CYBERX

BATTLE-TESTED INDUSTRIAL CYBERSECURITY

CYBERX PLATFORM

CLI REFERENCE

Version 1

Document version:

1.0

Last revised:

August 29, 2019

Contents

Glossary

Abbreviation	Meaning
AD	Active Directory
DB	Database
CM	Central Manager
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name System
DR	Disaster Recovery
FW	Firewall
Gbps	Billions of bits per second
HA	High Availability
HDD	Hard Disc Drive
HMI	Human Machine Interface
ICS	Industrialized Control System
M2M	Machine to Machine
SOC	Security Operations Center
NTP	Network Time Protocol
OPC	Open Platform Communications
OT	Operational Technology
PCAP	Packet Capture Application Programming
PLC	Programmable Logic Controller
SCADA	Supervisory Control and Data Acquisition
SIEM	Security Information and Event Management
SNMP	Simple Network Management Protocol
SOC	Security Operations Center
SPAN	Switched Port Analyzer
SYSLOG	System Logging Protocol
TCP	Transmission Control Protocol
UI	User Interface
VLAN	Virtual Local Area Network
VM	Virtual Machine
VNET	Virtual Network

1 Overview

The CyberX sensor enables customer business continuity with respect to cyber-attacks and improves everyday operations and uptime by automatically modeling the SCADA network as a state machine. Multiple proprietary and patented analysis engines continually monitor and alert on anomalous network activity.

The Central Manager provides centralized deployment of software, threat intelligence, and configuration updates across all CyberX sensors in the organization.

Both, the Central Manager and the sensors, are managed using the dedicated user-friendly GUI. In addition to the GUI settings, users can configure CyberX with the CLI.

Most of the GUI configuration options can be performed also using the CLI. There are highly technical configuration options that can be performed using the CLI only.

About this guide

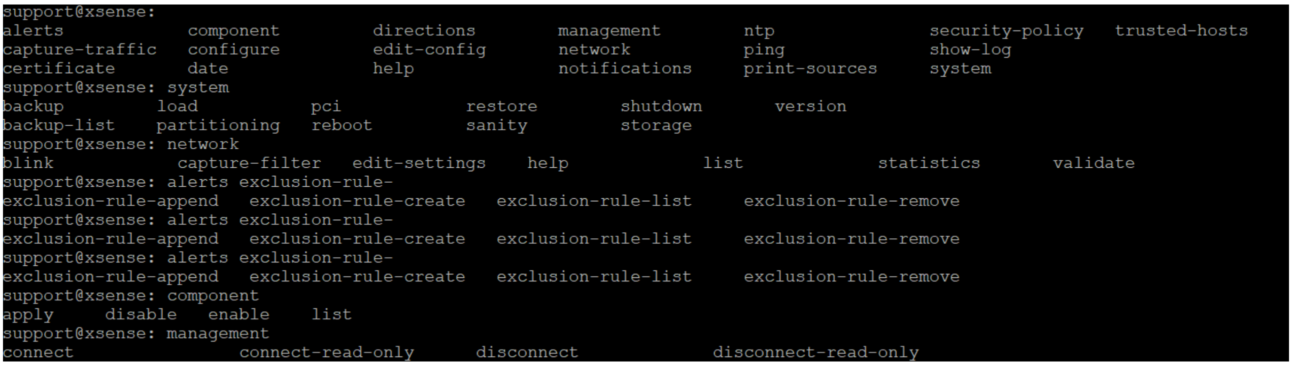
This guide documents the CyberX Command Line Interface (CLI) options, which are used to configure CyberX sensors.

Audience

This guide is written for CyberX Admin users.

Getting Started

To start working in the CLI, connect using a terminal, for example, Putty, and user "support". You can get the credentials for this user from the CyberX Technical Support: support@cyberx-labs.com.



```
support@xsense:
alerts            component         directions        management        ntp               security-policy   trusted-hosts
capture-traffic   configure         edit-config       network           ping              show-log
certificate       date              help              notifications     print-sources     system
support@xsense: system
backup         load           pci            restore        shutdown       version
backup-list    partitioning   reboot         sanity         storage
support@xsense: network
blink            capture-filter   edit-settings    help             list             statistics       validate
support@xsense: alerts exclusion-rule-
exclusion-rule-append   exclusion-rule-create   exclusion-rule-list     exclusion-rule-remove
support@xsense: alerts exclusion-rule-
exclusion-rule-append   exclusion-rule-create   exclusion-rule-list     exclusion-rule-remove
support@xsense: alerts exclusion-rule-
exclusion-rule-append   exclusion-rule-create   exclusion-rule-list     exclusion-rule-remove
support@xsense: component
apply     disable   enable    list
support@xsense: management
connect                connect-read-only      disconnect             disconnect-read-only
```

2 Alert exclusion rules

Alerts can be suppressed for specific situations where you do not need or want alerts to be generated. Exclusion rules are useful when planning maintenance activities or for network events for which you do not want to receive alerts.

Create local alert exclusion rules

```
alerts exclusion-rule-create [-h] -n NAME [-ts TIMES] [-dir DIRECTION]
 [-dev DEVICES] [-a ALERTS]
```

The following attributes can be used with the alert exclusion rules:

Attribute	Description
[-h]	Prints help information for the command
-n NAME	The name of the rule being created

[-ts TIMES]	The timespan for which the rule is active, specified as:
	`xx:yy-xx:yy`
	If you need to define more that one time period, use a comma between them, as follows:
	`xx:yy-xx:yy, xx:yy-xx:yy`

[-dir DIRECTION]	The address direction in which the rule is applied, specified as: `both | src | dst`

[-dev DEVICES]	The IP address and the address type of the assets to be excluded by the rule, specified as:
	`ip-x.x.x.x`
	`mac-xx:xx:xx:xx:xx:xx`
	`subnet: x.x.x.x/x`

[-a ALERTS]	The name of the alert to be excluded by the rule:
	`0x00000`
	`0x000001`

Append local alert exclusion rules

```
alerts exclusion-rule-append [-h] -n NAME [-ts TIMES] [-dir DIRECTION]
 [-dev DEVICES] [-a ALERTS]
```

The attributes used here are the same as the attributes explained in the Create local alert exclusion rules section. The difference in the usage is that here the attributes are applied to the existing rules.

Show local alert exclusion rules

```
alerts exclusion-rule-list [-h] -n NAME [-ts TIMES] [-dir DIRECTION]
 [-dev DEVICES] [-a ALERTS]
```

This command presents the list of existing exclusion rules.

Delete local alert exclusion rules

```
alerts exclusion-rule-remove [-h] -n NAME [-ts TIMES] [-dir DIRECTION]
 [-dev DEVICES] [-a ALERTS]
```

The following attribute can be used with the alert exclusion rules:

Attribute	Description
-n NAME	The name of the rule to be deleted

3 Sync time from NTP server

Enable NTP

Periodically retrieves time from the specified NTP server:

```
ntp enable IP
```

Specify the IP address of the NTP server.

Disable NTP sync

Disables time sync with the specified NTP server:

```
ntp disable IP
```

Specify the IP address of the NTP server.

4 Network configuration

Ping

Ping addresses outside the CyberX platform:

```
ping IP
```

Blink

Locates the required connection by causing the interface lights to blink.

```
network blink
```

Reconfigure the network

Enables changing the network configuration parameters:

```
network edit-settings
```

Show network settings

Displays the network adapter parameters (similar to Linux iconfig command):

```
network list
```

Validate the network configuration

Presents the output network settings:

```
network validate

example:

Current Network Settings:
interface: eth0
ip: 10.100.100.1
subnet: 255.255.255.0
default gateway: 10.100.100.254
dns: 10.100.100.254
monitor interfaces: eth1
```

Filter network configurations

The network capture-filter command allows administrators to eliminate the network traffic 'noise' that the appliance is receiving but does not need to analyze. This capability enables filtering using an Include list and / or an Exclude list:

```
network capture-filter
```

Would you like to supply devices and subnet masks you wish to ***include*** *in the capture filter? [y/N]:*

`yes` brings up a nano file where you can add assets, channels, ports and subsets according to the following syntax:

Divide arguments by dropping a row.

When you include an asset, channel or subnet, it means the sensor processes all the traffic valid for that argument, even if it includes ports and traffic it doesn't usually process.

Attribute	**Description**
1.1.1.1	Includes all the traffic for this asset
1.1.1.1,2.2.2.2	Includes all the traffic for this channel
1.1.1,2.2.2	Includes all the traffic for this subnet

Would you like to supply devices and subnet masks you wish to ***exclude*** *from the capture filter? [y/N]:*

`yes` brings up a nano file where you can add assets, channels, ports and subsets according to the following syntax:

Divide arguments by dropping a row.

When you exclude an asset, channel or subnet, it means the sensor excludes all the traffic valid for that argument.

Attribute	**Description**
1.1.1.1	Excludes all the traffic for this asset
1.1.1.1,2.2.2.2	Excludes all the traffic for this channel, meaning all the traffic between two assets
1.1.1.1,2.2.2.2,443	Excludes all the traffic for this channel by port
1.1.1	Excludes all the traffic for this subnet
1.1.1,2.2.2	Excludes all the traffic for between subnets

ports:

Include or exclude UDP/TCP ports is executed for all the traffic.

502 single port

502,443 both ports

Enter tcp ports to include (delimited by comma or Enter to skip):

Enter udp ports to include (delimited by comma or Enter to skip):

Enter tcp ports to exclude (delimited by comma or Enter to skip):

Enter udp ports to exclude (delimited by comma or Enter to skip):

components:

In which component do you wish to apply this capture filter?

Your options are: `all`, `dissector`, `collector`, `statistics-collector`, `rpc-parser`, `smb-parser`

In most use-cases, select `all`.

custom base capture filter:

The base capture filter is the baseline for the components. For example, what ports the component sees.

As a general thumb rule, do not change this. All the filters so far are added to the baseline after the changes are set. If you change, it will not be added, but instead it will overwrite the existing baseline.

Would you like to supply a custom base capture filter for the dissector component? [y/N]:

Would you like to supply a custom base capture filter for the collector component? [y/N]:

Would you like to supply a custom base capture filter for the statistics-collector component? [y/N]:

Would you like to supply a custom base capture filter for the rpc-parser component? [y/N]:

Would you like to supply a custom base capture filter for the smb-parser component? [y/N]:

type Y for "internal" otherwise N for "all-connected" (custom operation mode enabled) [Y/n]:

let's say I excluded subnet 1.1.1.

internal will exclude just that subnet

all connected will exclude that subnet and all the traffic to and from that subnet.

a general rule of thumbs says to choose *internal*

NOTE: all connected and *internal* are for all the filters in the tool, and are not session dependent, meaning you can't ever choose to do *internal* for some filters and *all connected* for others.

Comments:

filters can be viewed in `/var/cyberx/properties/cybershark.properties`

statistics-collector - bpf_filter property in `/var/cyberx/properties/net.stats.collector.properties`

dissector - override.capture_filter property in `/var/cyberx/properties/cybershark.properties`

rpc-parser - override.capture_filter property in `/var/cyberx/properties/rpc-parser.properties`

smb-parser - override.capture_filter property in `/var/cyberx/properties/smb-parser.properties`

collector - general.bpf_filter property in `/var/cyberx/properties/collector.properties`

This is how you can restore the default configuration:

user: **cyberx**

sudo cyberx-xsense-capture-filter -p all -m all-connected

5 Importing self-signed certificate

Import a certificate

Imports the HTTPS certificate:

```
certificate import FILE
```

You need to specify the full path to a *.crt file.

6 Defining client and server hosts

If CyberX did not automatically detect client and server hosts, use this command to specifically set client and server hosts.

```
directions [-h] [--identifier IDENTIFIER] [--port PORT] [--remove] [--add]
 [--tcp] [--udp]
```

The following attributes can be used with the `directions` command:

Attribute	Description
[-h]	Prints help information for the command
[--identifier IDENTIFIER]	The server identifier
[--port PORT]	The server port
[--remove]	Removes a client or server host from the list
[--add]	Adds a client or server host to the list
[--tcp]	Use TCP protocol when communicating with this host
[--udp]	Use UDP protocol when communicating with this host

7 Show the date

Returns the current date on the host in GMT format:

```
date
```

8 System actions

Reboot the host

```
system reboot
```

Shut the host down

```
system shutdown
```

Back up the system

Initiates an immediate backup (a non-scheduled backup):

```
system backup
```

Restore the system from a backup

Restores from the most recent backup:

```
system restore
```

List the backup files

Lists the available backup files:

```
system backup-list
```

Display the status of all CyberX platform services

Checks the sanity of the system, by listing the current status of all CyberX platform services:

```
system sanity
```

Show the software version

Displays the version of the software currently running on the system:

```
system version
```