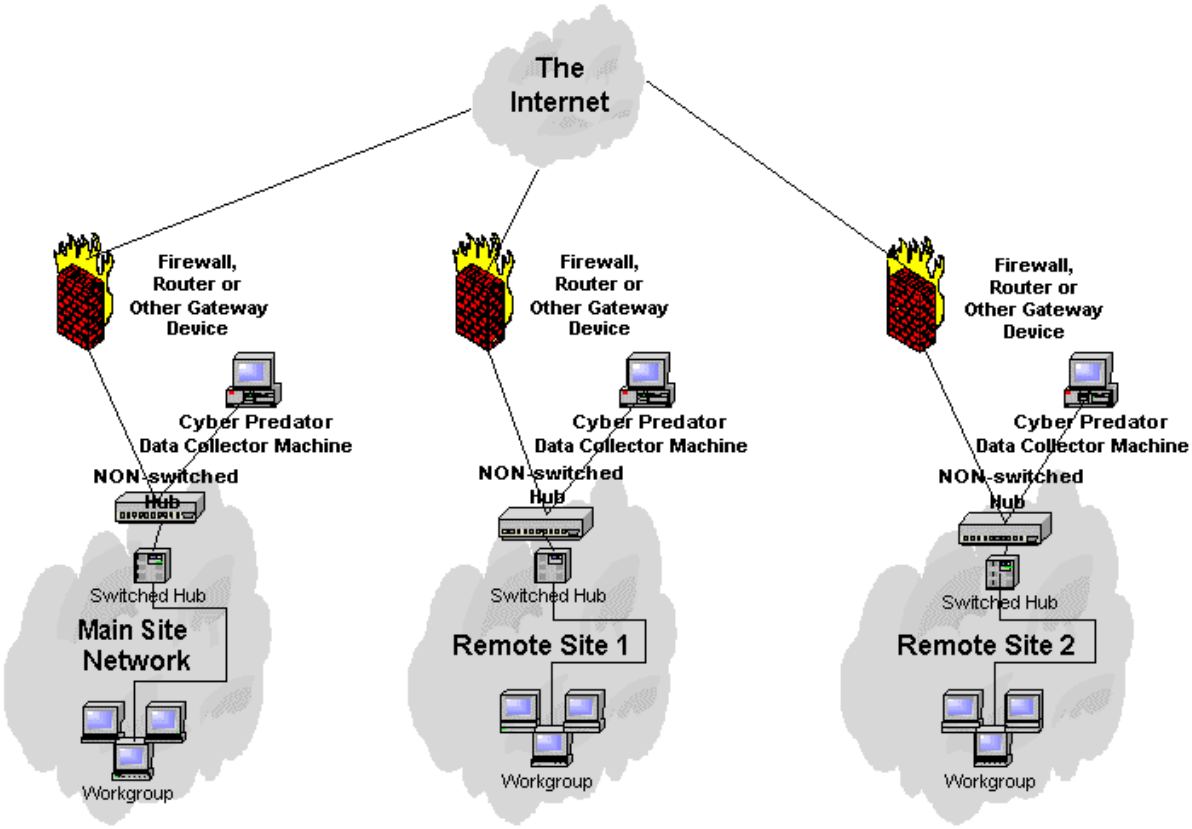
All the traffic from the main site and the remote sites would be visible to the DC machine via the NON-switched hub.

Cyber Predator installed to monitor many sites of a multi-site network that has separate Internet access for each site



As each site has a separate Internet access point, a Cyber Predator installation is required at each site to monitor that sites Internet traffic.

Cyber Predator installed to monitor many sites of a multi-site network that has separate Internet access for each site and switched hubs



As each site has a separate Internet access point, a Cyber Predator installation is required at each site to monitor that sites Internet traffic.

As each site has switched hubs, a NON-switched hub must be placed between the site network and the Internet access point, and the DC machine plugged into this hub.