iSG18GFP User Manual, Enhanced Security, Section E

iSG18GFP

Intelligent 18 Port Compact Service Aware Ethernet Switch
IEC 61850-3 and IEEE 1613 Compliant

Version 4.5.06.3, Mar 2023

SERVICES • SUPPORT • SECURITY • SOLUTIONS • SYSTEMS

COPYRIGHT NOTICE

TRADEMARKS

iS5Com is a registered trademark of iS5. All other trademarks belong to their respective owners.

REGULATORY COMPLIANCE STATEMENT

Product(s) associated with this publication complies/comply with all applicable regulations. For more details, refer to the Technical Specifications.

WARRANTY

iS5 warrants that all products are free from defects in material and workmanship for a specified warranty period from the invoice date (5 years for most products). iS5 will repair or replace products found to be defective within this warranty period including shipping costs. This warranty does not cover product modifications or repairs done by persons other than iS5-approved personnel, and this warranty does not apply to products that are misused, abused, improperly installed, or damaged by accident.

Refer to the Technical Specifications for the actual warranty period(s) of the product(s) associated with this publication.

DISCLAIMER

Information in this publication is intended to be accurate. iS5 shall not be responsible for its use or infringements on third-parties because of the use of this publication. There may occasionally be unintentional errors on this publication. iS5 reserves the right to revise the contents of this publication without notice.

CONTACT INFORMATION

iS5 Communications Inc
5895 Ambler Dr., Mississauga, Ontario, L4W 5B7
Tel: 1+ 905-670-0004
Website: http://www.is5com.com/

Technical Support
E-mail: support@is5com.com

Sales Contact
E-mail: info@is5com.com

Table of Contents

Table of Tables

Table of Figures

About the Document

1.1 iSG18GFP Overview

The iSG18GFP is an intelligent 18 port compact Service-Aware Ethernet switch, IEC 61850-3 and IEEE 1613 compliant, which is designed with a unique strong packet processing application-aware engine to fit the most critical industrial application.

The optional support of an integrated firewall on every port of the iSG18GFP provides a network-based distributed security. The switch also contains a VPN gateway with 2 operational modes: inter-site connectivity using IPSec tunnels and remote user access via SSH.

The iSG18GFP is a natural fit for installation at MV/LV transformer sites acting as secure access points for the Distributed Automation control of remote sites. This product is as a secure gateway for Ethernet, IP, and Serial services as an optimized platform for servicing these needs over the network core. The iSG18GFP provides maximum protection against cyber threats.

The iSG18GFP can be managed by the iDevice Management System (iDMS). The product is made of galvanized steel and has a wide operating temperature from -40°C to +85°C suitable for the harshest of environments without fans.

1.2 Using this Document

1.2.1 Documentation Purpose

This user guide describes the features available in the enhanced security (SE) product configuration of the iSG18GFP Ethernet switch only. These features are:

- Authentication Proxy Access
- Event Logger
- IPSec (X.509)
- Application Aware Firewall

☞ Please be advised if the SE is not part of your order, these features will be not available.

This document contains Section E of the iSG18GFP user manual. It includes chapters about Enhanced Security Licensing, Authentication Proxy Access (configuration & commands hierarchy and description), Event Logger, IPSec, Application Aware Firewall (configuration & commands hierarchy and description), etc.

This part of the document describes the SE features of the product.

- For basic networking features, refer to Section B, iSG18GFP User Manual, Basic, Section B, UM-B-iSG18GFP-4.5.06.01-EN.docx
- For general structure and features of the product, refer to iSG18GFP User Manual, General, Section G, UM-G-iSG18GFP-4.5.06.01-EN.docx
- For security features, refer to iSG18GFP User Manual, Security, Section S, UM-S-iSG18GFP-4.5.06.01-EN.docx

1.2.2 Intended Audience

This user guide is intended for network administrators responsible for installing and configuring network equipment. Users must be familiar with the concepts and terminology of Ethernet and local area networking (LAN) to use this user guide.

1.2.3 Documentation Suite

This document is one part of the full documentation suite provided with this product.

Table 1 – Documentation Suite Details

You are:	Document Function	Function
	Installation Guide	Contains information about installing the hardware and software; including site preparation, testing, and safety information.
➡	➡ User Guide	Contains information on configuring and using the system.
	Release Notes	Contains information about the current release, including new features, resolved issues (bug fixes), known issues, and late-breaking information that supersedes information in other documentation

1.2.4 Conventions Used

Conventions	Usage	Example
< >	Parameter inside < > indicate the Input fields of syntax	<integer (100-1000)>
[ ]	Parameter inside [ ] indicate Optional fields of syntax	[<output file>]
{ }	Grouping parameters in the syntax	{console}
|	Separating grouped parameters in the syntax	{console | vty | <line-number(0-16)>}
Calibri (Body) 10	Example	**`Your Product# enable 15`**

`Courier New 10 regular blue`
`Courier New 10 regular black`
	CLI command outputs	**`Current privilege level is 15`**
		`Your Product# show privilege`

☞	Pre-requisites or special information to which the user needs to pay special attention	☞ Alias name can be set only for the commands having equal to or less than 10 tokens.
✎	Notes	✎ `BFD support is enabled in an interface by default.`

1.3 List of Abbreviations

Table 2 – Acronyms Used in this Document

Acronym	Explanation
ACE	Application Configuration Environment
ACL	Access List
AH	Authentication Header
AES	Advanced Encryption Standard
ARP	Address Resolution Protocol
ASDU	Application Service Data Unit
CE	Customer Equipment
CLI	Command Line Interface
DNP3	Distributed Network Protocol
DPI	Deep Packet Inspection
FQDN	Fully Qualified Domain Name

Acronym	Explanation
GCE	Global Configuration Environment
GRE	Generic Routing Encapsulation
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
IGRP	Internet Group Management Protocol
IKE	Internet Key Exchange
IPS	Intrusion Prevention System
IPsec	Internet Protocol Security
ISAKMP	Internet Security Association and Key Management Protocol
LAN	Local Area Network
MAC	Media Access Control
NAT	Network Address Translation
TCP	Transport Control Protocol or Triple Data Encryption Algorithm
3DES	Triple Data Encryption Algorithm
OSPF	Open Shortest Path First
pcap	packet capture
PFS	Perfect Forward Secrecy
PPP	Point-to-Point Protocol
PSK	Pre-Shared Keys
RIP	Routing Information Protocol
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition (SCADA)
SE	Security Enhanced
SSH	Secure Shell
USB	Universal Serial Bus
VLAN	Virtual LAN
VPN	Virtual Private Network
VRRP	Virtual Router Redundancy Protocol

1.4 Terminology

- RTU is the name in general for all field devices for which authentication service is intended.
- APA or 'Authentication Proxy Access' is used to authenticate users.
- Client/user—any user intended to be conditioned by the APA when accessing the RTUs. The user (SSH client) opens an SSH authentication session to the APA (SSH server).
- Protocols—a list of TCP/UDP port numbers (protocols) defined as the 'interesting traffic'.
- Interesting traffic—a configurable list of protocols with which profiles are defined and for which logs are tracked.
- Profile—a set of conditions limiting a client to access specific RTUs using specific protocols and at a given time frame only.
- APA ports—physical ports of the iSG18GFP via which clients are expected to access and for which APA is enabled.

1.5 References

[1] Network Working Group, RFC 2408, Internet Security Association and Key Management Protocol (ISAKMP) https://tools.ietf.org/html/rfc2408 Online Accessed on June 14, 2018

[2] Network Working Group, RFC 2409, https://tools.ietf.org/html/rfc2409#section-5

[3] iSG18GFP User Manual, Security, Section S, UM-S-iSG18GFP-4.4-1-EN.docx

[4] RapidTables, https:/ /www.rapidtables.com/code/text/ascii-table.html Online, Accessed On June 13, 2018

[5] Wiki: OpenVPN GUI (for Windows), https://community.openvpn.net/openvpn/wiki/OpenVPN-GUI Online Accessed on July 4, 2018

[6] ovpn.com, Pros and cons of different VPN protocols, by Maximilian Holm, 10 Mar 2017 about Online Privacy https://www.ovpn.com/en/blog/pros-and-cons-of-different-vpn-protocols/, Online Accessed on July 4, 2018

Enhanced Security (SE) Licensing

The features pertaining to the security enhanced (SE) model of the iSG18GFP secure gateway are only available with the applicable license. Contact iS5Com’s technical support to obtain such license.

☞ Be advised that if SE is not part of your order, the features Authentication Proxy Access, Event Logger, IPSec (X.509), and Application Aware Firewall will be not available.

You may be required to provide the MAC address of your iSG18GFP secure gateway. It can be obtained in one of the following ways: by Command Line Interface (CLI) or iDMS.

2.1 Obtaining MAC Address

2.1.1 CLI

1. Type show system information from Global Configuration Environment (GCE) and refer to the displayed MAC address field (marked in **bold** below).

```
iSG18GFP# show system information
Hardware Version                    :
Firmware Version           : 4.4.00.14 U-Boot 2010.12 (Dec 11 2012 - –0:34:29)
Hardware Part Number                : iSG18GFP-HV-HV-D-8RJ45-2GSFP-XX-XX-SE iSG18GFP
System Name                         : iSG18GFP
System Contact             :
System Location            :
Logging Option             : Console Logging
Login Authentication Mode           : Local
Config Save Status                  : Not Initiated
Remote Save Status                  : Not Initiated
Config Restore Status               : Successful
Software Watchdog                   : Enable
Traffic Separation Control : none
Board Serial Number                 :
Manufacture Serial Number           :
Assembly Number                     :
Hardware Revision                   :
HW sub-type                         : 2232
CLEI                       : FFFFFFFFFFFFFFF
MAC address                         : E8:E8:75:10:2D:D8
License value                       : 000000000000
Device Type ID             : <null>
Part Number 2              : iSG18GFP-HV-HV-D-8RJ45-2GSFP-XX-XX-SE iSG18GFP
```

2.1.2 iDMS

1. Go to the iDMS main screen and click **System** tab. Click **CLI Memo** or **F11** to ensure that **CLI Memo** is enabled (a check mark next to it on the figure below).

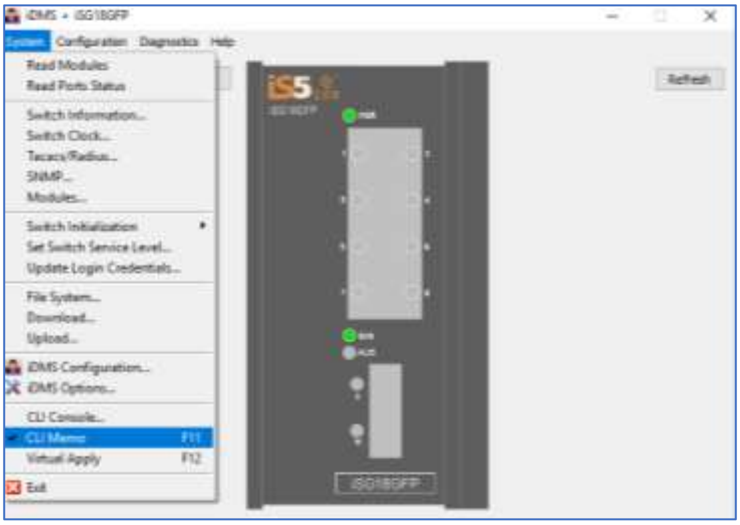
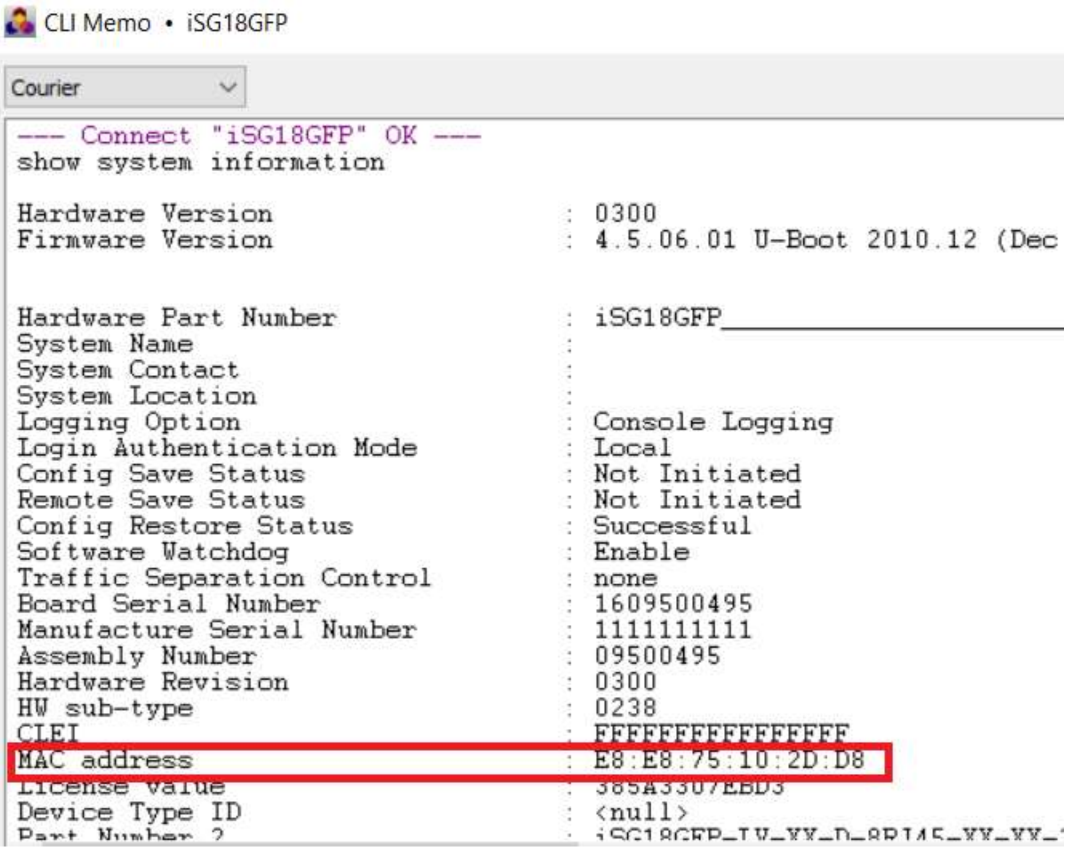


Figure 1 – iDMS System Tab with CLI Memo Enabled Shown

2. Click **Refresh** (it's in the top corner on right). The MAC address will be displayed as part of the overall information as shown below:



```
--- Connect "iSG18GFP" OK ---
show system information

Hardware Version                    : 0300
Firmware Version                    : 4.5.06.01 U-Boot 2010.12 (Dec


Hardware Part Number                : iSG18GFP
System Name                         :
System Contact                      :
System Location                     :
Logging Option                      : Console Logging
Login Authentication Mode           : Local
Config Save Status                  : Not Initiated
Remote Save Status                  : Not Initiated
Config Restore Status               : Successful
Software Watchdog                   : Enable
Traffic Separation Control          : none
Board Serial Number                 : 1609500495
Manufacture Serial Number           : 1111111111
Assembly Number                     : 09500495
Hardware Revision                   : 0300
HW sub-type                         : 0238
CLEI                                : FFFFFFFFFFFFFFFF
MAC address                         : E8:E8:75:10:2D:D8
License Value                       : 385A3307EBD3
Device Type ID                      : <null>
Part Number 2                       : iSG18GFP-LV-XX-D-8RJ45-XX-XX-
```

Figure 2: CLI Memo

2.2 Checking SE License Status

2.2.1 CLI

1. Type application connect command from Global Configuration Environment (GCE) to switch to Application Configuration Environment (ACE), and then use the license show command as follows.

```
iSG18GFP# application connect

[/]license show
```

The following output shall provide information on the current status of the SE license:

```
Installed license KEY        :  000000000000
License Type                 :  General
Valid             :  No
Restart Required :  No
Completed OK
```

2.2.2 iDMS

1. Go to iDMS main screen, click the **System** tab and select **Set Switch Service Level…**

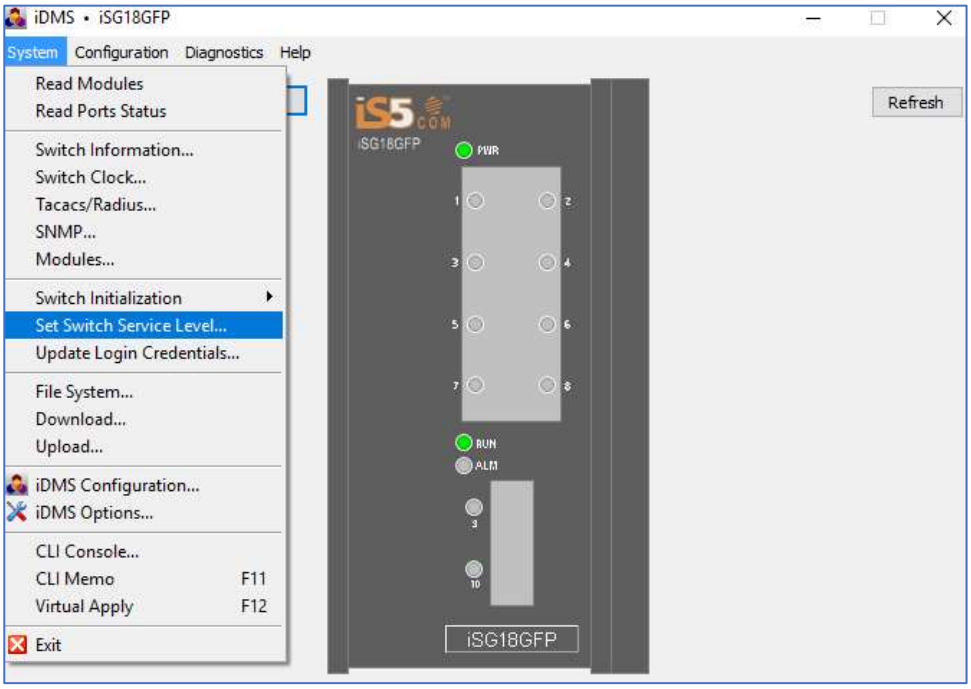
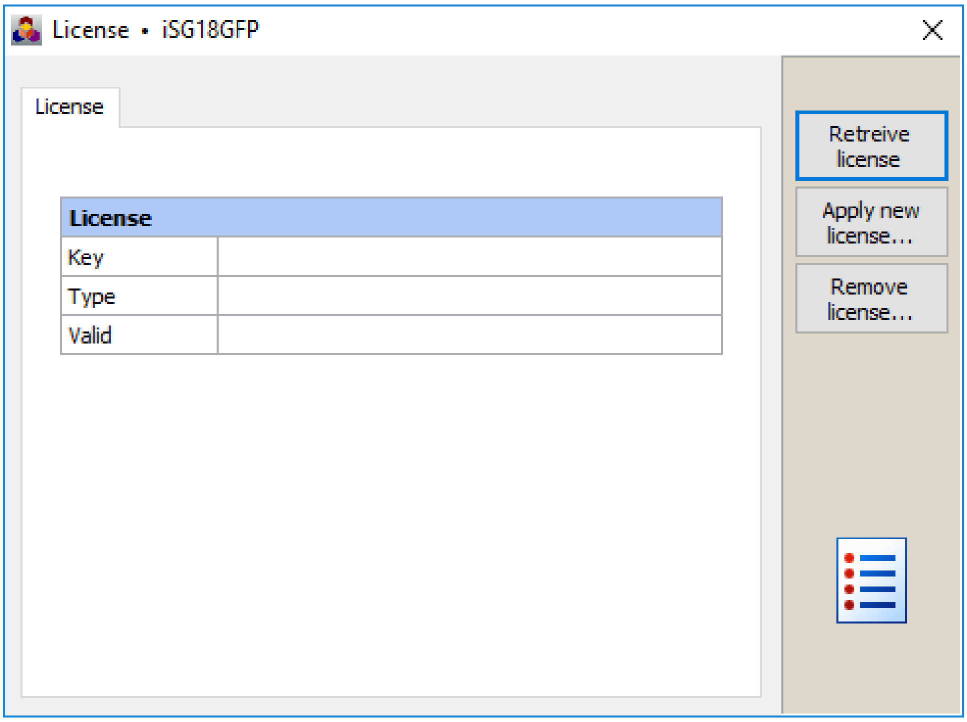


Figure 3 – iDMS Main Screen

2. A license screen appears. Click **Retrieve license** to retrieve the license key information, license key type, and its validity from the secure gateway. License retrieve data will appear under **License** tab.



License	
Key	
Type	
Valid	

Figure 4 – iDMS Retrieve license…

2.3 Installing SE License

The license number is provided by IS5Com in a format of 12 hexadecimal characters (0-9, A-F), such as 0123456789AB.

2.3.1 CLI

1. Run application connect command from GCE to switch to ACE and use the license install key command as following:

```
iSG18GFP# application connect

[/]license install key 0123456789AB
```

```
Installing Enhanced license...

Completed OK
```

Now restart the unit using the CLI reload command.

2.3.2 iDMS

1. Go to iDMS main screen, click the **System** tab and select **Set Switch Service Level…**

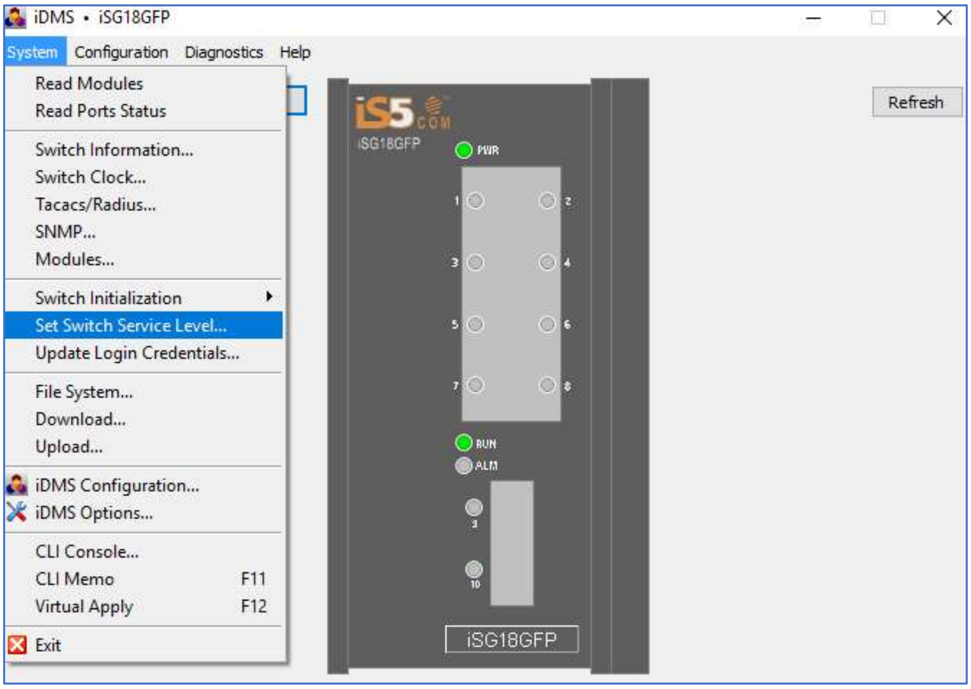
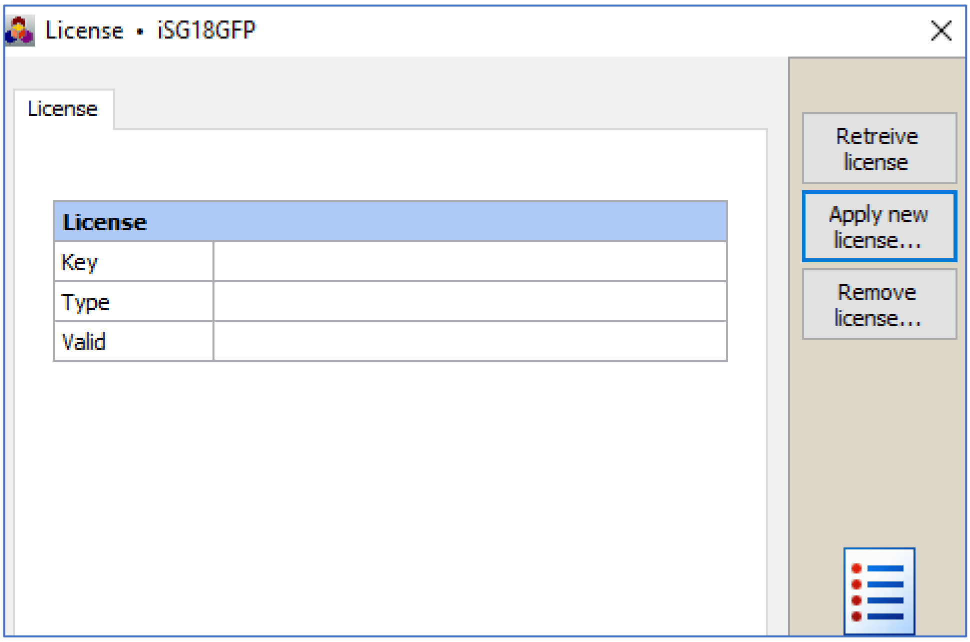


Figure 5 – iDMS Main Screen

2. A license screen appears. To have a new license installed, click **Apply new license…**



License	
Key	
Type	
Valid	

Figure 6 – iDMS License with Highlighted Apply new License…

3. To install a new license, click **Apply new license…** The **Apply new license** screen appears.

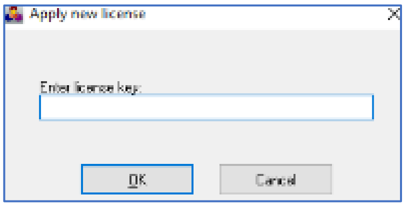
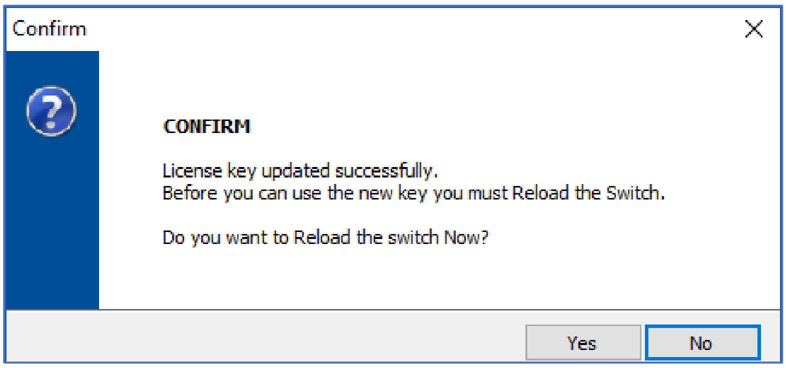


Figure 7 – iDMS Apply new License…

4. Type the license key and click **OK**. The following message appear:



CONFIRM

License key updated successfully.
Before you can use the new key you must Reload the Switch.

Do you want to Reload the switch Now?

Figure 8 – iDMS License Confirm Screen

5. To install the license, the iDMS must reload the secure gateway. Click **Yes** to reload the secure gateway.

2.4 Removing SE License

2.4.1 CLI

1. Run application connect command from GCE to switch to ACE and use the license remove command as following:

```
iSG18GFP# application connect

[/]license remove
```

```
Completed OK
```

2.4.2 iDMS

1. Go to iDMS main screen, click the **System** tab and select **Set Switch Service Level…**

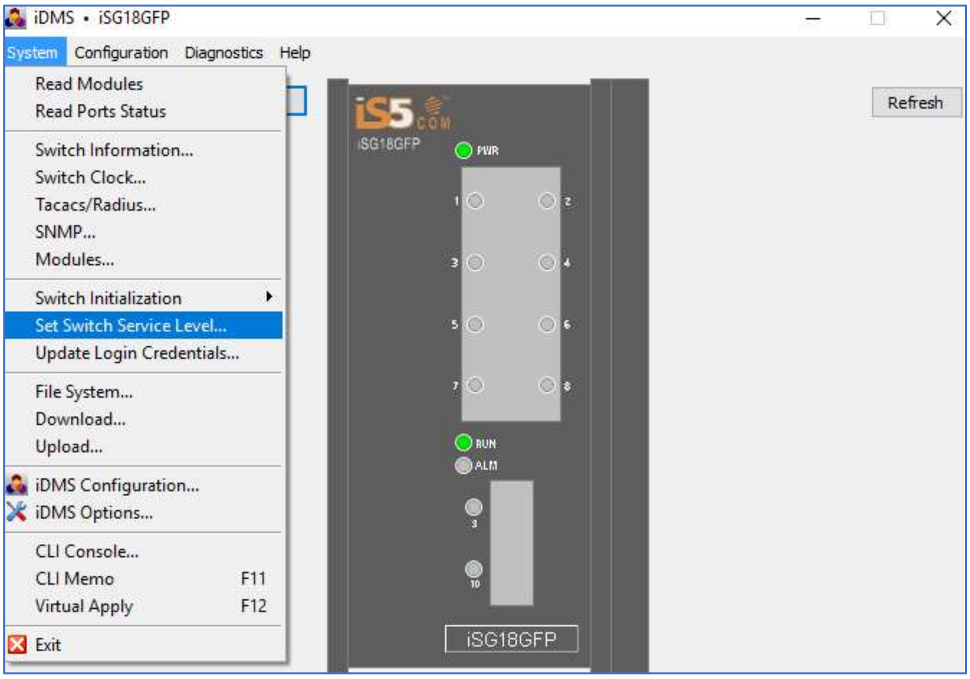
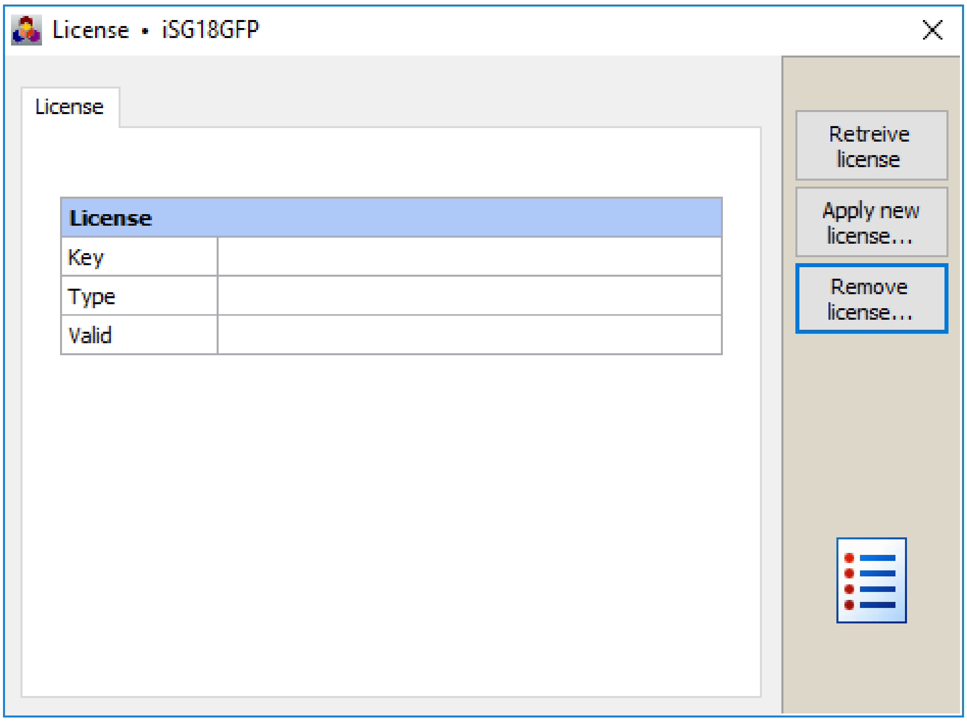


Figure 9 – iDMS Main Screen

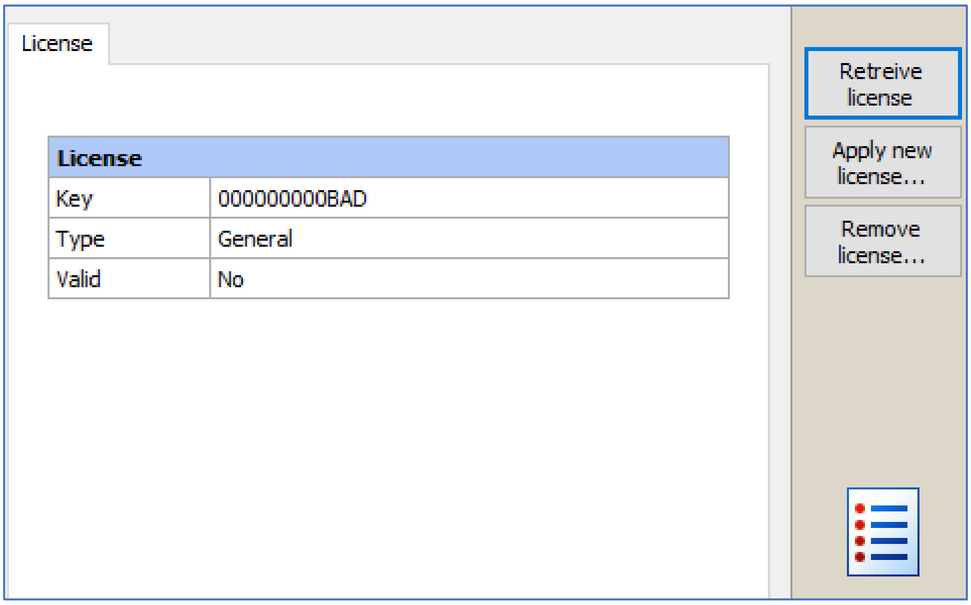
2. A license screen appears. To have a new license removed, click **Remove license…**



License	
Key	
Type	
Valid	

Figure 10 – iDMS License with Highlighted Remove license…

3. Click **Retrieve license** to verify that the installed license was removed. License retrieve data will appear under License tab.



License	
Key	000000000BAD
Type	General
Valid	No

Figure 11 – iDMS License Removal Verification

Authentication Proxy Access (APA)

The Authentication Proxy Access (APA) is a security feature allowing authentication for users to end point devices. These users are normally blocked by an access list.

3.1 Service Description

A typical use case is as follows:

A client is using own software tools and protocols to manage/control/monitor a remote terminal unit (RTU). The figure below exemplifies a user using Modbus tools to control a Modbus RTU device. The RTU may not have its own security capabilities for authentication and validation of a client.

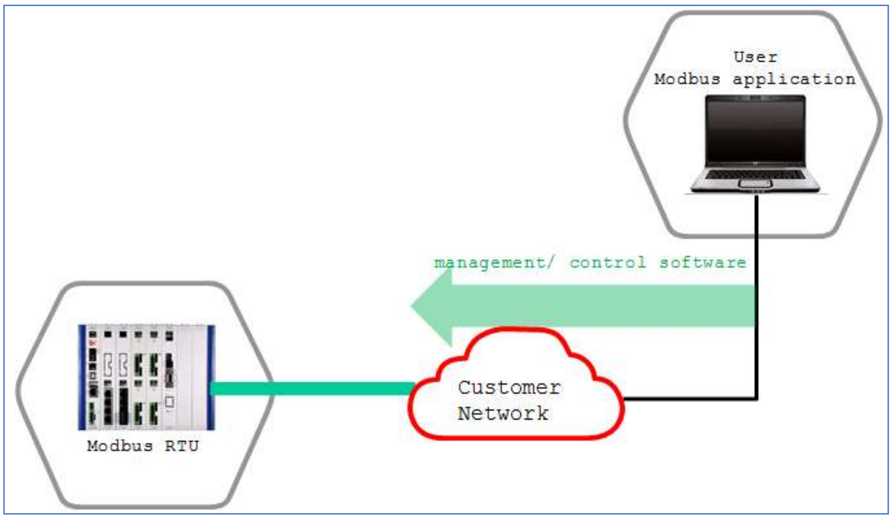


Figure 12 – User to RTU networking

By using the APA feature, the user will open an SSH connection to authenticate itself and be assigned with a specific predefined set of conditions prior to gaining access to the RTU. The next figure shows how the user has no access to the RTU at the default state if the APA is inactive.

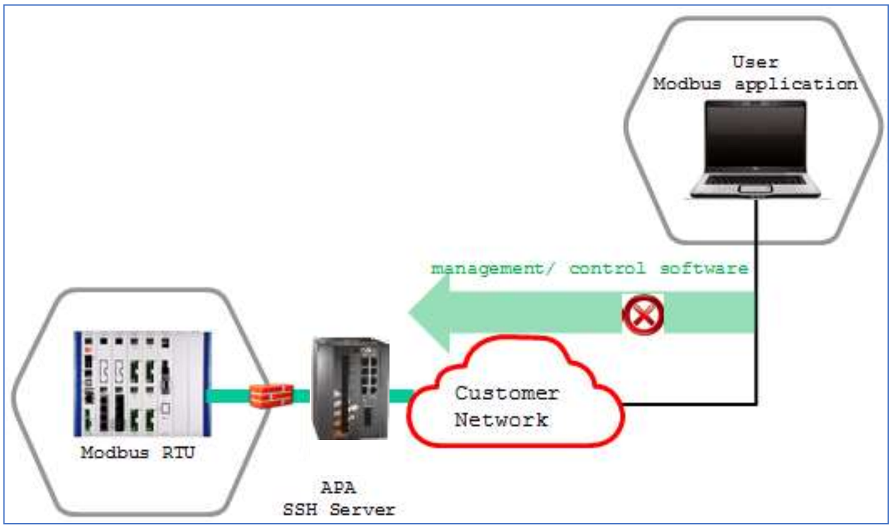


Figure 13 – Inactive APA is Denying Access to RTU

After successful log-in of the user, a profile is assigned to the user and access is granted to the RTU.

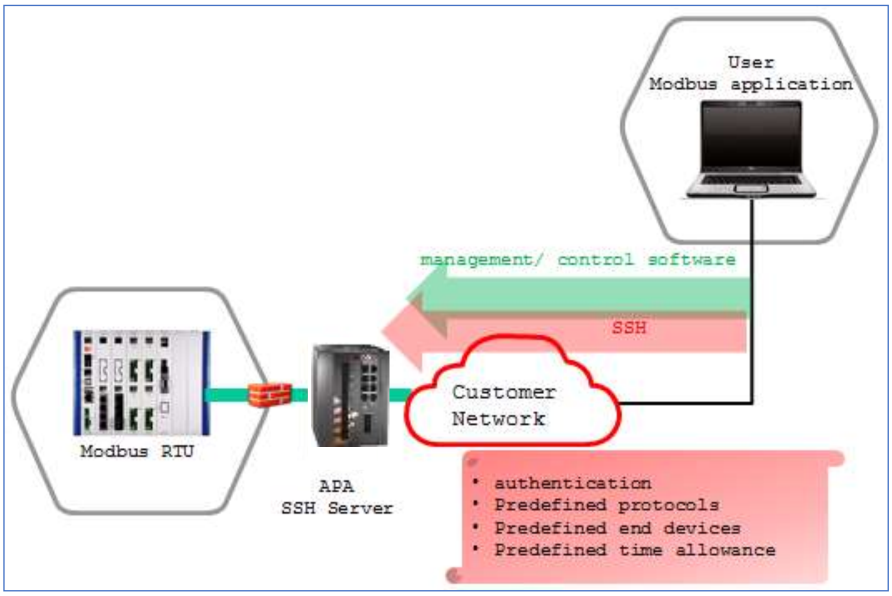


Figure 14 – User Authentication at APA

Key benefits of the APA service are the logs and capture of interesting traffic. The user actions are logged and the available for the RTU IP session is captured and saved.

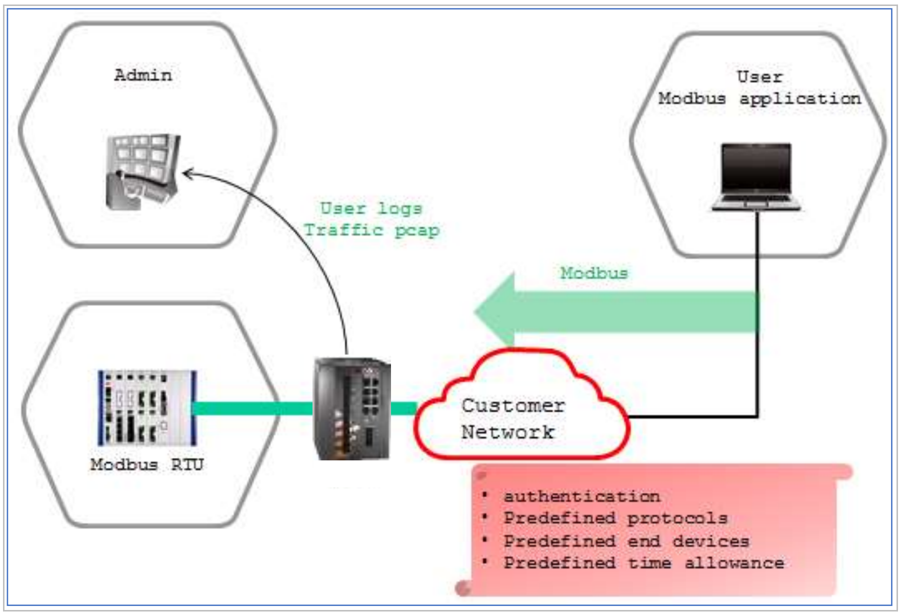


Figure 15 – Logs and RTU IP Session Capture

3.2 Implementation

3.2.1 Scalability of APA

The maximum values that are permitted are as follows:

- Admin Stations—50
- Users—maximum of 2 clients can be connected simultaneously; 50 users can be created.
- Profiles—5
- Protocols—25

3.2.2 Client Connection to APA

- A client requiring access to an RTU will open an SSH session to the APA interfaces for authentication.
- All physical ports of the iSG18GFP via which a client incoming connection is possible are to be specified at the APA ("APA ports").
- The client may use standard SSH text-based clients such as PuTTY, CRT, etc.
- The authentication is username and password based.
- Authentication attempts are limited to 3. After that the system will close the SSH server for one minute. After 9 attempts, the IP will be blocked.
- The APA allows up to two users connection simultaneously.

3.2.3 APA Security Access Lists

Configuration of the APA includes the following points:

- Server properties
- APA ports: defining of the APA ports
- Protocol list: defining of a list of TCP/UDP protocol ports as interesting traffic
- Profiles: defining of an RTU(s) and interesting traffic
- Users: defining of users
- Assignment of users to profiles

Once configuration is made and the APA is enabled, security L3 & L4 access lists (ACL) will be created and assigned to the APA ports and the RTU ports. The ACLs will enforce the following behavior.

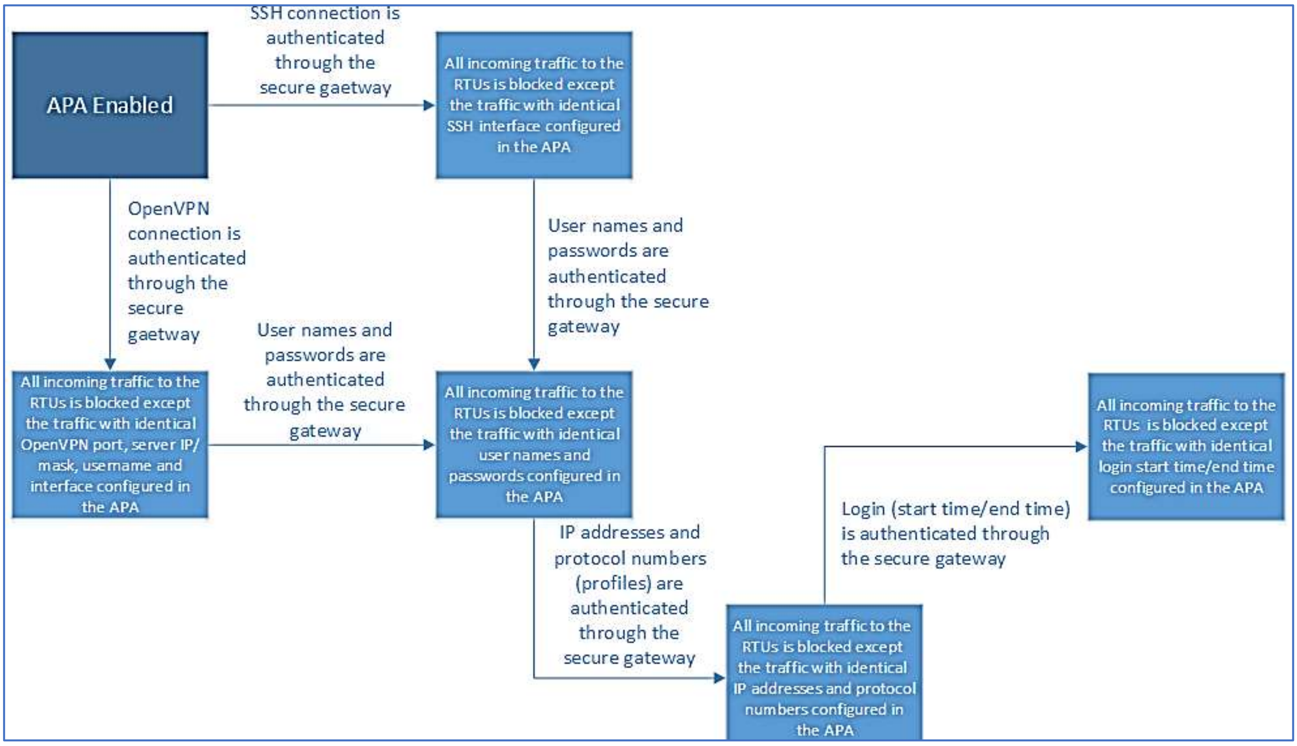

APA Enabled
SSH connection is authenticated through the secure gaetway
All incoming traffic to the RTUs is blocked except the traffic with identical SSH interface configured in the APA
OpenVPN connection is authenticated through the secure gaetway
User names and passwords are authenticated through the secure gateway
All incoming traffic to the RTUs is blocked except the traffic with identical OpenVPN port, server IP/ mask, username and interface configured in the APA
User names and passwords are authenticated through the secure gateway
All incoming traffic to the RTUs is blocked except the traffic with identical user names and passwords configured in the APA
IP addresses and protocol numbers (profiles) are authenticated through the secure gateway
All incoming traffic to the RTUs is blocked except the traffic with identical IP addresses and protocol numbers configured in the APA
Login (start time/end time) is authenticated through the secure gateway
All incoming traffic to the RTUs is blocked except the traffic with identical login start time/end time configured in the APA

Figure 16 – APA Security Access Lists

3.2.3.1 ACL Usage

The APA features use the following ACL resources. Thus, the system administrator should avoid tempering or using these.

3.2.3.1.1 IP Access List Extended

- priorities 11- 255. (up to 245 ACLs)

3.2.3.1.2 MAC Access Lists

- priority number 15 (single ACL)

3.2.4 User Activity Logs

The following are main syslog messages generated by the APA for user activity.

- "U“er %s was disconnected"
- ”T“me window has elapsed for assign id %d"
- ”U“er %s attempt to connect with occupied IP address(%s)"
- ”U“known User (%s) has tried to connect via VPN (port %d)"
- ”U“known User (%s) has tried to connect from %s"
- ”U“er %s attempted to perform an additional login attempt"
- ”V“N port does not match to user %s"
- ”C“n't’find VPN port:%s"
- ”N“ such user %s"
- ”U“er %s connection failed, reached to maximum connected users"
- ”U“er %s has connected successfully from %s"
- ”U“er %s attempted to connect from undefined APA interface"
- ”S“lence-timeout has elapsed for user:%s"

3.2.5 USB Usage Note

✎ In this version, the hardware configuration allows operation of a single USB device (cellular modem OR external USB interface). Therefore, if using an iSG18GFP unit with cellular modem, make sure to select the correct configuration of active USB device for your purposes. To do so, please refer to iSG18GFP User Manual, Security, Section S, UM-S-iSG18GFP-4.5.06.01-EN.docx.

3.3 Configuration

3.3.1 L3 Authentication Proxy Configuration

For L3 authentication proxy configuration, an user is required to log into the device and go to the ACE. To use the APA feature, the following parameters has to be configured.

3.3.1.1 Users

You can define users who will get permissions based on profiles that will be assigned to them. There is also a possibility to define the age of the user i.e. how many days the user account will be valid. Once the number of days matching the age of the user has elapsed, the user won't be allowed anymore to access iSG18GFP.

✎ When generating a username, follow the username rules that are written on the screen.

When configuring users, a password is required. Ensure that the passwords match the shown requirement. If those requirements won't be respected, then the user creation will be aborted. Retype Password header rewrites the same password for the user limitation you are generating to access the secure gateway.

✎ When generating a password, follow the password rules that are written on-screen.

✎ If the password does not meet the password rules, it will be orange colored.

3.3.1.2 Profiles

The profile is composed of a name as a title that contains the IP address and port number. Based on the profile limitation, only a user to whom a particular profile is assigned will be allowed access. A profile can be assigned to several users.

✎ When generating a profile, multiple IP / subnet mask addresses and protocols can be set to each profile.

3.3.1.3 Assigning Modes

Once users and profiles are created, there is a need to define usage conditions. These conditions describe when and how often will the user be granted access to iSG18GFP. Therefore, an assign will contain a user plus an assigned profile and its time limit for having access to iSG18GFP.

There are several assigning modes. Each mode describes a unique possibility that affects the users' access to iSG18GFP. A short explanation about the different types of assigning modes is shown below:

- **assign**: This mode works by assigning a username to a profile and adding the start time and end time of the assign. Before the start time and after the end time, the user is unable to access. Only in the specified timeframe, the user can access the iSG18GFP.
- **assign-one-time**: This mode is very similar to the "assign" mode, but it gives access only once. Once logged out, additional access for the user assigned is not possible unless manually configured by the administrator.
- **assign-repeatedly-daily**: This mode works by assigning a user and profile as in all others but with defined hours for daily start and end.
- **assign-repeatedly-weekly**: This mode works by assigning access to iSG18GFP on specific days of the week between certain start and end hours only per day. To use this, there is a need to configure one of the following parameters: "ends-on" or "ends afterends-on" is the date that the user will no longer be available. This date has to match with the end date that is configured. For example, if the end date day is a Friday, the end on date has to be a Friday as well.
    - "ends-after" is a value for the cycles of weeks for which the user account will be valid. For example, if to a user a weekly access from Monday to Friday is assigned by configuring start-time and end-time, the ends after parameter is set to 3. Then, after 3 weeks the user access will become inactive.

- **assign-repeatedly-monthly**: This mode is exactly the same as the weekly configuration but just adapted to months instead of weeks to make it easier to configure long term user activity.

3.3.1.4 Admin-Stations

This option gives the possibility to assign an IP address for which any access from it will be allowed.

3.3.1.5 Method

Method is a type of access to a port that will be given to a user. Any attempt to access the iSG18GFP from an unauthorized port will be declined and will be considered as an unauthorized attempt to access the unit.

There are 2 methods: SSH (Secure Shell) and VPN (Virtual Private Network) as follows:

- SSH: There is a need to define the physical Ethernet/cellular port that will be used for the connection.
- VPN: There is a need to define the physical port and the port number that will be used for the connection including the IP address of the VPN server, and it’s users name.

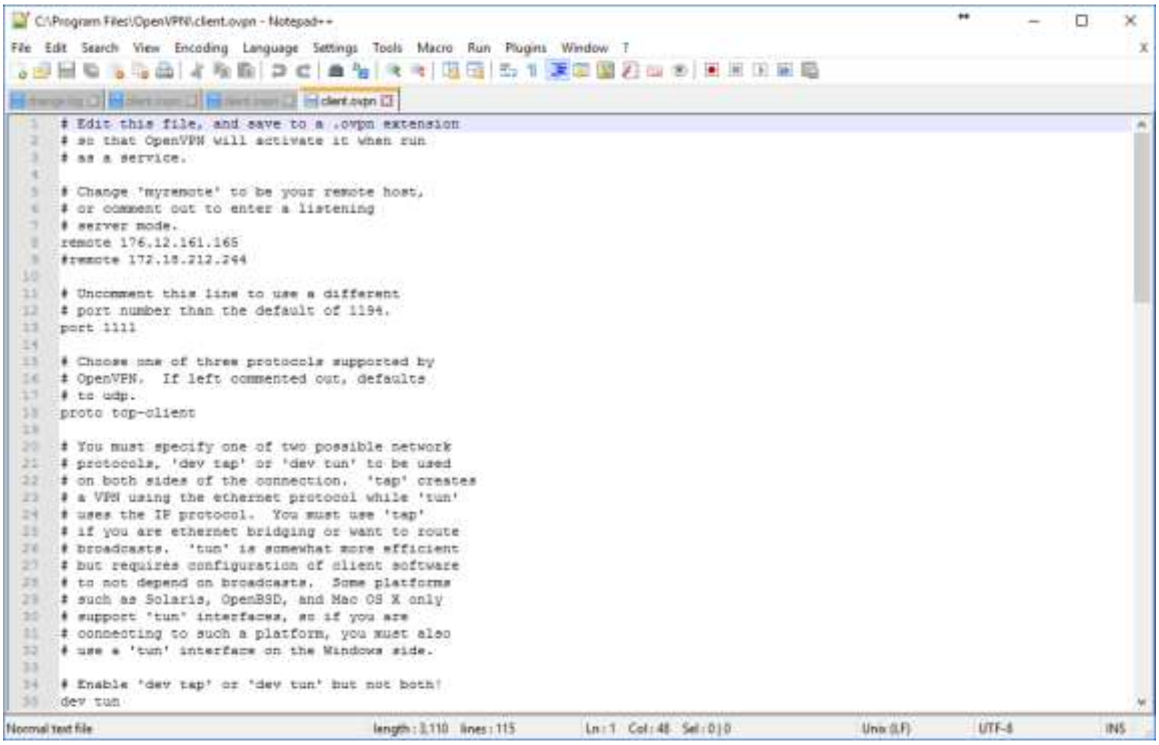
✎ SSH interfaces and open VPN interfaces must be exclusive. Each physical interface can be used either with SSH method of connection or VPN method of connection.

Any parameters such as user, profile, assign, etc. can be erased using the command `apa clear + ….`

To activate the feature, type `apa admin-status enable`

3.3.2 OpenVPN Configuration

1. Install **OpenVPN** client in your PC.
2. Go to C:\Program Files\OpenVPN and open ***client.ovpn*** file with Notepad++. client.ovpn file opens.


C:\Program Files\OpenVPN\client.ovpn - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
client.ovpn
Normal text file
length : 3,110 lines : 115
Ln : 1 Col : 48 Sel : 0 | 0
Unix (LF)
UTF-8
INS

```
1  # Edit this file, and save to a .ovpn extension
2  # so that OpenVPN will activate it when run
3  # as a service.
4
5  # Change 'myremote' to be your remote host,
6  # or comment out to enter a listening
7  # server mode.
8  remote 176.12.161.165
9  #remote 172.18.212.244
10
11 # Uncomment this line to use a different
12 # port number than the default of 1194.
13 port 1111
14
15 # Choose one of three protocols supported by
16 # OpenVPN.  If left commented out, defaults
17 # to udp.
18 proto tcp-client
19
20 # You must specify one of two possible network
21 # protocols, 'dev tap' or 'dev tun' to be used
22 # on both sides of the connection.  'tap' creates
23 # a VPN using the ethernet protocol while 'tun'
24 # uses the IP protocol.  You must use 'tap'
25 # if you are ethernet bridging or want to route
26 # broadcasts.  'tun' is somewhat more efficient
27 # but requires configuration of client software
28 # to not depend on broadcasts.  Some platforms
29 # such as Solaris, OpenBSD, and Mac OS X only
30 # support 'tun' interfaces, so if you are
31 # connecting to such a platform, you must also
32 # use a 'tun' interface on the Windows side.
33
34 # Enable 'dev tap' or 'dev tun' but not both!
35 dev tun
```

Figure 17: client.ovpn file

3. Change the IP address in line 8 (176.12.161.165) into a new IP address in which the SSL server will open an SSL session.
4. Change the port in line 13 (1111) according to the username generated in the APA:

- Port 1111, for tech1 (for example)
- Port 1112, for tech2 (for example)
- Port 1113, for tech3 (for example)

Right click the **OpenVPN GUI** and select **Connect**. OpenVPN opens.

5.

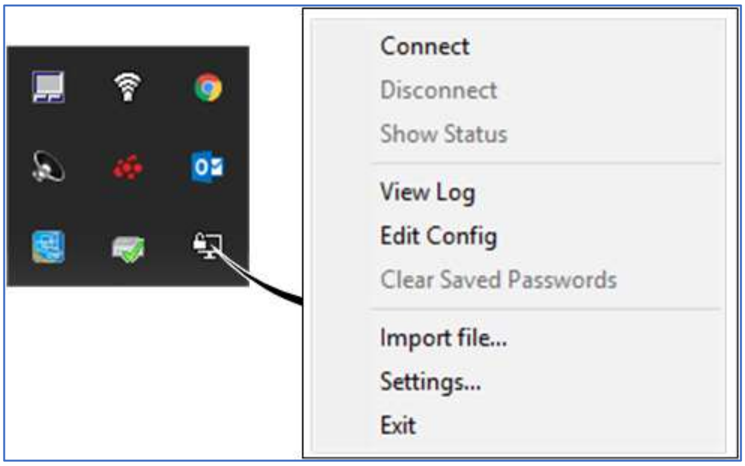
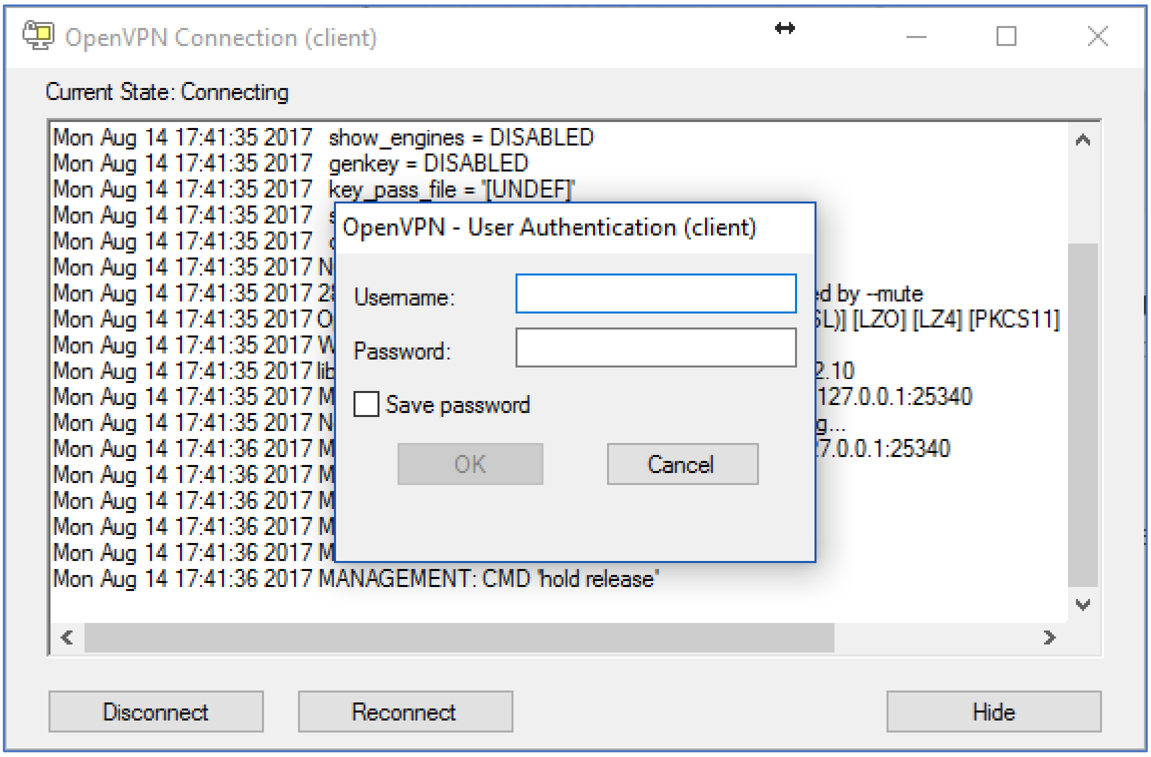


Figure 18: OpenVPN GUI



Current State: Connecting

```
Mon Aug 14 17:41:35 2017  show_engines = DISABLED
Mon Aug 14 17:41:35 2017  genkey = DISABLED
Mon Aug 14 17:41:35 2017  key_pass_file = '[UNDEF]'
Mon Aug 14 17:41:35 2017  s
Mon Aug 14 17:41:35 2017  c
Mon Aug 14 17:41:35 2017 N
Mon Aug 14 17:41:35 2017 2                              d by --mute
Mon Aug 14 17:41:35 2017 O                              SL)] [LZO] [LZ4] [PKCS11]
Mon Aug 14 17:41:35 2017 W
Mon Aug 14 17:41:35 2017 lib                            2.10
Mon Aug 14 17:41:35 2017 M                              127.0.0.1:25340
Mon Aug 14 17:41:35 2017 N                              g...
Mon Aug 14 17:41:36 2017 M                              7.0.0.1:25340
Mon Aug 14 17:41:36 2017 M
Mon Aug 14 17:41:36 2017 M
Mon Aug 14 17:41:36 2017 M
Mon Aug 14 17:41:36 2017 M
Mon Aug 14 17:41:36 2017 MANAGEMENT: CMD 'hold release'
```

OpenVPN - User Authentication (client)

Username:

Password:

□ Save password

Figure 19: OpenVPN Connection (client)

6. Enter the username according to the APA username you've generated and the port you have set-up).
7. Enter the password according to the APA username you've generated) and press OK.

Once OpenVPN client connects, the PC will have an IP address defined in the SSL server and OpenVPN session will be operational.

3.4 L3 Authentication Proxy Commands Hierarchy

```
+ application connect
```

+ apa admin-status

- enable

- disable

+ apa config

- user {username {(Small letters only)}|{password-age (between 0-99999 or never if blank)}| {proxy (none, ldap, radius)} + password {(string:8-32)}

- profile {name (string:1-50)} {address (A.B.C.D|A.B.C.D/XY)} {port (1-65535)} {rtu-id (1-25)

- assign {username (string:1-32)} {profile (string:1-50)} {start-time (mm:dd:yyy:hh:mn:ss)} {end-time (mm:dd:yyy:hh:mn:ss)}

- assign-one-time {username (string:1-32)} {profile (string:1-50)}{start-time (mm/dd/yyyy-hh:mm)} {end-time (mm/dd/yyyy-hh:mm)}

- assign-repeatedly-daily {username (string:1-32)} {profile (string:1-50)} {start-time (mm/dd/yyyy-hh:mm)} {end-time (mm/dd/yyyy-hh:mm)} {ends-after (<1-999)}| ends-on (mm/dd/yyyy)}

- assign-repeatedly-weekly {username (string:1-32)} {profile (string:1-50)} {start-time (mm/dd/yyyy-hh:mm)} {end-time (mm/dd/yyyy-hh:mm)} {ends-after (<1-999)}| ends-on (mm/dd/yyyy)}

- assign-repeatedly-monthly {username (string:1-32)} {profile (string:1-50)} {start-time (mm/dd/yyyy-hh:mm)} {end-time (mm/dd/yyyy-hh:mm)} {ends-after (<1-999)}| ends-on (mm/dd/yyyy)}

- admin-stations {address (A.B.C.D | A.B.C.D/XY)}

+ method

- ssh {fastethernet (1-8)}|{gigabitethernet (1-2)}|{cellular ppp0}

- vpn {port (1024-65535)} {server-network (A.B.C.D/2-30)} {username (string:1-10)} {fastethernet(1-8)}{gigabitethernet(1-2)} {cellular ppp0}

+ general

- silence {timeout (0-60)}

- ssh {ssh-port (1024-65535)}

+ apa update

- rtu {rtu-id (1-25)}

- assign {username (string:1-32)} {profile (string:1-50)} {start-time (mm:dd:yyy:hh:mn:ss)} {end-time (mm:dd:yyy:hh:mn:ss)} {id (id number)}

+ apa delete

```
            - user {username (string:1-10)}

            - profile {name (string:1-50)} {address (A.B.C.D|A.B.C.D/E)}  {port (1-65535)}  {rtu-id  (1-25)}

            - assign  {username (string:1-10)} {profile (string:1-50)} {id (string:1-1250)}

            - admin-stations  {address (A.B.C.D/XY)|(A.B.C.D)}

        + method

            - ssh {fastethernet (1-8)}|{gigabitethernet (1-2)}|{cellular ppp0}

            - vpn {port (1024-65535)}{fastethernet(1-8)}{gigabitethernet(1-2)} {cellular ppp0}
    + apa clear
            - user

            - profiles

            - assigns

            - all

            - interfaces

            - logs

            - counters

        + apa disconnect {username (string:1-10)}

        + apa export

            - all {Remote-address (A.B.C.D)}

            - pcaps {Remote-address (A.B.C.D)}

            - logs {Remote-address (A.B.C.D)}

        + apa show

            - detailed

            - interfaces

            - users

            - rtus

            - profiles

            - assigns

            - admin-stations

            - log           - counters
```

3.5 L3 Authentication Proxy Commands Description

Table 3 – Authentication Proxy Commands

Command	Description

Command	Description
remote-log-results-exportSend the captured logs to a USB stick or TFTP server.application connectAccess the ACE mode. apa admin-statusEnable/disable the APA. apa config	Access the config mode of the APA.
<user>	Sets the user credentials (i.e., username, password, age, and proxy). Up to 50 users can be configured. A set of conditions limit specific users from accessing the secure gateway. The limitation is done through predefined passwords saved in the secure gateway.
<profile>	Configures the profile name, address and ports. Up to 25 profiles can be configured. A set of conditions limiting profiles to access the secure gateway using specific IP address/subnet mask and protocols (protocols ports) only.
<assign>	Sets the conditions giving users with a profile the ability to access the secure gateway, only within a single time frame. The profile and user must be pre-defined.
<assign-one-time>	Sets of conditions limiting users with a profile to access the secure gateway only one single time. The profile and user must be pre-defined.
< assign-repeatedly-daily>	Sets of conditions limiting users with a profile to access the secure gateway daily for pre-defined hours. The profile and user must be pre-defined.
< assign-repeatedly-weekly>	Sets of conditions limiting users with a profile to access the secure gateway on a weekly basis or less during pre-defined hours. The profile and user must be pre-defined.
< assign-repeatedly-monthly>	Sets of conditions limiting users with a profile to access the secure gateway on a monthly basis or less during pre-defined hours. The profile and user must be pre-defined.
<admin-station>	A command to configure the admin station – an admin station is always allowed to access the unit independent of any date or protocol limitation.
apa config method	Set the connection method and ports to connect to the unit(ssh/vpn).
<ssh>	Configuring the SSH connection type, and the ports to be attached to this configuration (Fa/Gb/Cell).

Command	Description
<vpn>	Configuring the VPN connection type and the ports to be attached to this configuration (Fa/Gb/Cell).
apa config general	For general parameter configuration (timeout and ssh-ports).
apa update	To make changes and updates on the existing configuration such as RTU ID and assign parameters (such as start time, end time, etc.)
apa delete	To delete a user or a profile that is not needed anymore or that might have been used for malicious use.
apa clear	This command is for clearing a whole category, such as users – it will erase all the users. The same applies for profiles, assigns, logs, counters, etc. There is also a possibility to clear all by typing "apa clear all."
apa disconnect	To disconnect a user by the username.
apa export	To export the PCAPS and logs via TFTP server.
apa show	Several show commands providing the configured APA parameters such as user's levels of connections, profiles, logs and counters.

3.6 Authentication Proxy Syslogs

The following events will generate a log and be sent to the syslog server, if configured.

Below are the events and examples of the sent log:

# outside of time window

```
Sep  8 15:29:46 SmartSwitch APA_USER_LOGIN[2923]: APA_USER_LOGIN USER tech1 HAS ATTEMPTED TO CONNECT FROM 172.18.212.32 HAS FAILED. NOT IN TIME WINDOW
```

# succesful login

```
Sep  8 16:10:35 SmartSwitch APA_USER_LOGIN[3607]: APA_USER_LOGIN USER tech1 CONNECTED_SUCCESSFULLY from 172.18.212.32
```

# user is already connected

```
Sep  8 16:11:25 SmartSwitch APA_USER_LOGIN[3793]: APA_USER_LOGIN USER tech1 IS ALREADY CONNECTED from 172.18.212.32
```

# different user from occupied IP

```
Sep  8 16:35:09 SmartSwitch APA_USER_LOGIN[4238]: APA_USER_LOGIN USER tech2 TRIED TO CONNECT WITH OCCUPIED IP ADDRESS 172.18.212.32
```

# max users (2 users is the limit)

```
Sep  8 16:43:42 SmartSwitch APA_USER_LOGIN[6223]: APA_USER_LOGIN FAILED LOGIN#012Max users allowed are logged in.
```

#end of time window for a user

```
Sep  8 15:50:04 SmartSwitch APA[6621]: APA User tech1 was disconnected
Sep  8 15:50:04 SmartSwitch APA[6621]: APA Time window has elapsed for assign id 1
```

Event Logger

The Event Logger feature acts as a proxy for syslog clients. Its intention is modifying of the clients' original syslog messages to include additional information of identification before sending it to the network's syslog server.

4.1 Service Description

Use Case: A network includes multiple syslog clients at distributed locations and a centralized syslog server. A network admin would like to:

1. Aggregate messages from multiple clients.
    a. Save the original messages.
    b. Enrich the messages with additional information about the aggregator.
        i. Location
        ii. Region
        iii. Host name
        iv. A unique numeric value identifying the aggregator syslog messages.
    c. Send the edited messages from a single common source (the aggregator).
2. Better identify the clients.
    a. Edit the clients' syslog messages with additional information about the client.
        i. Group identifier to which the client belongs to. For example, group id=1 may be the network manager way to identify PLCs while group id=2 represents RTUs.
        ii. Set a constant severity level to all syslog messages originated by a specific client.

4.2 Implementation

The Event Logger implementation consists of the following:

1. Syslog server for distributed syslog clients. This is supported as TCP and UDP simultaneously.

2. Syslog client towards the network syslog server. This is supported with TCP. Up to 2 remote servers can be set as destinations.

3. Syslog messages aggregator that collects and saves the original client messages. The information is saved automatically to the unit's flash drive.

4. Syslog message proxy that is adding additional information to the original message before sending it to the network syslog server.

5. Usage of the underlying link redundancy mechanism that allows continuous operation over cellular network (on supporting units) on wired network disconnection.

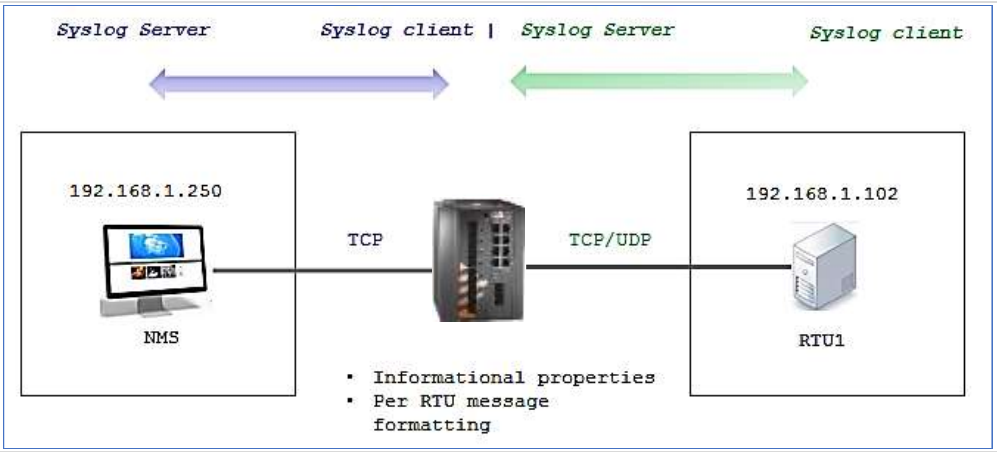

Syslog Server
Syslog client | Syslog Server
Syslog client
192.168.1.250
NMS
TCP
TCP/UDP
192.168.1.102
RTU1
• Informational properties
• Per RTU message formatting

Figure 20 – Event Logger as Client and Server

✎ The event logger uses facility 3 (Daemon) for outgoing messages.

✎ The event logger local syslog server must use the local ACE application-host interface.

4.2.1 Message Format

The Event Logger will keep the client’s original information as data of a new message. It will add to it the following information:

1. **New time**: The transmit time from the logger to the network server.
2. **New priority**: As per the configuration options, you can set a syslog priority for messages originating from a client.
3. **New host name**: The event logger name.
4. **Client message ID**: An identifier for the clients’ original message.
5. **Region**: Configurable text to represent a region where the Event Logger is installed.
6. **Location**: A second configurable text to represent the location where the Event Logger is installed.
7. **End of message identifier**: An optional two-byte value which can be used to determine how the end of a message is identified at the server from the logger.

The fields added by the logger are separated by a single space by default. The option of using a different delimiter other than space is available. For example, the fields can be separated with the symbol # or @.

4.2.2 Example

A client’s original message is as follows:

```
<134>Mar  8 17:34:34 client CFA  Slot0/8 Link Status [DOWN]
```

The new message from the logger (for identification here only, the original message is shown in *italic*) is:

<29>,Mar 08 18:31:55,spoke1,079,Rome,sub_st1,001,*<134>Mar 8 17:34:34 client CFA Slot0/8 Link Status [DOWN]*,#

The Event Logger has made the following additions/ changes to the message.

- Changed the message priority from 134 (facility local0, severity informational> to 29 (facility Daemon, severity notification>.
- The Event Logger given name is spoke1.
- The client original message identifier is 079.
- The Event Logger is installed in a region called Rome at location called sub_st1.
- The client is identified as belonging to group 001.
- The new fields are separated with a comma.
- The message is ended with the character #.

4.2.3 EOM Field

The logger configuration supports adding a decimal value at the end of the syslog message. This value can be another option for the network syslog server to parse the message with and deduct information about its origin. The actual usage of this field is dependent on the network syslog server itself.

The EOM (End Of Medium) is a configurable decimal value in the range 0-65535. This value is seen 'on the wire' as a two byte structure [byte1,<0-FF>][byte2,<0-FF>].

Typically, the server will parse this value not as a single decimal value but as a sequence of these two bytes. Dependent on the server implementation it may further present the values of these bytes as special characters/ symbols.

Assuming for example that the server parses the value of each byte per the ASCII table, the user can configure the EOM value so that the ASCII printable characters are added at the end of the message.

The default state of the EOM field is disabled.

The following examples consider the server supports the ASCII printable characters. The ASCII table of printable characters is included below for reference.

- For an EOM configured value of 44, the symbol "," (comma) will be added at the end of the syslog message.
- If a sequence of two special characters is desired, the best option is to look at the hexadecimal representation of each symbol in the table and then conclude the corresponding decimal value to configure at the logger EOM.

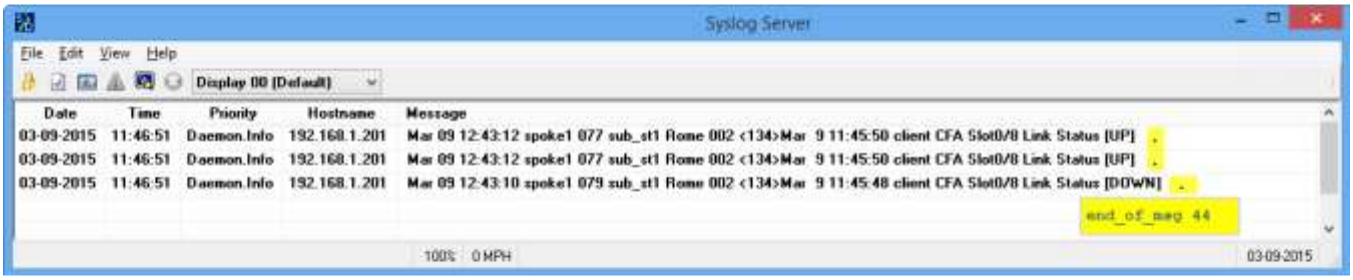
For example, to add # /, we will consider each symbol as an independent byte and look at the table for its hex value.

Byte structure:	[Byte1]	[Byte2]
Special characters:	[#]	[/]
Hex Value:	[23]	[2F]

We combine 23 and 2F—together these 2 bytes show 232F. Using a calculator, a corresponding decimal value of 9007 is to be configured in the EOM field.

4.2.3.1 EOM View in Syslog Server

Below is an example of a syslog server displaying a comma character for an EOM configured value of 44.



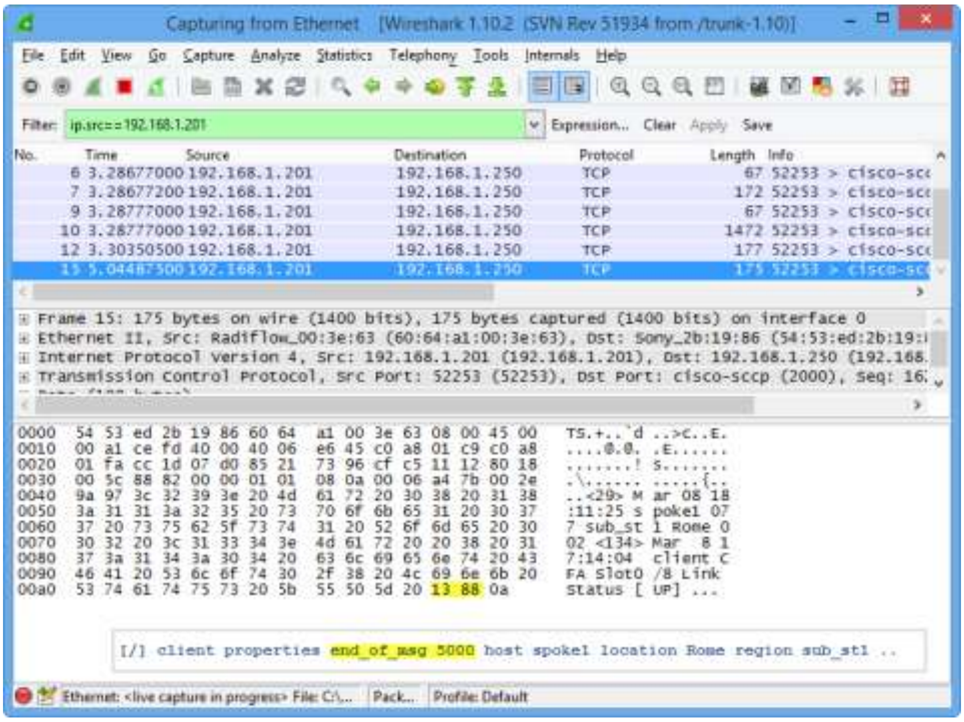
Date	Time	Priority	Hostname	Message
03-09-2015	11:46:51	Daemon.Info	192.168.1.201	Mar 09 12:43:12 spoke1 077 sub_st1 Rome 002 <134>Mar 9 11:45:50 client CFA Slot0/8 Link Status [UP] ,
03-09-2015	11:46:51	Daemon.Info	192.168.1.201	Mar 09 12:43:12 spoke1 077 sub_st1 Rome 002 <134>Mar 9 11:45:50 client CFA Slot0/8 Link Status [UP] ,
03-09-2015	11:46:51	Daemon.Info	192.168.1.201	Mar 09 12:43:10 spoke1 079 sub_st1 Rome 002 <134>Mar 9 11:45:48 client CFA Slot0/8 Link Status [DOWN] ,

end_of_msg 44

Figure 21 – Example of Syslog Server Displaying Commas

4.2.3.2 EOM View in Wireshark

Below is an example of a Wireshark view of the two bytes of the configured EOM value.


Capturing from Ethernet [Wireshark 1.10.2 (SVN Rev 51934 from /trunk-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save
Ethernet: <live capture in progress> File: C:\... Pack... Profile: Default

Filter: ip.src==192.168.1.201

```
No.   Time       Source         Destination    Protocol  Length Info
    6 3.28677000 192.168.1.201  192.168.1.250  TCP           67 52253 > cisco-scc
    7 3.28677200 192.168.1.201  192.168.1.250  TCP          172 52253 > cisco-scc
    9 3.28777000 192.168.1.201  192.168.1.250  TCP           67 52253 > cisco-scc
   10 3.28777000 192.168.1.201  192.168.1.250  TCP         1472 52253 > cisco-scc
   12 3.30350500 192.168.1.201  192.168.1.250  TCP          177 52253 > cisco-scc
   15 5.04487500 192.168.1.201  192.168.1.250  TCP          175 52253 > cisco-scc
```

```
⊞ Frame 15: 175 bytes on wire (1400 bits), 175 bytes captured (1400 bits) on interface 0
⊞ Ethernet II, Src: Radiflow_00:3e:63 (60:64:a1:00:3e:63), Dst: Sony_2b:19:86 (54:53:ed:2b:19:
⊞ Internet Protocol Version 4, Src: 192.168.1.201 (192.168.1.201), Dst: 192.168.1.250 (192.168.
⊞ Transmission Control Protocol, Src Port: 52253 (52253), Dst Port: cisco-sccp (2000), Seq: 16:
```

```
0000  54 53 ed 2b 19 86 60 64  a1 00 3e 63 08 00 45 00   TS.+..`d ..>c..E.
0010  00 a1 ce fd 40 00 40 06  e6 45 c0 a8 01 c9 c0 a8   ....@.@. .E......
0020  01 fa cc 1d 07 d0 85 21  73 96 cf c5 11 12 80 18   .......! s.......
0030  00 5c 88 82 00 00 01 01  08 0a 00 06 a4 7b 00 2e   .\...... .....{..
0040  9a 97 3c 32 39 3e 20 4d  61 72 20 30 38 20 31 38   ..<29> M ar 08 18
0050  3a 31 31 3a 32 35 20 73  70 6f 6b 65 31 20 30 37   :11:25 s poke1 07
0060  37 20 73 75 62 5f 73 74  31 20 52 6f 6d 65 20 30   7 sub_st 1 Rome 0
0070  30 32 20 3c 31 33 34 3e  4d 61 72 20 20 38 20 31   02 <134> Mar  8 1
0080  37 3a 31 34 3a 30 34 20  63 6c 69 65 6e 74 20 43   7:14:04  client C
0090  46 41 20 53 6c 6f 74 30  2f 38 20 4c 69 6e 6b 20   FA Slot0 /8 Link
00a0  53 74 61 74 75 73 20 5b  55 50 5d 20 13 88 0a      Status [ UP] ...
```

```
[/] client properties end_of_msg 5000 host spoke1 location Rome region sub_st1 ..
```

Figure 22 – Wireshark View of the 2 Bytes of EOM Value

Download the network sniffer Wireshark 2.6.1 (64-bit) at https://www.wireshark.org/

4.2.4 The ASCII Printable Characters Table

The ASCII printable characters table is shown here for your convienience. Please refer to available sources such as http://www.asciitable.com/ for the extended table and additional information.

The logger implementation itself has no specific relation to the ASCII table. The OEM field allow to set values for the last two bytes of the syslog message. The parsing of these values is done by the network syslog server and is usualy based on the ASCII table.

Table 4 – ASCII Printable Characters Table

Dec	Hex	Binary	Character	Description
32	20	00100000	**Space**	**space**
33	21	00100001	**!**	exclamation mark
34	22	00100010	**"**	double quote
35	23	00100011	**#**	number
36	24	00100100	**$**	dollar
37	25	00100101	**%**	percent
38	26	00100110	**&**	ampersand
39	27	00100111	**'**	single quote
40	28	00101000	**(**	left parenthesis
41	29	00101001	**)**	right parenthesis
42	2A	00101010	*****	asterisk
43	2B	00101011	**+**	plus
44	2C	00101100	**,**	comma
45	2D	00101101	**-**	minus
46	2E	00101110	**.**	period

Dec	Hex	Binary	Character	Description
47	2F	00101111	**/**	slash
48	30	00110000	**0**	zero
49	31	00110001	**1**	one
50	32	00110010	**2**	two
51	33	00110011	**3**	three
52	34	00110100	**4**	four
53	35	00110101	**5**	five
54	36	00110110	**6**	six
55	37	00110111	**7**	seven
56	38	00111000	**8**	eight
57	39	00111001	**9**	nine
58	3A	00111010	**:**	colon
59	3B	00111011	**;**	semicolon
60	3C	00111100	**<**	less than
61	3D	00111101	**=**	equality sign
62	3E	00111110	**>**	greater than
63	3F	00111111	**?**	question mark
64	40	01000000	**@**	at sign
65	41	01000001	**A**	
66	42	01000010	**B**	
67	43	01000011	**C**	
68	44	01000100	**D**	
69	45	01000101	**E**	
70	46	01000110	**F**	
71	47	01000111	**G**	
72	48	01001000	**H**	
73	49	01001001	**I**	
74	4A	01001010	**J**	
75	4B	01001011	**K**	
76	4C	01001100	**L**	
77	4D	01001101	**M**	
78	4E	01001110	**N**	
79	4F	01001111	**O**	
80	50	01010000	**P**	
81	51	01010001	**Q**	
82	52	01010010	**R**	
83	53	01010011	**S**	
84	54	01010100	**T**	
85	55	01010101	**U**	

Dec	Hex	Binary	Character	Description
86	56	01010110	**V**	
87	57	01010111	**W**	
88	58	01011000	**X**	
89	59	01011001	**Y**	
90	5A	01011010	**Z**	
91	5B	01011011	**[**	left square bracket
92	5C	01011100	****	backslash
93	5D	01011101	**]**	right square bracket
94	5E	01011110	**^**	caret / circumflex
95	5F	01011111	_	underscore
96	60	01100000	`	grave / accent
97	61	01100001	**a**	
98	62	01100010	**b**	
99	63	01100011	**c**	
100	64	01100100	**d**	
101	65	01100101	**e**	
102	66	01100110	**f**	
103	67	01100111	**g**	
104	68	01101000	**h**	
105	69	01101001	**i**	
106	6A	01101010	**j**	
107	6B	01101011	**k**	
108	6C	01101100	**l**	
109	6D	01101101	**m**	
110	6E	01101110	**n**	
111	6F	01101111	**o**	
112	70	01110000	**p**	
113	71	01110001	**q**	
114	72	01110010	**r**	
115	73	01110011	**s**	
116	74	01110100	**t**	
117	75	01110101	**u**	
118	76	01110110	**v**	
119	77	01110111	**w**	
120	78	01111000	**x**	
121	79	01111001	**y**	
122	7A	01111010	**z**	
123	7B	01111011	**{**	left curly bracket
124	7C	01111100	**|**	vertical bar

Dec	Hex	Binary	Character	Description
125	7D	01111101	**}**	right curly bracket
126	7E	01111110	**~**	tilde
127	7F	01111111	DEL	delete

Source: RapidTables, https://www.rapidtables.com/code/text/ascii-table.html Online, Accessed On June 13, 2018 [4]

4.3 Event Logger Commands Hierarchy

```
+ application connect

+ event_logger

– enable

–  disable

+ server

- add {local_server_address <A.B.C.D>} [port (514,<0-65535>)]
[protocol (udp,<udp| tcp>)]

– remove local_server_address <A.B.C.D>

– ..

+ client

– add {remote_server_address <A.B.C.D>} {port (514,<0-65535>)}

– remove remote_server {address <A.B.C.D>}

– properties {host <text>} {location <text>} {region <text>}  [eom_enable(disable,
<disable|enable>)] [end_of_msg(0,<0-65535>)]
[separator <>]

– ..

+ rtu

- add {address <A.B.C.D>} [group(0,<0-255>)]
{severity <emergency | alert | critical | error | warning | notice | informational |
debug>}

- remove {address <A.B.C.D>}

– ..

+ access_panel

- add {type mercury} {address <A.B.C.D>} [port (def=443,<1-65535>)]
{user_name<>} {password<>} [group(0,<0-255>)]
```

{severity <emergency | alert | critical | error | warning | notice | informational | debug>}

- remove {address <A.B.C.D>}

– enable

– disable

– ..

+ if–mngr

- show

+ clearall

+ show

– server

- client

- rtu

- access_panel

– counters

– results file_names

– cur server_status

- cur tcp_clients

4.4 Event Logger Commands Description

Table 5 – Event Logger Commands Description

<table>
<tr><th>Command</th><th>Description</th></tr>
<tr><td>Event logger</td><td>Access the Event Logger.</td></tr>
<tr><td>Enable</td><td>Enable the feature.</td></tr>
<tr><td>Disable</td><td>Disable the feature.</td></tr>
<tr><td>Server add| remove</td><td>Set the properties of the iSG18GFP Event Logger as a syslog server.
<b>local_server_address:</b> the IP address of the local ‘application host’ ACE interface. This interface will be used for the syslog server functionality and will listen to TCP/UDP connections from syslog clients. State the IPv4 address in <A.B.C.D> format.
<b>port:</b> the local syslog server can listen to UDP or TCP packets from clients; the port is configurable by this field. Default: 514.
<b>protocol:</b> the local syslog server listens to UDP and TCP packets from clients. If changing the default port 514 is required, specify the protocol. default- udp.</td></tr>
<tr><td>Client</td><td>Set the properties of the iSG18GFP Event Logger as a syslog client. As a syslog client, the event logger works only in TCP mode towards a remote syslog server. The TCP port is configurable.</td></tr>
<tr><td>add|remove</td><td><b>remote_server_address:</b> the IP address of the target syslog server. Up to 2 servers can be set.
<b>port:</b> the TCP port number to be used. Default: 514.</td></tr>
<tr><td>Properties</td><td>As a syslog client, the event logger can add information to the original message which was received from the rtu syslog client.
<b>eom_enable:</b> enable or disable the end of message field. Default- disable.
<b>end_of_msg:</b> a numeric value to be entered at the end of the syslog message to be used as a measure of identification. Depending on the value, this object may be printable or not, per the ASCII table. Default- 0.
<b>host:</b> a string representing the Event Logger. Spaces are not allowed.
<b>location:</b> a string representing the Event Logger location. No spaces are allowed.
<b>region:</b> a string representing the Event Logger region. No spaces are allowed.
<b>separator:</b> choose the type of character to use as separator between the text fields. Supported are all letters, numbers and the following special characters: ~!@#$%^&amp;*()-_+=[]{}&lt;&gt;/\|.,:;

The symbol “?” (question mark) is not supported. Default is a single space.</td></tr>
</table>

Command	Description
	Set S (the capitol letter S) for a single space as the separator.
Rtu add| remove	'rtu' refers to the customer end device which is a syslog client, and for which the event logger will log and parse messages before sending to the network syslog server. **address**: the IPv4 address of the rtu with which it sends the syslog messages to the event logger. **group**: a numeric value used as an identifier. Default-0. **Severity**: set the syslog severity per rtu. Any syslog message originated from the specified rtu will be assigned this new severity by the logger before sending to the network syslog server.
access_panel add| remove	'access_panel' refers to the customer end device, which is an event client, and for whom the Event Logger will log and parse messages before sending to the network syslog server. The 'access_panel' addresses vendor specific devices, using propriety protocols for the event message format. **type**: the vendor device type. Currently supported is 'mercury'. **address**: the IPv4 address of the mercury panel with which it sends the event messages to the Event Logger. **port**: the port number used by the mercury panel for communication. Default- 443. **username**: username of the mercury panel used to access it. **password**: password of the mercury panel used to access it.
show	Show the configuration and state of the Event Logger.
clearall	Clears all Event Logger files.
if-mngr	Enters to features pertaining to the link redundancy mechanism.
Show	Show the configuration and state of the link redundancy operations.

4.5 Example of Event Logger

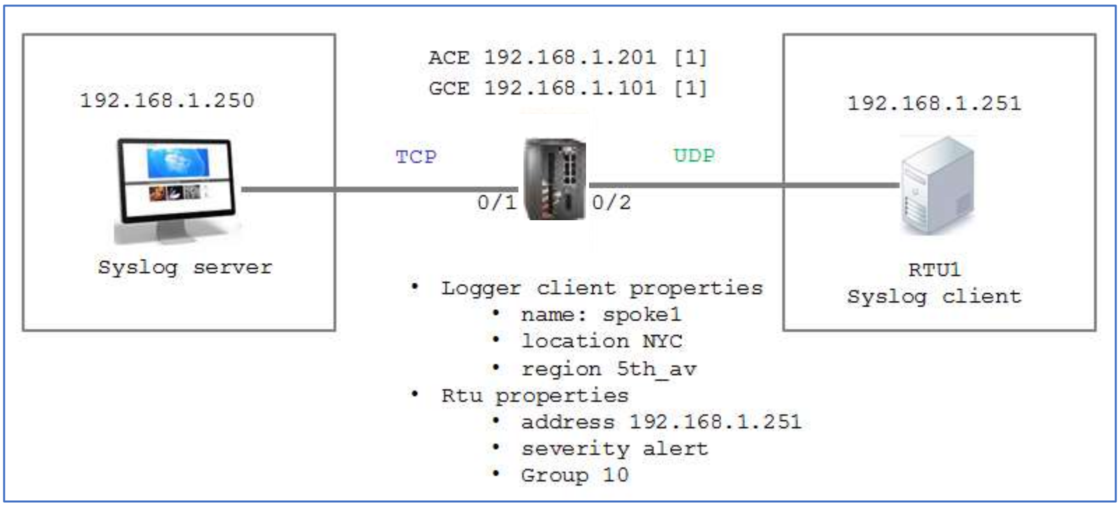


Figure 23 – Example of Event Logger Architecture

4.5.1 Configuration

1. Set host name (optional).

```
set host-name logger
```

2. Set management interface (optional).

```
config

interface vlan 1

ip add 192.168.1.101 255.255.255.0

no shutdown

end
```

3. Create an ACE Interface, 'application-host' type.

```
application connect

router interface create address-prefix 192.168.1.201/24 vlan 1 purpose application-host
```

4. Assign to the event logger to use the 'application-host' ACE interface as its local syslog server interface.

```
event_logger server add local_server_address 192.168.1.201 protocol udp port 514

event_logger server add local_server_address 192.168.1.201 protocol tcp port 514
```

5. Assign to the event logger syslog client properties and detail the remote syslog server address and tcp port.

```
event_logger client add remote_server_address 192.168.1.250 port 514
```

6. Assign the event logger syslog client properties, detail the descriptive fields.

```
event_logger client properties end_of_msg 5000 host spoke1 location NYC region 5TH_AV
```

7. Assign the group descriptive value and new severity for the specific RTU.

```
event_logger rtu add address 192.168.1.251 severity alert group 10
```

8. Set the logger’s local time.

```
date 2015.05.10-10:00:00
```

9. Enable the event logger.

```
event_logger enable

exit; write startup-cfg
```

4.5.2 Showing Outputs

```
[event_logger/]show server

STATE       : enabled

TCP PORT       : 514

UDP PORT       : 514

ADDRESS    : 192.168.1.201

 [event_logger/]show client

STATE       : enabled

REGION     : 5th_av

LOCATION    : NYC

HOST NAME   : spoke1

EOM        : 5000

ADDRESS    : 192.168.1.250

PORT       : 514

 [event_logger/]show rtu

+---------------+----------+-------+

|     IP      | SEVERITY | GROUP |

+===============+==========+=======+

| 192.168.1.251 |    1    |  10   |

+---------------+----------+-------+

[event_logger/]show cur server_status

EVENT LOGGER is CONNECTED
```

```
[event_logger/]show cur tcp_clients

KUKU

+----+------+--------+

| IP | PORT | SOCKET |

+====+======+========+

[event_logger/]
```

4.5.3 Testing Event Logger Setup

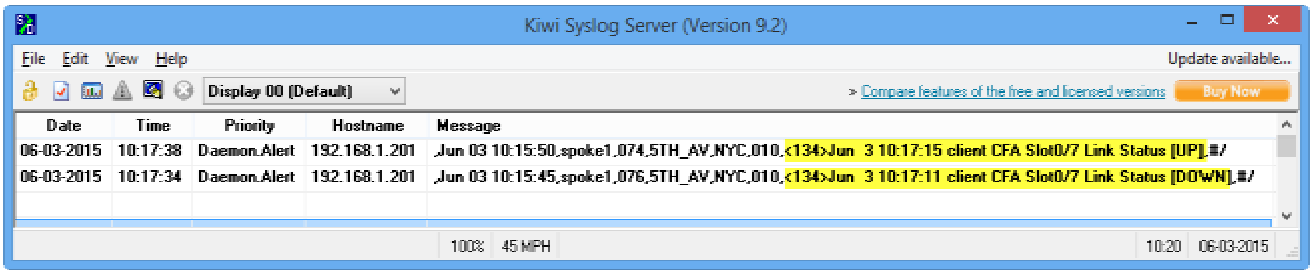
1. Place a USB drive that is formatted to FAT32 to the iSG18GFP Event Logger. To format in FAT32, refer to https://www.online-tech-tips.com/computer-tips/formatting-external-hard-drive-to-fat-32/
2. Send a syslog message from the client to the Event Logger. In the example below, the client is a switch sending link up/ link down notifications.
3. The Event Logger will reformat the message and send it to the syslog server.

- The original message of the client (facility local0, severity informational>):

```
<134>Jun 03 10:17:11 client CFA Slot0/7 Link Status [DOWN]

<134>Jun 03 10:17:15 client CFA Slot0/7 Link Status [UP]
```

- The syslog message received at the server (as seen in the Logger) is as shown.

```
<25>,Jun 03 10:15:45,spoke1,076,5TH_AV,NYC,010,<134>Jun  3 10:17:11 client CFA Slot0/7 Link Status [DOWN],#/
<25>,Jun 03 10:15:50,spoke1,074,5TH_AV,NYC,010,<134>Jun  3 10:17:15 client CFA Slot0/7 Link Status [UP],#/
```



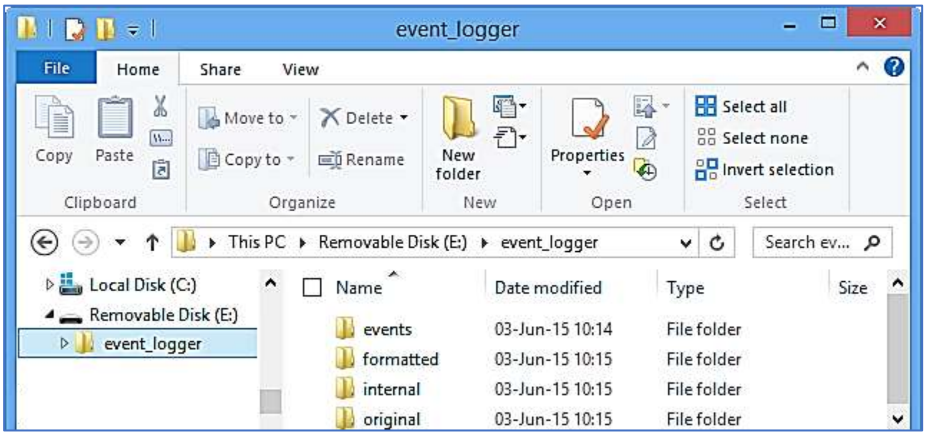
Date	Time	Priority	Hostname	Message
06-03-2015	10:17:38	Daemon.Alert	192.168.1.201	Jun 03 10:15:50,spoke1,074,5TH_AV,NYC,010,<134>Jun 3 10:17:15 client CFA Slot0/7 Link Status [UP],#/
06-03-2015	10:17:34	Daemon.Alert	192.168.1.201	Jun 03 10:15:45,spoke1,076,5TH_AV,NYC,010,<134>Jun 3 10:17:11 client CFA Slot0/7 Link Status [DOWN],#/

Figure 24 – Testing Event Logger Setup

- Verify that the logs are saved on the USB.

```
[/]event_logger show results file_names
MANAGEMENT EVENT LOGS:
Log.2015.6.3
ORIGINAL MESSAGES LOGS:
Log.2015.6.3
FORMATTED MESSAGES LOGS:
Log.2015.6.3
[/]
```

- Remove the USB and place in in your PC to view the files. A directory called event_logger will be present at the root directory of the USB drive.



Name	Date modified	Type	Size
events	03-Jun-15 10:14	File folder	
formatted	03-Jun-15 10:15	File folder	
internal	03-Jun-15 10:15	File folder	
original	03-Jun-15 10:15	File folder	

Figure 25 – Directory event_logger

The files can be opened with a text editor such as Notepad or Notepad ++.

IPSec

5.1 ISAKMP

Internet Security Association and Key Management Protocol (ISAKMP) “defines procedures and packet formats to establish, negotiate, modify and delete Security Associations (SA). A SA is a relationship between two or more entities that describes how the entities will utilize security services to communicate securely.

SAs contain all the information required for execution of various network security services, such as the IP layer services (such as header authentication and payload encapsulation), transport or application layer services, or self-protection of negotiation traffic. ISAKMP defines payloads for exchanging key generation and authentication data. These formats provide a consistent framework for transferring key and authentication data which is independent of the key generation technique, encryption algorithm and authentication mechanism.” RFC2408 [1].

Internet Key Exchange (IKE) negotiates the IPSec (Internet Protocol Security) SA (security associations). This process requires that the IPSec systems first authenticate themselves to each other and establish (IKE) shared keys.

Phase 2 is where SAs are negotiated on behalf of the VPN GRE services.

5.1.1 ISAKMP Phase 1 of Negotiation

During Phase 1, two ISAKMP VPN peers establish a secure, authenticated channel for communication. This is called ISAKMP SA or IKE Security Association.

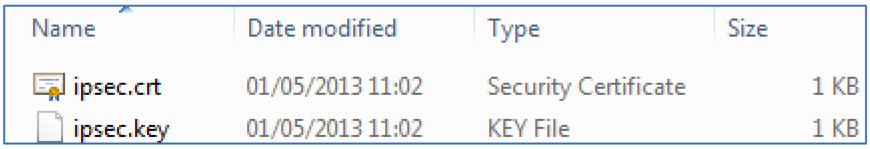
The authentication is supported with Pre-Shared Keys or Digital Signatures (X.509). This document section pertains to X.509 only. Please refer to S section for the rest of the functionality.

5.1.1.1 Authentication with RSA Signatures (X.509)

Digital signatures, such as the Rivest-Shamir-Adleman (RSA) signature, are public key based strong authentication mechanisms. X.509 uses an RSA signature.

A user is required to generate certificates from a trusted source and import them to the VPN parties (Hubs & Spokes). Two files are required, one is the certificate itself, and the other is the key. The files should have extensions of *.crt* and *.key.*

Below is a screenshot of two such files in a PC with TFTP client and a CLI example for importing them.



Name	Date modified	Type	Size
ipsec.crt	01/05/2013 11:02	Security Certificate	1 KB
ipsec.key	01/05/2013 11:02	KEY File	1 KB

Figure 26 – The Certificate Files

1. Import the key file.

```
iSG18GFP# rsa-signature import tftp://172.17.203.31/ipsec.key

 RSA signature file (ipsec.key) imported successfully
```

2. Import the certificate file.

```
iSG18GFP# rsa-signature import tftp://172.17.203.31/ipsec.crt
```

```
RSA signature file (ipsec.crt) imported successfully

Validate successful import
```

```
iSG18GFP# show rsA-signature list

ipsec.crt

ipsec.key
```

3. Activate the certificate.

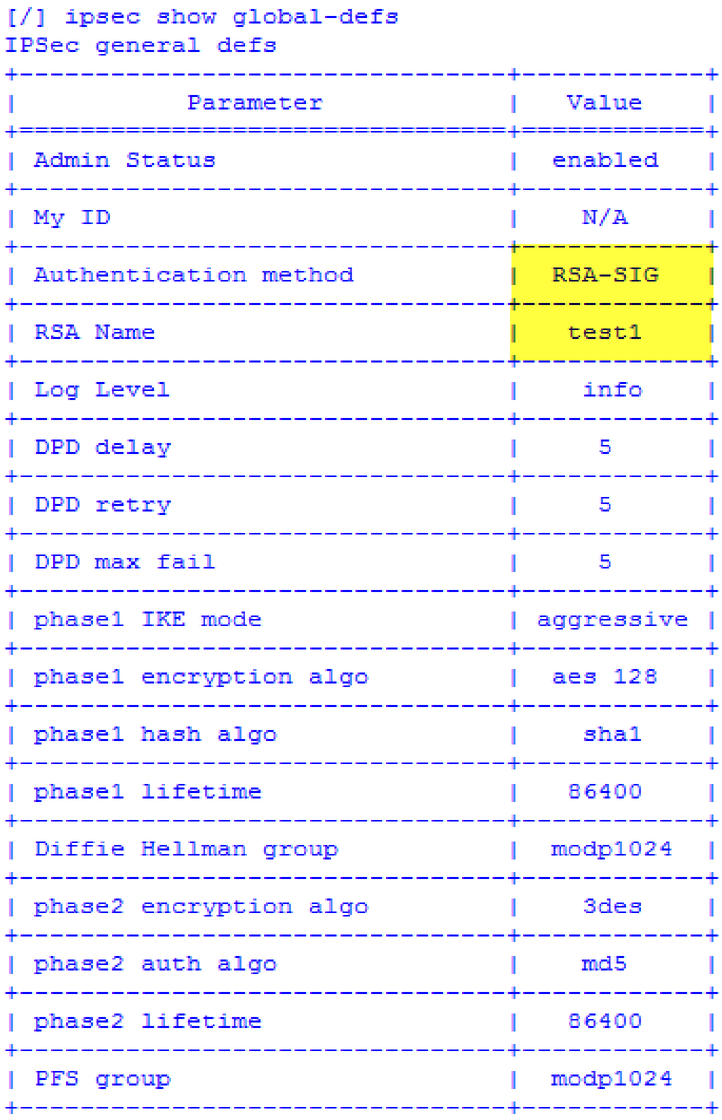
```
application connect

ipsec rsa-signature activate crt-file ipsec.crt key-file ipsec.key rsa-sig-name test_1
```

4. Update the ipsec isakmp to use the certificate instead of the PSK.

```
ipsec isakmp update authentication-method rsasig
```

The ipsec isakmp property "my id" is not of importance when using certificates as the authentication method.

The above configuration example will result in the following show output:



```
[/] ipsec show global-defs
IPSec general defs
+----------------------------------+------------+
|            Parameter             |   Value    |
+==================================+============+
| Admin Status                     |  enabled   |
+----------------------------------+------------+
| My ID                            |    N/A     |
+----------------------------------+------------+
| Authentication method            |  RSA-SIG   |
+----------------------------------+------------+
| RSA Name                         |   test1    |
+----------------------------------+------------+
| Log Level                        |    info    |
+----------------------------------+------------+
| DPD delay                        |     5      |
+----------------------------------+------------+
| DPD retry                        |     5      |
+----------------------------------+------------+
| DPD max fail                     |     5      |
+----------------------------------+------------+
| phase1 IKE mode                  | aggressive |
+----------------------------------+------------+
| phase1 encryption algo           |  aes 128   |
+----------------------------------+------------+
| phase1 hash algo                 |    sha1    |
+----------------------------------+------------+
| phase1 lifetime                  |   86400    |
+----------------------------------+------------+
| Diffie Hellman group             |  modp1024  |
+----------------------------------+------------+
| phase2 encryption algo           |    3des    |
+----------------------------------+------------+
| phase2 auth algo                 |    md5     |
+----------------------------------+------------+
| phase2 lifetime                  |   86400    |
+----------------------------------+------------+
| PFS group                        |  modp1024  |
+----------------------------------+------------+
```

5.1.1.2 IKE

ISAKMP ([MSST98]) provides a framework for authentication and key exchange but does not define them. ISAKMP is designed to be key exchange independent; that is, it is designed to support many different IKEs.

Oakley describes a series of key exchanges—called "modes"-- and details the services provided by each (e.g. perfect forward secrecy for keys, identity protection, and authentication). RFC 2409 [2]

5.1.1.3 Authenticated Key Exchange Modes

There are two basic methods used to establish an authenticated key exchange: Main Mode and Aggressive Mode. Each generates authenticated keying material from an ephemeral Diffie-Hellman exchange. Exchanges in IKE are not open ended and have a fixed number of messages. Receipts of a Certificate Request payload MUST NOT extend the number of messages transmitted or expected. Section 5 [2]

5.1.1.3.1 Main

The Main Mode is a highly secure option for ISAKMP Phase1 as it involves identity protection. The session flow is as follows:

- An IKE session begins with the initiator sending a proposal or proposals to the responder. The proposals define what encryption and authentication protocols are supported, the lifetime of the keys, and whether Phase 2 Perfect Forward Secrecy should be implemented. The proposal may contain several offerings. The responder chooses from the offerings and replies to the initiator.
- The next exchange passes Diffie-Hellman (D-H) public keys and ancillary data. All further negotiation is encrypted within the IKE SA.
- The third exchange authenticates the ISAKMP session. Once the IKE SA is established, IPSec negotiation (Quick Mode) begins.

For applications in which the IP addresses used for the VPN network are not static (e.g. a cellular spoke retrieving dynamic IP from the ISP over its PPP interface), the Main Mode of IKE is not applicable.

Pre-Shared Key

When used in Main Mode, the PSK should be in the form of IP address and use the VPN network addresses of the parties.

✎ In applications where the VPN is used over a cellular link, the IKE mode to be used is Aggressive.

5.1.1.3.2 Aggressive

In Aggressive Mode, the negotiation is quicker as the session is completed in only 3 messages (packets). The disadvantage is that the identity of the peers is not protected.

The first two messages negotiate policy, exchange Diffie-Hellman public values and ancillary data necessary for the exchange, and identities. In addition, the second message authenticates the responder. The third message authenticates the initiator and provides a proof of participation in the exchange. The flow is as follows:

- The initiator sends the proposal, key material and ID (all required SA data).
- The responder replies with authentication of the session and its ID.
- The initiator authenticates the session in the follow-up message.

Pre-Shared Key

When used in Aggressive Mode, the PSK may be either in the form of IP address or FQDN (Fully Qualified Domain Name). The PSK doesn't have to be an actual IP address of a VPN network interface as it considers the entered value as text (in the format of IP) and not as a valid IP address.

-->

✎ In applications where VPN is used over a cellular link, the IKE mode to be used is Aggressive. The PSK may be of IP format or FQDN.

.

5.1.1.4 Settings Structure

- Authentication method (PSK, X.509)
- Diffie–Hellman key exchange group (Oakley groups)
- IKE exchange mode
    - Main
    - Aggressive
- Encryption algorithm
    - Advanced Encryption Standard (AES)
        - 128 and 256 key size options
        - symmetric algorithm
    - Triple Data Encryption Algorithm (3DES)
        - It comprises of three DES keys, K1, K2 and K3, each of 56 bits
- Authentication HASH algorithms
        - Secure Hash Algorithm SHA-1 (160 bit)
        - Secure Hash Algorithm SHA-2 (256 |512 bit)
        - Message Digest (MD5) (128 bit)
- Life time and Dead Peer Discovery settings

5.1.2 ISAKMP Phase 2 of Negotiation

Phase 2 is where SAs are negotiated on behalf of services such as IPsec or any other service which needs key material and/or parameter negotiation. For iSG18GFP, at this phase, the negotiation of SA for secure VPN GRE (Generic Routing Encapsulation) data using IPSec is made.

5.1.2.1 Modes

The mode supported by IS5Com between end stations supporting IPSec (VPN parties) is transport mode (refer to the Settings Structure).

5.1.2.2 Perfect Forward Secrecy

The PFS is part of the key agreement session and has a purpose to ensure that a session key derived from a set of long-term public and private keys will not be compromised if one of the (long-term) private keys is compromised in future. The VPN (GRE, IPSEC) sessions can negotiate new keys for every communication and if a key is compromised then only the specific session it protected will be revealed.

The PFS uses the D-H groups as well but independently from Phase 1.

5.1.2.3 Settings Structure

- Supported mode
    - Transport (yes)
    - Tunnel (no)
- Authentications HASH algorithms
    - Secure Hash Algorithm SHA-1 (160 bit)
    - Secure Hash Algorithm SHA-2 (256 |512 bit)
    - Message Digest (MD5) (128 bit)
- Perfect Forward Secrecy type (PFS)
- Encryption algorithm
    - Advanced Encryption Standard (AES)
        - 128 and 256 key size options
        - Symmetric algorithm
    - Triple Data Encryption Algorithm (3DES)
        - Comprises of three DES keys, K1, K2 and K3, each of 56 bits
- Life time

- Soft – hard coded. At this threshold value, the IKE starts a new phase 2 exchange.
- Hard- SA which has exceeded this threshold value will be discarded.

5.2 IPSec Command Association

Below is the detailed configuration of the IPSec in their respective association to the ISAKMP structure. Highlighted in blue are the CLI names of the configurable fields.

Enable IPSec

{enable |disable}

Settings

Log level (log-level)

Dead Peer Discovery

delay (dpd-delay)

max failure (dpd-maxfail)

max retires (dpd-retry)

flush Security Association (flush-sa proto)

id-type (id-type)

soft timer (soft-lifetime)

Phase 1

Authentication method {pre_shared_key | rsasig}

Diffie-Hellman key exchange Group (dh-group)

Internet Key Exchange mode (ike-phase1-mode)

Encryption Algorithm (phase1-encryption-algo)

Hash Algorithm (phase1-hash-algo)

Life Time (phase1-lifetime)

Phase 2

Perfect Forward Secrecy (pfs-group)

Encryption Algorithm (phase2-encryption-algo)

Authentication Algorithm (phase2-auth-algo)

Life Time (phase2-lifetime)

IPSec Policy

Name (notes)

Source address (src-address-prefix)

Destination address (dst-address-prefix)

Source protocol port (src-port)

Destination protocol port (src-port)

Protocol (protocol)

Preshared Keys

Key : (key)

Own PSK id : (id)

Partner PSK id : (id)

Partner PSK id : (id)

Certificates X.509

Import crt file (flush-sa proto)

Import key file (rsA-signature import)

Activate certificate file (rsa-signature activate)

Certificate name (rsa-sig-name)

5.3 IPSec Commands Hierarchy

+ root

+ application connect

+ ipsec {enable | disable}

– flush-sa proto {ah | esp | ipsec | isakmp}

– rsa-signature activate {crt-file <file name> | key-file <file name> |rsa-sig-name <name>}

+ isakmp update

- authentication-method {pre_shared_key | rsasig}

- dh-group <none | modp768 | modp1024 | modp1536 | modp2048 | modp3072 |modp4096 | modp6144>

– pfs-group < none | modp768 | modp1024 | modp1536 | modp2048 | modp3072 |modp4096 | modp6144 |modp8192>

– dpd-delay <5,0-120> dpd-maxfail <5,2-20> dpd-retry <5,1-20>

– log-level <error |warning |notify |info |debug |debug2>

– my-id <>

– soft-lifetime <1-99>

– id-type {none| fqdn| asn1dn}

– ike-phase1-mode <*aggressive* |main> phase1-encryption-algo <3des | *aes-128* | aes-256> phase1-hash-algo <md5 |*sha1* |sha256 |sha512>

– phase2-auth-algo < hmac_md5 | hmac_sha1 | hmac_sha256 | hmac_sha512> phase2-encryption-algo <3des |aes-128 |aes-256>

- phase1-lifetime <86400,(180-946080000)> phase2-lifetime <86400,(180-946080000)>

– rsa-sig-name <name> rsa-ca-cert <name.crt>

+ policy {create | remove | show} mode (transport,<transport| tunnel>

- ➢ For both transport and tunnel modes
  {src-address-prefix <A.B.C.D/E>} {dst-address-prefix < A.B.C.D/E >}
  [src-port <>] [dst-port <> [notes <text>]
  [protocol (any,<gre |tcp |udp| any| icmp| ipencap| modbus_tcp|iec104|dnp3>)]

- ➢ For tunnel mode

{endpoint-dst-address < A.B.C.D >} [endpoint-dst-port <0-999,999>]

[endpoint-src-address < A.B.C.D >] [endpoint-src-port <0-999,999>]

+ preshared {create | remove} key <> id <>

+ show

- log {grep| num-of-lines }

- global-defs

- policy

- preshared

- rsa-signature-file

- sa [proto {ah | esp | ipsec | isakmp}]

5.4 IPSec X.509 Commands Hierarchy

```
+ root

-rsA-signature import {flash:<file name> | sftp://<user:password@<ip>/<file_name> |
tftp://<ip>/<file_name> }

- show rsA-signature list

+ application connect

+ certificates

        + local

    - export {certificate-file-pem <text>}{name <text>}{tftp-address <A.B.C.D>}

    - import {certificate-file-pem <text>}{name <text>} [comment <text>]{tftp-address
<A.B.C.D>}[private-key-pem <string>]

    -generate {scep-url <url>} [scep-password-string <string>] {name <text>} {common-name
<text>} {country(region) <text>} [state(province) <text>] [locality(city) <text>] [organization
<text>] [e-mail <email address>] [organization-unit <text>] [key-size (2048,<1024|
1536| 2048>)]

[auto-regenerate-days (0,<0-14>)]
[auto-regenerate-days-warning (0,<0-14>)]
[comments <text>]
[enrollment-method (online-scep,<file-based| online-scep>)]

- remove name <text>

- show [name <text>]

- update {name <text>} {[auto-regenerate-days (0,<0-14>)]
[auto-regenerate-days-warning (0,<0-14>)] [comments <text>]}

+ ca

- export {certificate-file-pem <text>} {name <text>} {tftp-address <A.B.C.D>}

- import {import-method file-base}{certificate-file-pem <text>}
{name <text>} {tftp-address <text>} [comment <text>]

- import {import-method online-scep}
{name <text>} {http-url <url>} [comment <comments>]
[auto-update-days (0,<0-14>)] [auto-update-days-warning (0,<0-14>)]

- remove name <text>

- show [name <text>]

- update name <text> {[auto-update-days (0,<0-14>)] [auto-update-days-warning (0,<0-14>)]
[comments <text>]}
```

```
        + crl

- export certificate-file-pem <text> {name <text>}
          {tftp-address <A.B.C.D>}

- import {import-method file-based} {certificate-file-pem <>}
{ca-name <text>} {name <text>} [comment <comments>]
{tftp-address <A.B.C.D>}

-   import {import-method online-http}
{ca-name <text>} {name <text>} [comment <comments>] {http-url <url>}   [update-interval-sec
(0,<0-60480>)]

- remove name <text>

- show [name <text>]

- update name <text> {[update-interval-sec (0,<0-60480>)]
[comments <text>]}
```

5.5 IPsec Commands

Table 6 – IpSec Commands Description

Command	Description
application connect	Enter the industrial application menu.
certificates	Show the files available.
local	
export	This option is not supported in the current release.
import	• **certificate-file-pem:** the certificate name and extension at the server. • **name:** name for the certificate with which it will be saved locally in the unit. Mandatory field. • **tftp-address:** IPv4 address of the server holding the certificate. • **comment:** optional descriptive test. • **private-key-pem:** server key.
generate	• **Name:** use a unique name to identify the certificate request. Alpha numeric, special characters supported except the sign !. mandatory field. • **Comments:** optional descriptive test. No spaces allowed. • **Common-name:** add a common name typically used to identify the host. • **Country (region):** the country where the unit is installed. • **State(province):** the state where the unit is installed. • **Locality(city):** the city where the unit is installed. • **Organization:** formal name of the company you are working at. • **Email:** your email address. • **organization-unit:** name of the department you work at. • **auto-regenerate-days:** 0-14. Applicable in 'enrollment-method' of 'online-scep' only. Send regenerate request x days prior to the certificate expiration date. default=0 (no automatic request). • **auto-regenerate-days-warning:** 0-14. Applicable in 'enrollment-method' of 'online-scep' only. Send a warning x day prior to the certificate expiration date. default=0 (no automatic message). • **scep-url:** url address of SCEP server. For example, http://iS5Com.com

Command	Description
	• **scep-password-string:** authentication password at server. • **key-size:** 1024| 1536| 2048. Default 2048. Large key size enhances security but is slower to generate. • **enrollment-method:** file-based| online-scep. Default online-scep. 'field based' is not supported at this version.
remove	• **name:** the name of the certificate with which it was saved when generated/ imported.
show	• **name:** the name of the certificate with which it was generated/ imported.
update	• **name:** the name of the certificate with which it was generated/ imported • **comment:** option descriptive test. • **auto-regenerate-days:** 0-14. Applicable in 'enrollment-method' of 'online-scep' only. Send regenerate request x days prior to the certificate expiration date. default=0 (no automatic request). • **auto-regenerate-days-warning:** 0-14. Applicable in 'enrollment-method' of 'online-scep' only. Send a warning x days prior to the certificate expiration date. default=0 (no automatic message).
ca	
export	• **certificate-file-pem:** export the file to the server. Applicable when using 'file based' only. This option is not supported in the current version. • **name:** the name of the certificate with which it was saved when generated/ imported. • **tftp-address:** IPv4 address of the target server.
import	• **certificate-file-pem:** the certificate name and extension at the server. Applicable when using 'file based' only. • **name:** name for the certificate with which it will be saved locally at the unit. Mandatory field. • **tftp-address:** IPv4 address of the server holding the certificate. • **comment:** • **http-url:** URL address of SCEP server. • **import-method:** ad-hoc operation using 'file based' (TFTP) or automatically with SCEP protocol using 'online-scep' option. • **auto-update-days:** 0-14. Applicable in 'enrollment-method' of 'online-scep' only. Send update request x days prior to the

Command	Description

	certificate expiration date.
	default=0 (no automatic request).
	- **auto-update-days-warning**: 0-14. Applicable in 'enrollment-method' of 'online-scep' only. Send a warning x days prior to the certificate expiration date.
	default=0 (no automatic message).

remove	- **name**: the name of the certificate with which it was saved when generated/ imported.
show	- **name**: the name of the certificate with which it was saved when generated/ imported.
update	- **name**: the name of the certificate with which it was saved when generated/ imported. - **comment**: optional descriptive test. - **auto-update-days**: 0-14. Applicable in 'enrollment-method' of 'online-scep' only. Send update request x days prior to the certificate expiration date. default=0 (no automatic request). - **auto-update-days-warning**: 0-14. Applicable in 'enrollment-method' of 'online-scep' only. Send a warning x day prior to the certificate expiration date. default=0 (no automatic message).
crl	
export	This option is not supported in the current release.
import	- **certificate-file-pem**: the certificate name and extension at the server. - **name**: name for the certificate with which it will be saved locally at the unit. Mandatory field. - **tftp-address**: IPv4 address of the server holding the certificate. - **comment**: optional descriptive test. - **ca-name**: - **http-url**: URL address of the server managing the automatic crl updates. - **import-method**: ad-hoc operation using 'file based' (TFTP) or automatically with SCEP protocol using 'online-scep' option. - **update-interval-sec**: time interval for the unit to check for an updated crl.
remove	- **name**: the name of the certificate with which it was saved when generated/ imported.
show	- **name**: the name of the certificate with which it was saved when generated/ imported.
update	- **name**: the name of the certificate with which it was saved when generated/ imported. - **comment**: optional descriptive test.

Command	**Description**
	• **update-interval-sec**: time interval for the unit to check for an updated crl.
rsA-signature import	• Import the X.509 certificate file and key file to the application from a connected USB drive or tftp /sftp servers. These files are mandatory for IPSec to encrypt using X.509 certificates. • These files are not required if IPSec is used with pre-shared keys.
show rsA-signature list	• Show the files available.
Application connect	• Enter the industrial application menu.
IPsec	• Enter the IPsec configuration mode.
Enable | disable	• Default is disable.
rsa-signature activate	• Activation of the available certificate and key files. • **Crt-file**: name of the certificate file. • **Key-file**: name of the key file. • **rsa-sig-name**: user configurable name for the signature.
isakmp update	
authentication-method	• **pre_shared_key**: pre-shared keys will be used. (default) • **Rsasig**: X.509 certificates will be used.
dh-group	• Diffie-Hellman key exchange Group. Relates to phase 1. • determines the strength of the key used in the key exchange process. The higher the group number, the stronger the key and security increases. • Options: ▪ none ▪ modp768 (DH group 1) ▪ modp1024 (default) (DH group 2) ▪ modp1536 (DH group 3 and 5) ▪ modp2048 (DH group 14) ▪ modp3072 (DH group 15) ▪ modp4096 (DH group 16) ▪ modp6144 (DH group 17) ▪ modp8192 (DH group 18)
pfs-group	• Perfect Forward Secrecy type. Relates to phase 2. • determines the strength of the key used in the key exchange process. The higher the group number, the stronger the key and security increases. • Options:

Command	Description
	▪ none ▪ modp768 ▪ modp1024 (default) ▪ modp1536 ▪ modp2048 ▪ modp3072 ▪ modp4096 ▪ modp6144 ▪ modp8192
dpd-delay	• Dead Peer Discovery delay. defines the interval between following keep alive messages. Permissible range: 0-120 • (default is 5)
dpd-maxfail	• Dead Peer Discovery max attempts to determine failure. Permissible range :2-20 (default is 5)
dpd-retry	• Dead Peer Discovery max retry attempts. A retry is initiated after a failure at “dpd-maxfail”. • Permissible range: 1-20 • (default is 5)
log-level	Syslog warnings levels to be logged. • error • Warning • notify • info (default) • debug • debug2
my-id	• Own pre-shared id. • Dependent on “id-type” set, my-id can be in either domain name format or ipv4 format. • If “id-type” is set to “none”:No need to set value in “my-id” as it will automatically use a valid IP address. • If “id-type” is set to “FQDN”:“my-id” should be set with a domain name format. For example:* Spoke.iS5Com.com
Id-type	• Set the type of form used for the IPSec local id. • **None**: the units own pre-shared id will be the default ip interface. • **Address**: this option is not supported in current version. • **fqdn**: the units own pre-shared id will be in a domain name format. For example, spoke.iS5Com.com

Command	Description
	default: none
ike-phase1-mode	Internet Key Exchange mode type use for Phase 1. Aggressive (default) main
phase1-encryption-algo	Encryption Algorithm used for phase 1. 3des aes-128 (default) aes-256
phase1-hash-algo	Hash Algorithm used for phase 1. md5 sha1 (default) sha256 sha512
phase1-lifetime	The lifetime of the key generated between the stations. 180-946080000 sec. Default is 86400.
phase2-auth-algo	Authentication Algorithm for phase 2. hmac_md5 (default) hmac_sha1 hmac_sha256 hmac_sha512
phase2-encryption-algo	Encryption Algorithm for phase 2. 3des (default) aes-128 aes-256
Phase2-lifetime	The lifetime of the key generated between the stations. 180-946080000 sec. Default is 86400
soft-lifetime	When a dynamic IPSec SA is created, two types of lifetimes are used: hard and soft. The hard lifetime specifies the lifetime of the SA. The soft lifetime, which is derived from the hard lifetime, informs the IPSec key management system that the SA is about to expire. This allows the key management system to negotiate a new SA before the hard lifetime expires. Permissible values are 1-99 and represents percentage. soft lifetime = <1-99>*hard lifetime /100
rsa-sig-name	The name set by the user for the signature.

Command	Description
Policy create	Configure the policy to determine the type of traffic to encrypt. • **mode**: choose mode of operation ▪ transport- this is the default mode. Supported for route based VPNs. ▪ tunnel- policy based vpn. Supported only for IPSec VPN. • **src-ip**: A.B.C.D/x format. The ACE IP interface which is the local end of the tunnel. • **dst-ip**: A.B.C.D/x format. The IP interface which is the remote end of the tunnel. • **src-port**: source port number at the packet originated from the 'src-ip'. • **dst-port**: destination port number at the packet originated from the 'src-ip'. • **protocol**: the type of protocol to encrypt. For example any, TCP,UDP,GRE, icmp, ipencap. Default- 'any'. When using IPSec VPN, the use of 'ipencap' is mandatory at the policy. • **endpoint-dst-address**: applicable in IPSEC VPN at 'policy based' mode only. A.B.C.D IPv4 format. Encryption will be made for packets which are sent with this destination IP address. • **endpoint-src-address**: applicable in IPSEC VPN at 'policy based' mode only. A.B.C.D IPv4 format. Encryption will be made for packets which are sent with this source IP address. • **endpoint-dst-port**: applicable in IPSEC VPN at 'policy based' mode only. Numeriv value <0-999,999>. Encryption will be made for packets which are sent with this destination port number. • **endpoint-src-port**: applicable in IPSEC VPN at 'policy based' mode only. Numeric value <0-999,999>. Encryption will be made for packets which are sent with this source port number.
Preshared {create | remove}	• Configuration of pre shared identifiers for local node and all remote IPsec nodes. • **ID**: unique identifier for the IPSec participant node Can be in either domain name format or ipv4 format.) • **Key**: pre-shared key which should be common for all nodes participating. text, numerical or combination string.

Command	Description
	• **notes:** name of the policy.
Show	Show IPsec.

5.5.1 IPSec defaults

```
/] ipsec show global-defs
PSec general defs
--------------------------------+----------------
           Parameter            |     Value
================================+================
 Admin Status                   |    disabled
--------------------------------+----------------
 ID Type                        |      none
--------------------------------+----------------
 My ID                          |      N/A
--------------------------------+----------------
 Authentication method          | pre_shared_key
--------------------------------+----------------
 RSA Name                       |      N/A
--------------------------------+----------------
 Log Level                      |      info
--------------------------------+----------------
 DPD delay                      |       5
--------------------------------+----------------
 DPD retry                      |       5
--------------------------------+----------------
 DPD max fail                   |       5
--------------------------------+----------------
 phase1 IKE mode                |   aggressive
--------------------------------+----------------
 phase1 encryption algo         |     aes128
--------------------------------+----------------
 phase1 hash algo               |      sha1
--------------------------------+----------------
 phase1 lifetime                |     86400
--------------------------------+----------------
 Diffie Hellman group           |    modp1024
--------------------------------+----------------
 phase2 encryption algo         |      3des
--------------------------------+----------------
 phase2 auth algo               |    hmac_md5
--------------------------------+----------------
 phase2 lifetime                |     86400
--------------------------------+----------------
 PFS group                      |    modp1024
--------------------------------+----------------
```

Application Aware Firewall

The integrated SCADA protocol Deep Packet Inspection (DPI) firewall provides network-based distributed security. The implemented firewall is "application-aware," meaning it inspects the contents of the data packets of selected SCADA protocols according to the rules set by the user. Using the DPI firewall, the secure gateway becomes distributed Intrusion Prevention System (IPS) and implements detailed service-aware inspection.

The following SCADA protocols are supported:

- IP protocols: Modbus TCP, IEC 104, DNP3, S7
- Serial protocols: Modbus RTU, IEC 101, DNP3 RTU

The firewall checks each packet in detail:

- **Protocol validity**: The firewall checks whether the packet structure and its control fields comply with the standard and whether the session flow follows the expected logic (i.e. session initiated by master, response matches request, session setup sequence, etc.).
- **Application logic**: For every pair of source and destination devices, the firewall verifies that only the allowed communication is performed by checking the function code and the command parameters according to the operator defined values.

6.1 Supported Hardware

The hardware having the part number SE support the firewall capability with no further licensing required.

6.2 IP Firewall Service flow

For a protocol flow to be inspected by the firewall, the following is achieved by the IS5Com's iDMS.

- Access Control Lists (ACL)s are placed on the relevant ports to redirect the traffic flow to the application firewall port Gigabit Ethernet 0/4 (internal port). The ACLs will allow traffic between predefined members only. ACLs will permit traffic only of the TCP/UDP type correlating to the predefined protocol determined by the user. Other ports should be blocked (by using the block non-explicit traffic function in the firewall).

- The ACLs validate the packet direction and drop them in violation of a proper session.

- A file holding a list of allowed messages is created upon user configuration and is downloaded to the secure gateway. The file holds specific addressing properties of the target devices under the relevant SCADA protocol (for example, Common Address of ASDU in IEC104). The packet inspection is done not only by the 5-tuple (IP address/port number, destination IP address/port number and the protocol in use) but as well in the payload itself (DPI).

- Service packets will be inspected towards this file.

- A packet originated and designated to a service member will be directed to the firewall for in depth inspection of the payload before allowed to pass to the network.

6.3 Firewall Flow Illustration

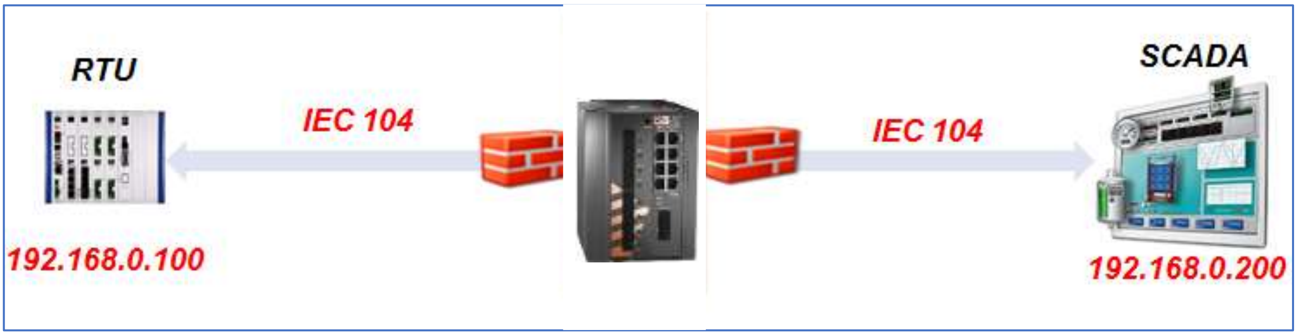
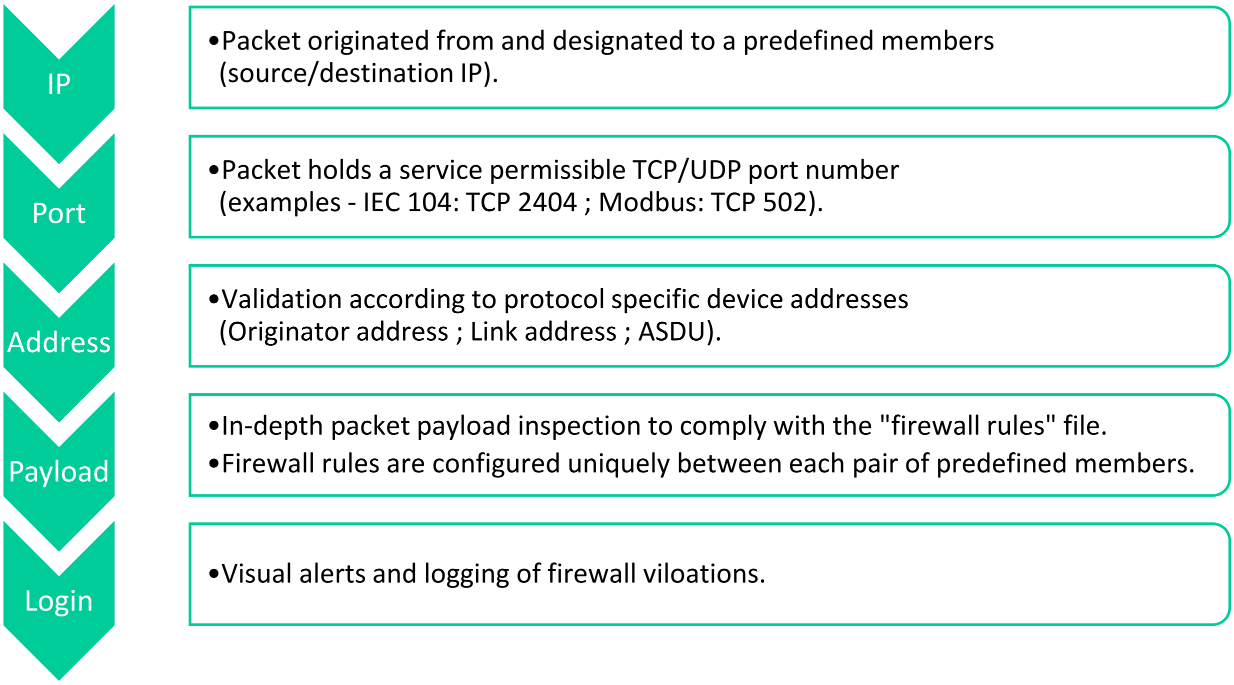


Figure 27 – Firewall Flow Illustration



- Packet originated from and designated to a predefined members (source/destination IP).
- Packet holds a service permissible TCP/UDP port number (examples - IEC 104: TCP 2404 ; Modbus: TCP 502).
- Validation according to protocol specific device addresses (Originator address ; Link address ; ASDU).
- In-depth packet payload inspection to comply with the "firewall rules" file.
- Firewall rules are configured uniquely between each pair of predefined members.
- Visual alerts and logging of firewall viloations.

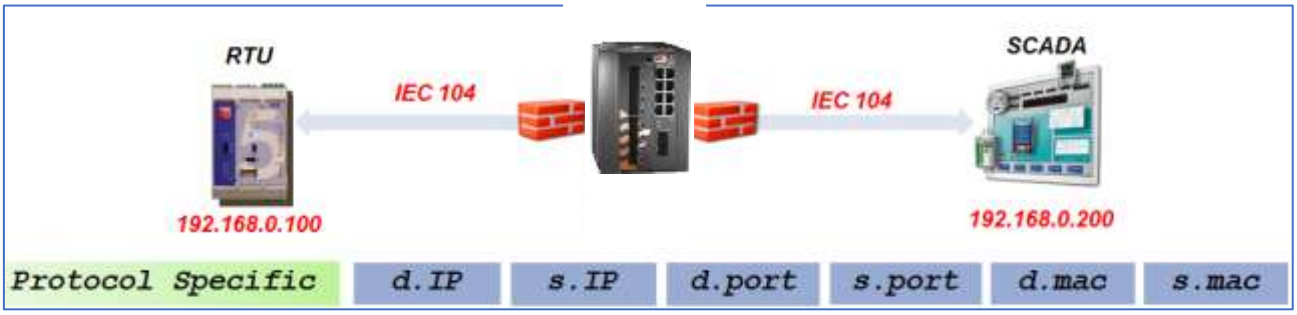


Figure 28 – Firewall Flow Illustration – Protocol Specific

6.4 Configuration

Firewall end-to-end service and provisioning is supported using iDMS only.

Configuration set up in the system using iDMS should not be tampered with by the user by accessing via CLI.

Go to **iDMS** main screen, click **Configuration** menu and choose **Firewall…**

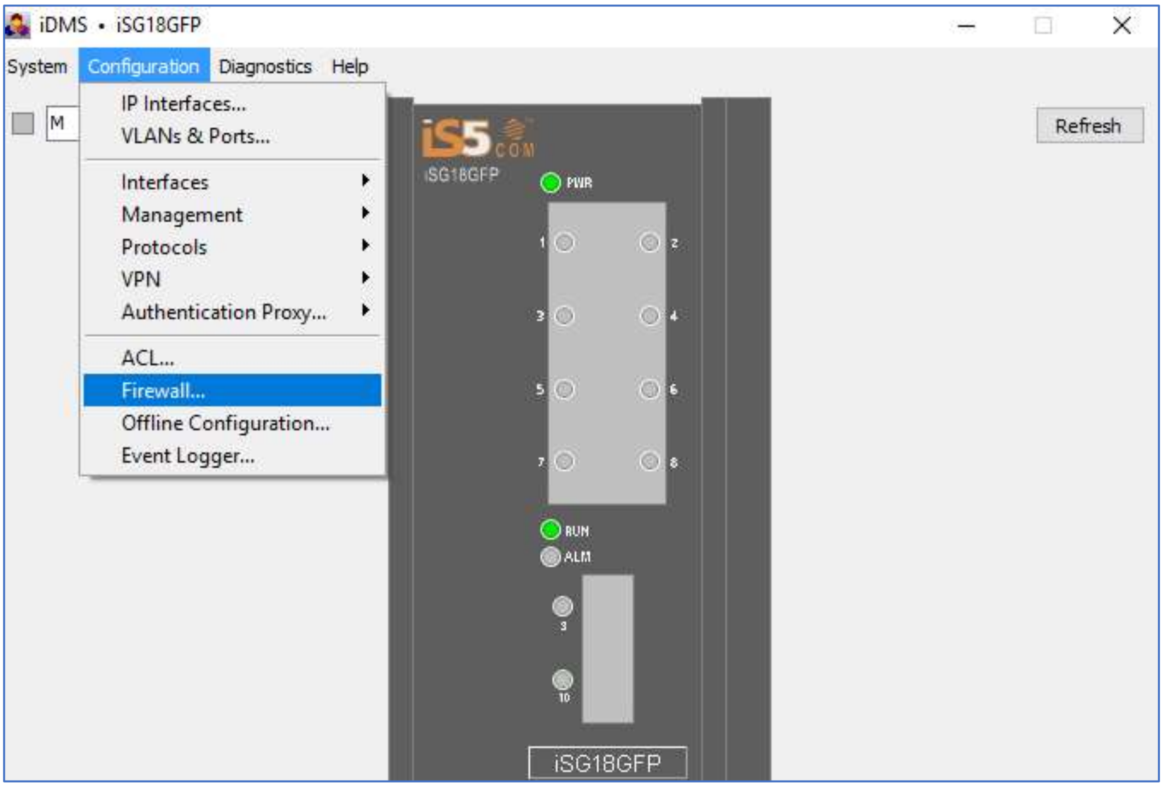
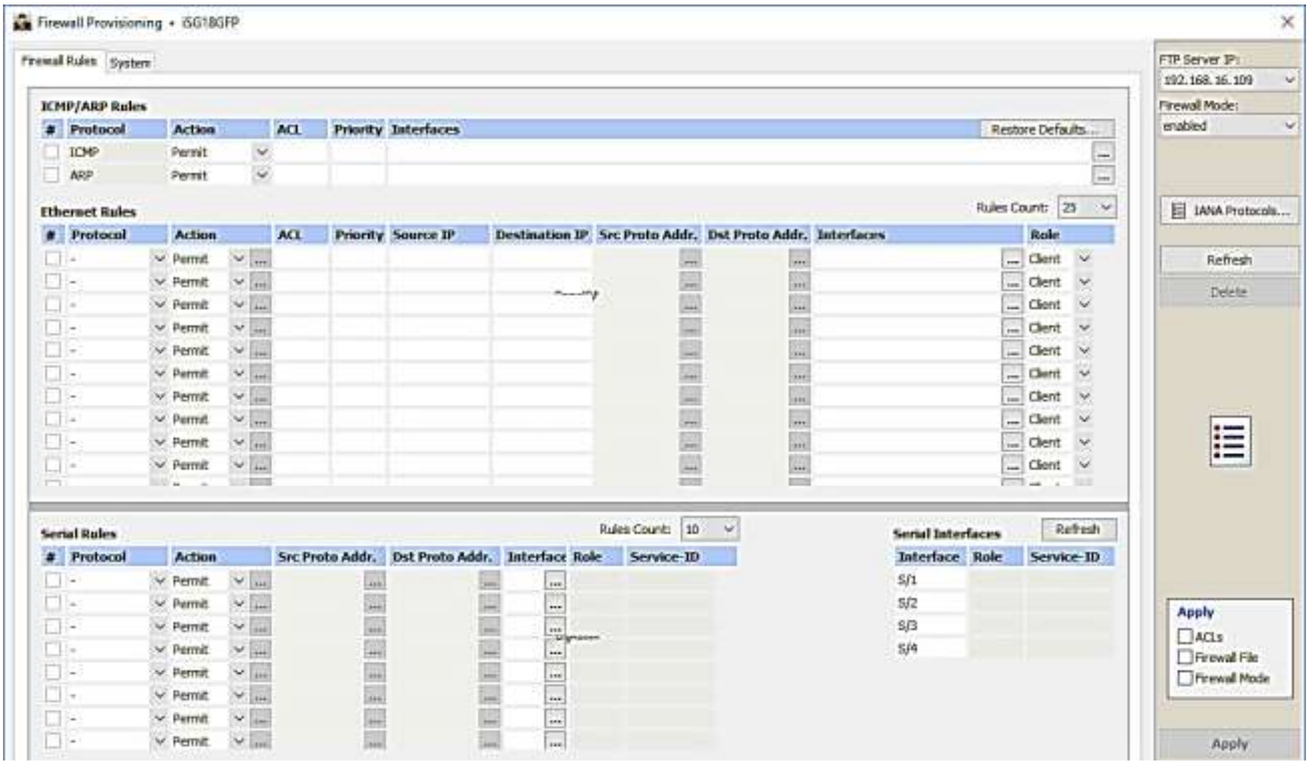


Figure 29 – Configuration of Firewall Interface

The Firewall Provisioning screen appears.



ICMP/ARP Rules

#	Protocol	Action	ACL	Priority	Interfaces
□	ICMP	Permit			
□	ARP	Permit			

Ethernet Rules

Rules Count: 25

#	Protocol	Action	ACL	Priority	Source IP	Destination IP	Src Proto Addr.	Dst Proto Addr.	Interfaces	Role
□	-	Permit								Client
□	-	Permit								Client
□	-	Permit								Client
□	-	Permit								Client
□	-	Permit								Client
□	-	Permit								Client
□	-	Permit								Client
□	-	Permit								Client
□	-	Permit								Client
□	-	Permit								Client

Serial Rules

Rules Count: 10

#	Protocol	Action	Src Proto Addr.	Dst Proto Addr.	Interface	Role	Service-ID
□	-	Permit					
□	-	Permit					
□	-	Permit					
□	-	Permit					
□	-	Permit					
□	-	Permit					
□	-	Permit					
□	-	Permit					

Serial Interfaces

Interface	Role	Service-ID
S/1		
S/2		
S/3		
S/4		

FTP Server IP: 192.168.16.109

Firewall Mode: enabled

Apply
□ ACLs
□ Firewall File
□ Firewall Mode

Figure 30 – Firewall Interface

The **Firewall Provisioning** screen is divided into the following sections:

1) **FTP server IP address**—the iDMS runs an internal FTP server and its address is the local IP address of the computer that runs it. The secured gateway has an internal FTP client, in which all firewall rules are uploaded from the FTP server. This section allows the user to select FTP server address (if the computer has more than one local IP address) that will be able to upload the firewall rules into the secured gateway.

2) **Firewall Mode** (firewall functionality in the secured gateway):

- Enabled firewall works according to its rules (if specific data packets are not allowed according to the firewall rule, it will be dropped and all data packets that are allowed will be passed).
- Disabled firewall doesn't work according to its rules (all data traffic is allowed, even if firewall rules exist).
- Simulate — the firewall will allow all data traffic, but it will notify the user through Syslog and firewall logs that a specific data packet/s that was supposed to be dropped (if the firewall was enabled) passed. This mode shows the user if the firewall rules are configured correctly.

3) **Rules Count** —allows the firewall rules as indicated in the dropdown selection box.

4) **Internet Assigned Numbers Authority (IANA)** protocols—it shows all well-known protocols and allows adding and modifying generic or custom-built protocols. The custom-built protocols can be later added to the firewall rules. It is also possible to modify the well-known protocol ports, if needed.

5) **Refresh and delete** section—it shows all uploaded firewall rules and enables deleting some or all the firewall rules.

6) **Apply** section—it allows applying either or both GCE ACLs and ACE firewall rules (Firewall File) to the secured gateway or changing the firewall mode.

7) **Tabs** section—it shows FTP server logs, system logs, and firewall rules and enables blocking non-explicit traffic of specific or most of the secured gateway physical ports.

8) **Firewall rules** main section—it allows permitting/denying firewall rules in the secured gateway.
✎ With SCADA protocols, a detailed firewall rules are shown.

9) **IP connectivity** section—it allows permitting/denying the secured gateway to establish firewall IP connectivity using ICMP (Internet Control Message Protocol) and ARP (Address Resolution Protocol); these permissions run over GCE ACLs.

ICMP is used by network devices, including routers, to send error messages and operational information indicating, for example, that a requested service is not available or that a host or router could not be reached. ARP finds the hardware address, also known as Media Access Control (MAC) address, of a host from its known IP address. ARP maintains a cache (table) in which MAC addresses are mapped to IP addresses.

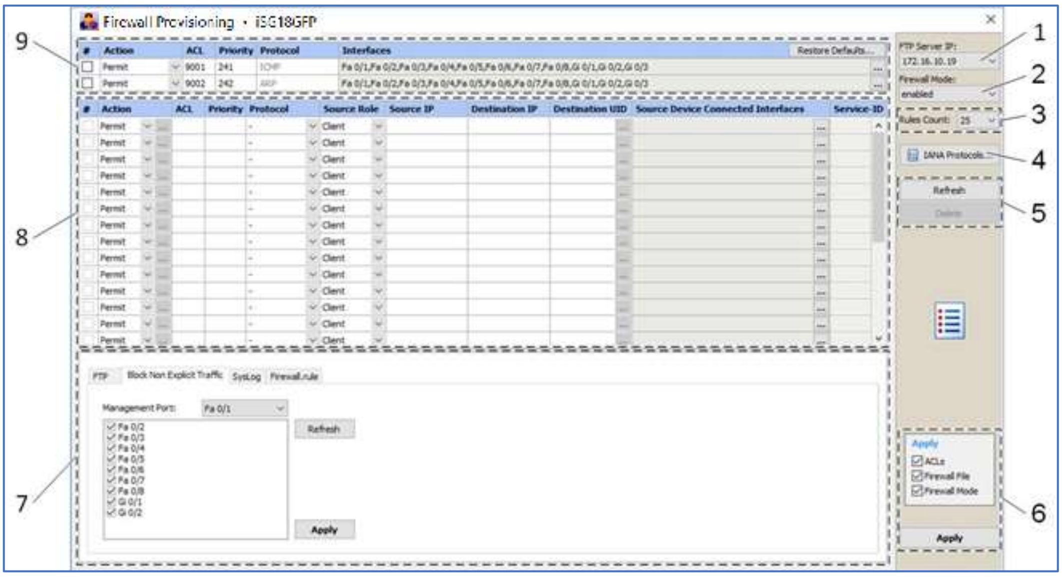
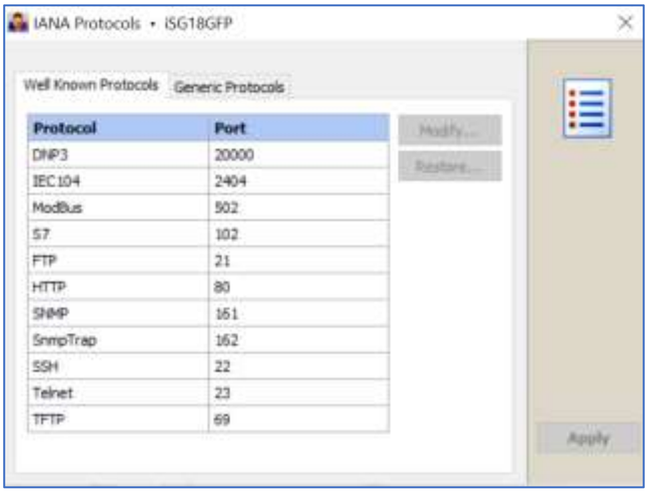


Figure 31 – Firewall Provisioning Areas

6.4.1 IANA Protocols Detailed Description

Go to **Firewall main** screen and select **IANA Protocols…** All well-known protocols and their default ports are shown under **Well Known Protocols** tab.

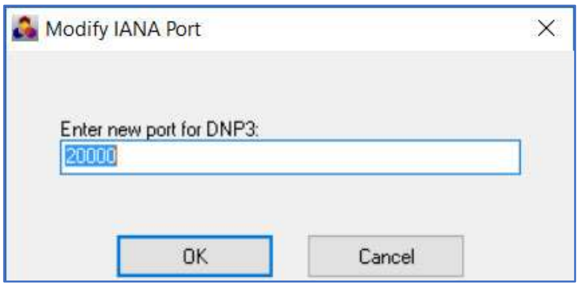
6.4.1.1 Well Known Protocols



Protocol	Port
DNP3	20000
IEC104	2404
ModBus	502
S7	102
FTP	21
HTTP	80
SNMP	161
SnmpTrap	162
SSH	22
Telnet	23
TFTP	69

Figure 32 – Well Known Protocols

1. If modifying a well-known protocol's default port, select the well-known protocol, and click **Modify… Modify IANA Port** screen opens.

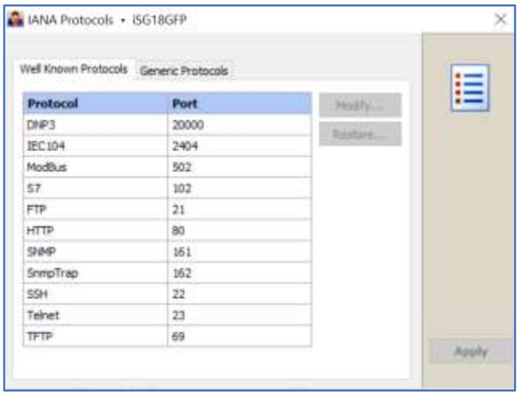


Enter new port for DNP3: 20000

Figure 33 – Modify IANA Port

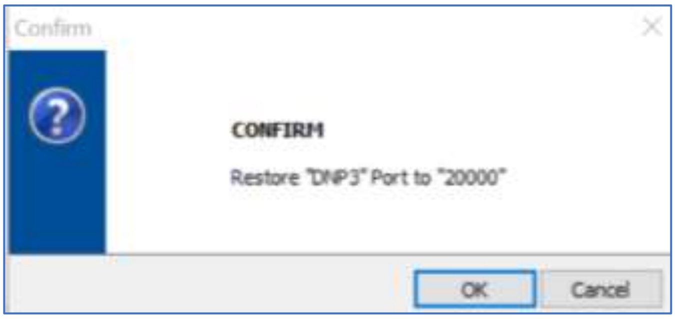
2. Enter the new port number for the well-known protocol and click **OK**.

3. If well-known protocol modified port restoration is needed, select the specific well-known protocol, and click **Restore…** The **Confirm** screen appears.



Protocol	Port
DNP3	20000
IEC104	2404
ModBus	502
S7	102
FTP	21
HTTP	80
SNMP	161
SnmpTrap	162
SSH	22
Telnet	23
TFTP	69

Figure 34 – The IANA Protocols Screen



CONFIRM

Restore "DNP3" Port to "20000"

Figure 35 – The Confirmation Screen

4. Click **OK** to restore the well-known protocol port.

6.4.1.2 Generic Protocols

1. If a generic protocol is needed, select **Generic Protocols** tab. All generic protocols are shown under **Generic Protocols** tab.

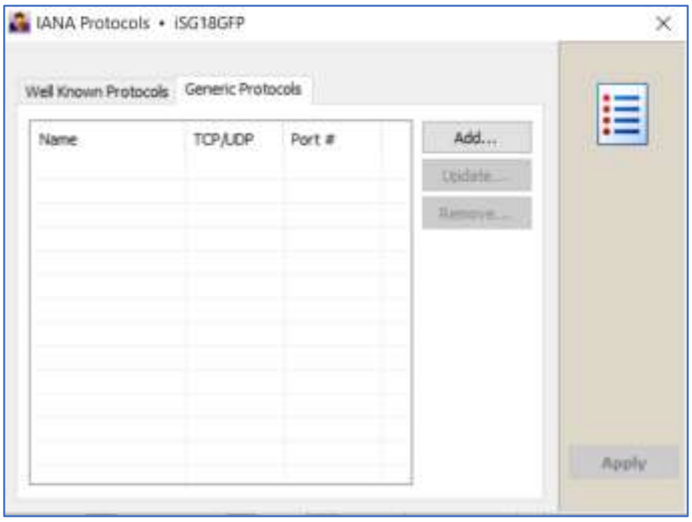
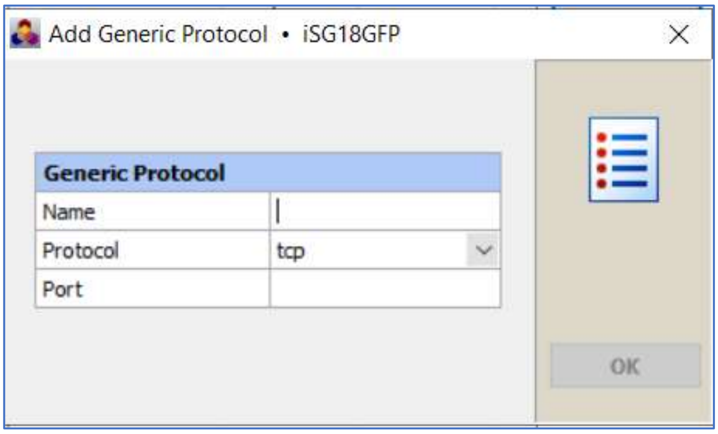


Figure 36 – Generic Protocols Screen

2. To add a generic protocol, click **Add…** The **Add Generic Protocol** window opens.

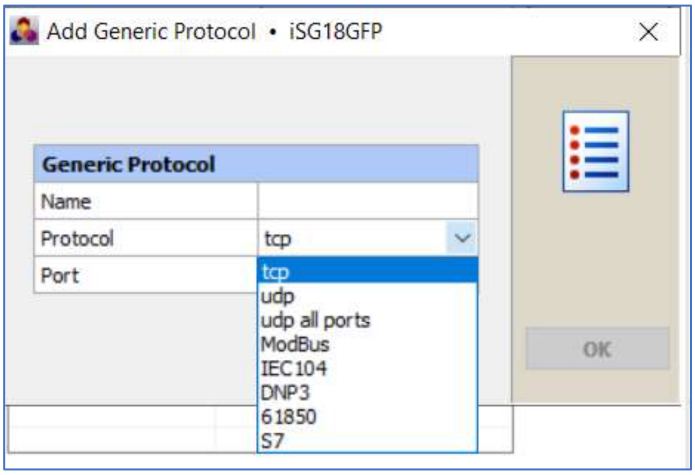


Add Generic Protocol • iSG18GFP

Generic Protocol	
Name	
Protocol	tcp
Port	

Figure 37 – Add Generic Protocol

3. Write the name of your generic protocol in Name field.
4. Select transportation protocol (**TCP/UDP/UDP all ports/ModBus/IEC104/DNP3/S7**) by selecting it from the drop-down box.



Add Generic Protocol • iSG18GFP

Generic Protocol	
Name	
Protocol	tcp
Port	

Figure 38 – Add Generic Protocol Screen Drop-Down Box Options

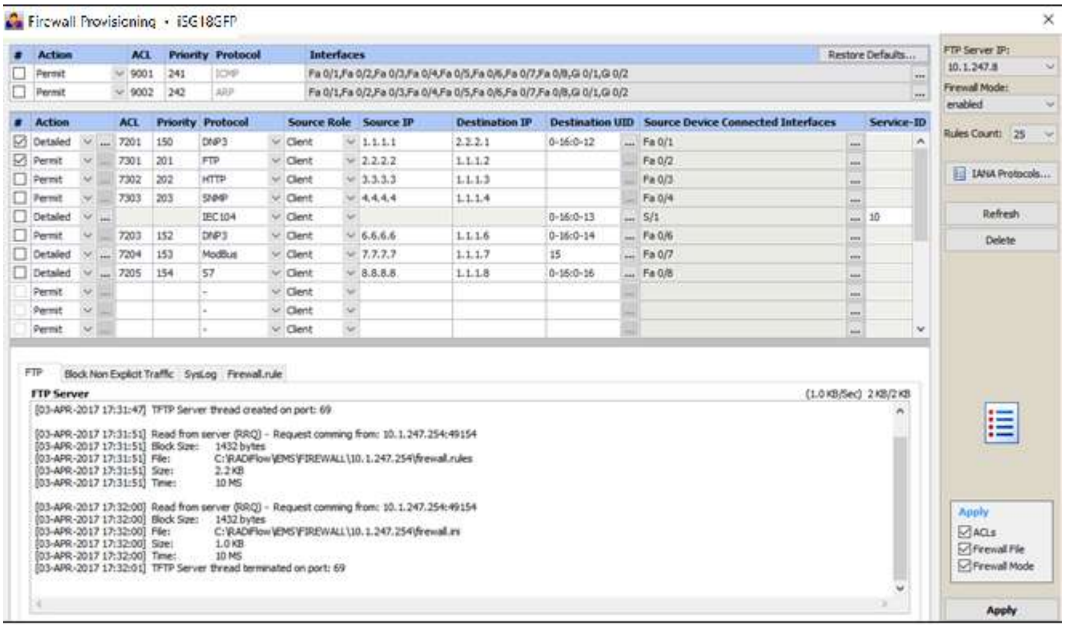
When selecting UDP for all ports, the **Port** field will be disabled.

5. Write the dedicated port number you want to assign in Port field.
6. Click **OK**.

The just added generic protocol will be available to be selected from the drop-down box in the Firewall Rules main section.

6.4.2 FTP tab

Go to **Firewall Provisioning** screen and select **FTP**. In the **FTP**, all FTP server logs will be shown.



#	Action	ACL	Priority	Protocol	Interfaces
□	Permit	9001	241	ICMP	Fa 0/1,Fa 0/2,Fa 0/3,Fa 0/4,Fa 0/5,Fa 0/6,Fa 0/7,Fa 0/8,Gi 0/1,Gi 0/2
□	Permit	9002	242	ARP	Fa 0/1,Fa 0/2,Fa 0/3,Fa 0/4,Fa 0/5,Fa 0/6,Fa 0/7,Fa 0/8,Gi 0/1,Gi 0/2

#	Action	ACL	Priority	Protocol	Source Role	Source IP	Destination IP	Destination UID	Source Device Connected Interfaces	Service-ID
☑	Detailed	7201	150	DNP3	Client	1.1.1.1	2.2.2.1	0-16:0-12	Fa 0/1	
☑	Permit	7301	201	FTP	Client	2.2.2.2	1.1.1.2		Fa 0/2	
□	Permit	7302	202	HTTP	Client	3.3.3.3	1.1.1.3		Fa 0/3	
□	Permit	7303	203	SNMP	Client	4.4.4.4	1.1.1.4		Fa 0/4	
□	Detailed			IEC104	Client			0-16:0-13	S/1	10
□	Permit	7203	152	DNP3	Client	6.6.6.6	1.1.1.6	0-16:0-14	Fa 0/6	
□	Detailed	7204	153	ModBus	Client	7.7.7.7	1.1.1.7	15	Fa 0/7	
□	Detailed	7205	154	S7	Client	8.8.8.8	1.1.1.8	0-16:0-16	Fa 0/8	
	Permit			-	Client					
	Permit			-	Client					
	Permit			-	Client					

FTP Server IP: 10.1.247.8

Firewall Mode: enabled

Rules Count: 25

FTP | Block Non Explicit Traffic | SysLog | Firewall.rule

FTP Server (1.0 KB/Sec) 2 KB/2 KB

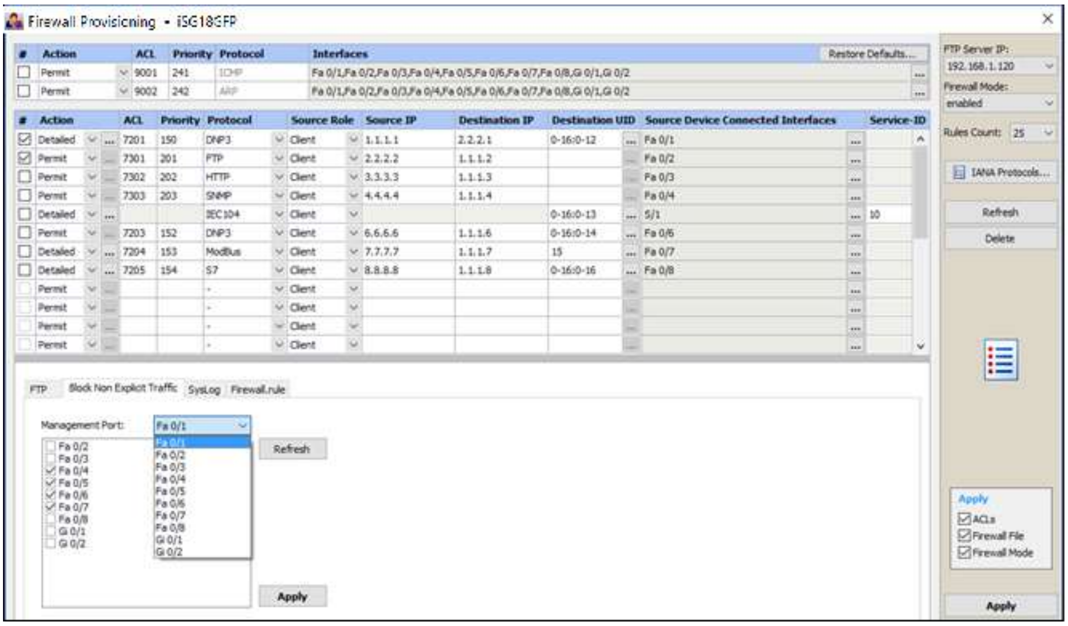
```
[03-APR-2017 17:31:47]  TFTP Server thread created on port: 69

[03-APR-2017 17:31:51]  Read from server (RRQ) - Request comming from: 10.1.247.254:49154
[03-APR-2017 17:31:51]  Block Size:     1432 bytes
[03-APR-2017 17:31:51]  File:           C:\RADiFlow\EMS\FIREWALL\10.1.247.254\firewall.rules
[03-APR-2017 17:31:51]  Size:           2.2 KB
[03-APR-2017 17:31:51]  Time:           10 MS

[03-APR-2017 17:32:00]  Read from server (RRQ) - Request comming from: 10.1.247.254:49154
[03-APR-2017 17:32:00]  Block Size:     1432 bytes
[03-APR-2017 17:32:00]  File:           C:\RADiFlow\EMS\FIREWALL\10.1.247.254\firewall.ini
[03-APR-2017 17:32:00]  Size:           1.0 KB
[03-APR-2017 17:32:00]  Time:           10 MS
[03-APR-2017 17:32:01]  TFTP Server thread terminated on port: 69
```

Apply
☑ ACLs
☑ Firewall File
☑ Firewall Mode

Figure 39 – FTP Server Logs

6.4.3 Block Non-Explicit Traffic tab

Go to **Firewall Provisioning** and select **Block Non-Explicit Traffic**. The **Block Non-Explicit Traffic** appears.



#	Action	ACL	Priority	Protocol	Interfaces
□	Permit	9001	241	ICMP	Fa 0/1,Fa 0/2,Fa 0/3,Fa 0/4,Fa 0/5,Fa 0/6,Fa 0/7,Fa 0/8,Gi 0/1,Gi 0/2
□	Permit	9002	242	ARP	Fa 0/1,Fa 0/2,Fa 0/3,Fa 0/4,Fa 0/5,Fa 0/6,Fa 0/7,Fa 0/8,Gi 0/1,Gi 0/2

#	Action	ACL	Priority	Protocol	Source Role	Source IP	Destination IP	Destination UID	Source Device Connected Interfaces	Service-ID
☑	Detailed	7201	150	DNP3	Client	1.1.1.1	2.2.2.1	0-16:0-12	Fa 0/1	
☑	Permit	7301	201	FTP	Client	2.2.2.2	1.1.1.2		Fa 0/2	
□	Permit	7302	202	HTTP	Client	3.3.3.3	1.1.1.3		Fa 0/3	
□	Permit	7303	203	SNMP	Client	4.4.4.4	1.1.1.4		Fa 0/4	
□	Detailed			IEC104	Client			0-16:0-13	S/1	10
□	Permit	7203	152	DNP3	Client	6.6.6.6	1.1.1.6	0-16:0-14	Fa 0/6	
□	Detailed	7204	153	ModBus	Client	7.7.7.7	1.1.1.7	15	Fa 0/7	
□	Detailed	7205	154	S7	Client	8.8.8.8	1.1.1.8	0-16:0-16	Fa 0/8	
	Permit			-	Client					
	Permit			-	Client					
	Permit			-	Client					
	Permit			-	Client					

FTP Server IP: 192.168.1.120

Firewall Mode: enabled

Rules Count: 25

FTP | Block Non Explicit Traffic | SysLog | Firewall.rule

Management Port: Fa 0/1

Fa 0/1
Fa 0/2
Fa 0/3
Fa 0/4
Fa 0/5
Fa 0/6
Fa 0/7
Fa 0/8
Gi 0/1
Gi 0/2

□ Fa 0/2
□ Fa 0/3
☑ Fa 0/4
☑ Fa 0/5
☑ Fa 0/6
☑ Fa 0/7
□ Fa 0/8
□ Gi 0/1
□ Gi 0/2

Apply
☑ ACLs
☑ Firewall File
☑ Firewall Mode

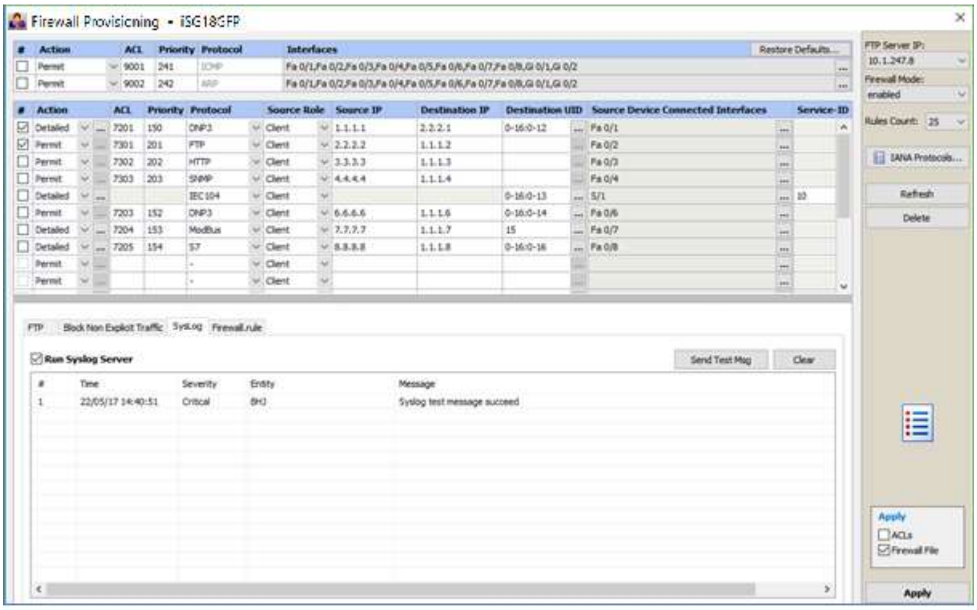
Figure 40 – Block Non-Explicit Traffic

To block non-explicit traffic on a specific physical port, select all or some of the ports that needs to be blocked by adding checkmark in their respective checkboxes and click **Apply**.

It is impossible to block a management port. To select the management port, in the drop-down box, click one of the physical ports in the secure gateway. Once a management port is selected, it will disappear from the list of the possible ports to be blocked.

6.4.4 SysLog tab

Go to **Firewall Provisioning** and select **SysLog**. All system logs will appear.



#	Action	ACL	Priority	Protocol	Interfaces
□	Permit	9001	241	ICMP	Fa 0/1,Fa 0/2,Fa 0/3,Fa 0/4,Fa 0/5,Fa 0/6,Fa 0/7,Fa 0/8,Gi 0/1,Gi 0/2
□	Permit	9002	242	ARP	Fa 0/1,Fa 0/2,Fa 0/3,Fa 0/4,Fa 0/5,Fa 0/6,Fa 0/7,Fa 0/8,Gi 0/1,Gi 0/2

#	Action	ACL	Priority	Protocol	Source Role	Source IP	Destination IP	Destination UID	Source Device Connected Interfaces	Service-ID
☑	Detailed	7201	150	DNP3	Client	1.1.1.1	2.2.2.1	0-16:0-12	Fa 0/1	
☑	Permit	7301	201	FTP	Client	2.2.2.2	1.1.1.2		Fa 0/2	
□	Permit	7302	202	HTTP	Client	3.3.3.3	1.1.1.3		Fa 0/3	
□	Permit	7303	203	SNMP	Client	4.4.4.4	1.1.1.4		Fa 0/4	
□	Detailed			IEC104	Client			0-16:0-13	S/1	10
□	Permit	7203	152	DNP3	Client	6.6.6.6	1.1.1.6	0-16:0-14	Fa 0/6	
□	Detailed	7204	153	ModBus	Client	7.7.7.7	1.1.1.7	15	Fa 0/7	
□	Detailed	7205	154	S7	Client	8.8.8.8	1.1.1.8	0-16:0-16	Fa 0/8	
	Permit			-	Client					
	Permit			-	Client					

FTP Server IP: 10.1.247.8

Firewall Mode: enabled

Rules Count: 25

☑ Run Syslog Server

#	Time	Severity	Entity	Message
1	22/05/17 14:40:51	Critical	BHJ	Syslog test message succeed

Apply

□ ACLs

☑ Firewall File

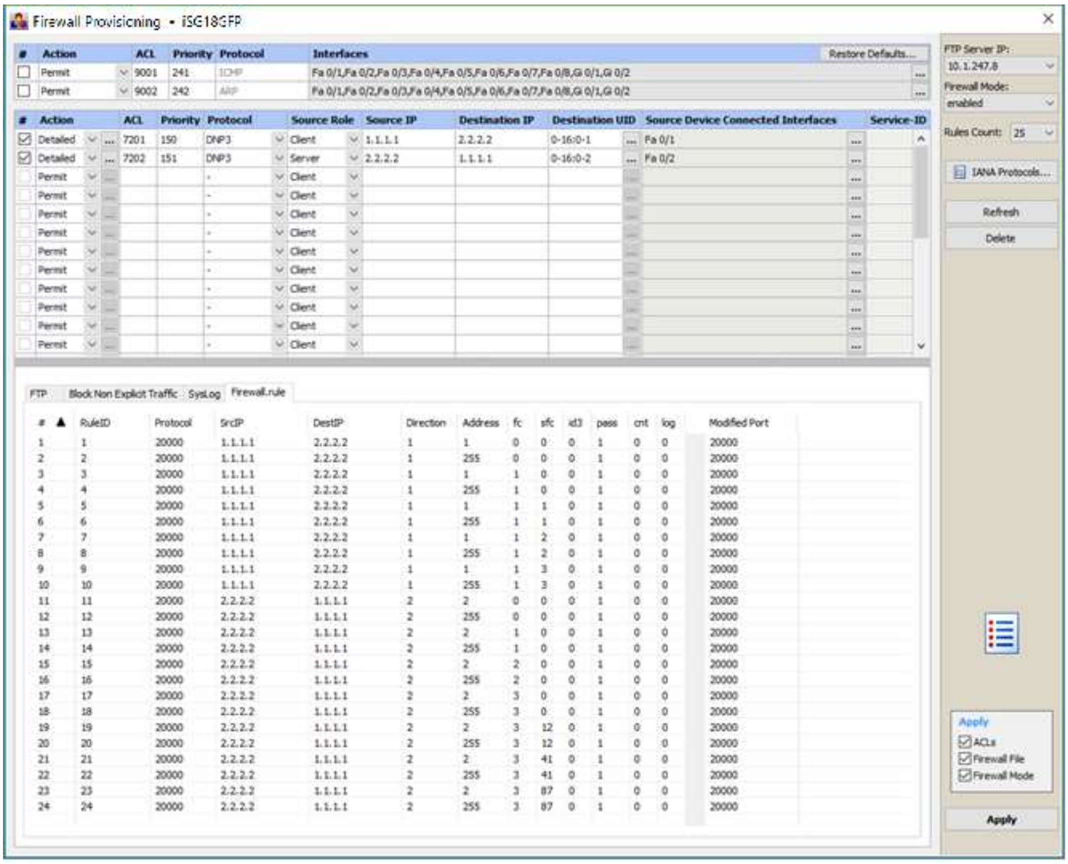
Figure 41 – SysLog tab

1. Check/uncheck **Run SysLog Server** box to enable/disable the SysLog Server.
2. Click **Send Test Msg** to check if the SysLog Server is operational or not.
3. Click **Clear** button to clear SysLog Server Logs.

✎ Most of the logs that will appear will be debug logs.

6.4.5 Firewall Rules Tab

Go to **Firewall Provisioning** and select **Firewall.rule**. All Firewall rules will appear in the Firewall.rule tab.



#	Action	ACL	Priority	Protocol	Interfaces
□	Permit	9001	241	ICMP	Fa 0/1,Fa 0/2,Fa 0/3,Fa 0/4,Fa 0/5,Fa 0/6,Fa 0/7,Fa 0/8,Gi 0/1,Gi 0/2
□	Permit	9002	242	ARP	Fa 0/1,Fa 0/2,Fa 0/3,Fa 0/4,Fa 0/5,Fa 0/6,Fa 0/7,Fa 0/8,Gi 0/1,Gi 0/2

#	Action	ACL	Priority	Protocol	Source Role	Source IP	Destination IP	Destination UID	Source Device Connected Interfaces	Service-ID
☑	Detailed	7201	150	DNP3	Client	1.1.1.1	2.2.2.2	0-16:0-1	Fa 0/1	
☑	Detailed	7202	151	DNP3	Server	2.2.2.2	1.1.1.1	0-16:0-2	Fa 0/2	
□	Permit			-	Client					
□	Permit			-	Client					
□	Permit			-	Client					
□	Permit			-	Client					
□	Permit			-	Client					
□	Permit			-	Client					
□	Permit			-	Client					
□	Permit			-	Client					
□	Permit			-	Client					
□	Permit			-	Client					

FTP Server IP: 10.1.247.8

Firewall Mode: enabled

Rules Count: 25

Apply
☑ ACLs
☑ Firewall File
☑ Firewall Mode

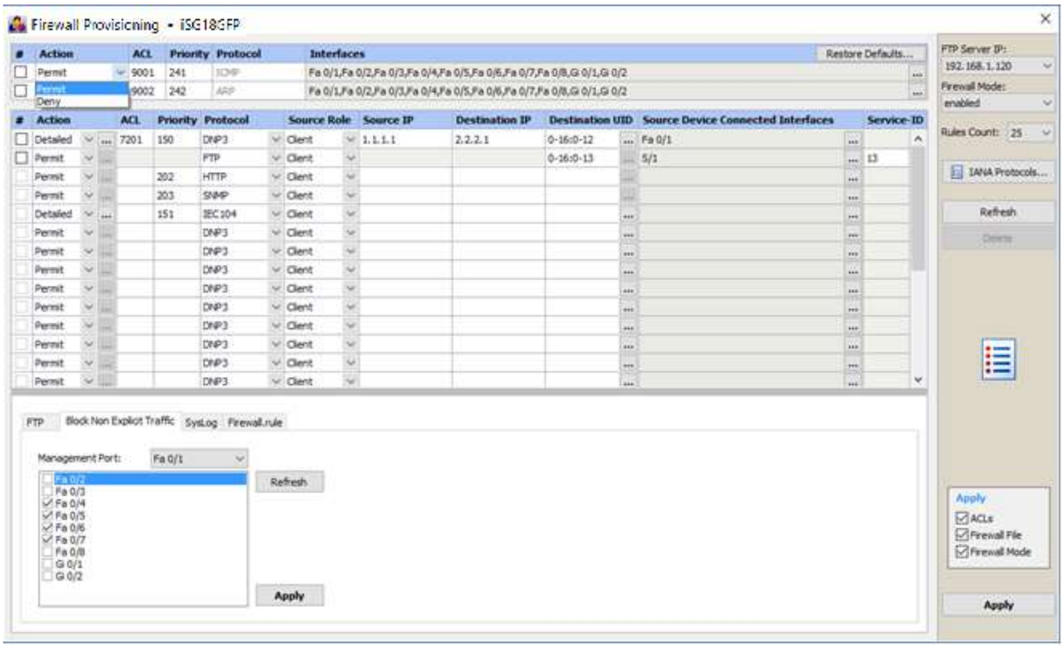
#	▲	RuleID	Protocol	SrcIP	DestIP	Direction	Address	fc	sfc	id3	pass	cnt	log	Modified Port
1		1	20000	1.1.1.1	2.2.2.2	1	1	0	0	0	1	0	0	20000
2		2	20000	1.1.1.1	2.2.2.2	1	255	0	0	0	1	0	0	20000
3		3	20000	1.1.1.1	2.2.2.2	1	1	1	0	0	1	0	0	20000
4		4	20000	1.1.1.1	2.2.2.2	1	255	1	0	0	1	0	0	20000
5		5	20000	1.1.1.1	2.2.2.2	1	1	1	1	0	1	0	0	20000
6		6	20000	1.1.1.1	2.2.2.2	1	255	1	1	0	1	0	0	20000
7		7	20000	1.1.1.1	2.2.2.2	1	1	1	2	0	1	0	0	20000
8		8	20000	1.1.1.1	2.2.2.2	1	255	1	2	0	1	0	0	20000
9		9	20000	1.1.1.1	2.2.2.2	1	1	1	3	0	1	0	0	20000
10		10	20000	1.1.1.1	2.2.2.2	1	255	1	3	0	1	0	0	20000
11		11	20000	2.2.2.2	1.1.1.1	2	2	0	0	0	1	0	0	20000
12		12	20000	2.2.2.2	1.1.1.1	2	255	0	0	0	1	0	0	20000
13		13	20000	2.2.2.2	1.1.1.1	2	2	1	0	0	1	0	0	20000
14		14	20000	2.2.2.2	1.1.1.1	2	255	1	0	0	1	0	0	20000
15		15	20000	2.2.2.2	1.1.1.1	2	2	2	0	0	1	0	0	20000
16		16	20000	2.2.2.2	1.1.1.1	2	255	2	0	0	1	0	0	20000
17		17	20000	2.2.2.2	1.1.1.1	2	2	3	0	0	1	0	0	20000
18		18	20000	2.2.2.2	1.1.1.1	2	255	3	0	0	1	0	0	20000
19		19	20000	2.2.2.2	1.1.1.1	2	2	3	12	0	1	0	0	20000
20		20	20000	2.2.2.2	1.1.1.1	2	255	3	12	0	1	0	0	20000
21		21	20000	2.2.2.2	1.1.1.1	2	2	3	41	0	1	0	0	20000
22		22	20000	2.2.2.2	1.1.1.1	2	255	3	41	0	1	0	0	20000
23		23	20000	2.2.2.2	1.1.1.1	2	2	3	87	0	1	0	0	20000
24		24	20000	2.2.2.2	1.1.1.1	2	255	3	87	0	1	0	0	20000

Figure 42 – Firewall.rule tab

6.4.6 IP Connectivity

Go to **Firewall Provisioning** and then to IP connectivity (see section 9, Figure 31 – Firewall Provisioning Areas).

1. Go to **Action** and from the drop-down box select to permit or deny ICMP and/or ARP.



Firewall Provisioning • iSG18GFP

#	Action	ACL	Priority	Protocol	Interfaces
☐	Permit	9001	241	ICMP	Fa 0/1,Fa 0/2,Fa 0/3,Fa 0/4,Fa 0/5,Fa 0/6,Fa 0/7,Fa 0/8,Gi 0/1,Gi 0/2
☐	Permit Deny	9002	242	ARP	Fa 0/1,Fa 0/2,Fa 0/3,Fa 0/4,Fa 0/5,Fa 0/6,Fa 0/7,Fa 0/8,Gi 0/1,Gi 0/2

#	Action	ACL	Priority	Protocol	Source Role	Source IP	Destination IP	Destination UID	Source Device Connected Interfaces	Service-ID
☐	Detailed	7201	150	DNP3	Client	1.1.1.1	2.2.2.1	0-16:0-12	Fa 0/1	
☐	Permit			FTP	Client			0-16:0-13	5/1	13
	Permit		202	HTTP	Client					
	Permit		203	SNMP	Client					
	Detailed		151	IEC104	Client					
	Permit			DNP3	Client					
	Permit			DNP3	Client					
	Permit			DNP3	Client					
	Permit			DNP3	Client					
	Permit			DNP3	Client					
	Permit			DNP3	Client					
	Permit			DNP3	Client					
	Permit			DNP3	Client					
	Permit			DNP3	Client					

FTP Server IP: 192.168.1.120

Firewall Mode: enabled

Rules Count: 25

Management Port: Fa 0/1

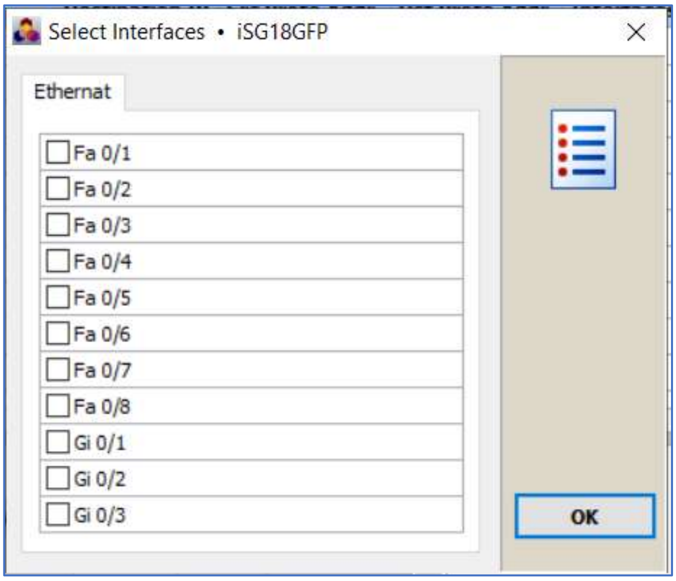
☐ Fa 0/2
☐ Fa 0/3
☑ Fa 0/4
☑ Fa 0/5
☑ Fa 0/6
☑ Fa 0/7
☐ Fa 0/8
☐ Gi 0/1
☐ Gi 0/2

Apply
☑ ACLs
☑ Firewall File
☑ Firewall Mode

Figure 43 – IP Connectivity, Action

- ICMP default ACL is 9001, it is possible to change it between 10 to 9500 if necessary.
- ICMP default priority is 241, it is possible to change it between 1 to 255 if necessary.
- ARP default ACL is 9002, it is possible to change it between 10 to 9500 if necessary.
- ARP default priority is 242, it is possible to change it between 1 to 255 if necessary.
- If any of the default settings was changed, it is possible to revert it back to its default settings by clicking **Restore Defaults…** in the IP connectivity section.
- It is recommended to leave the default ACLs and priority numbers as shown in IP connectivity.

2. In # column, check/uncheck which IP connectivity rules to be applied to the firewall rules.
3. In **Interfaces** column, click **Interfaces**. The **Select Interfaces** screen opens.



Select Interfaces • iSG18GFP

Ethernat

☐ Fa 0/1
☐ Fa 0/2
☐ Fa 0/3
☐ Fa 0/4
☐ Fa 0/5
☐ Fa 0/6
☐ Fa 0/7
☐ Fa 0/8
☐ Gi 0/1
☐ Gi 0/2
☐ Gi 0/3

Figure 44 – Select Interfaces, IP tab

4. If the IP connectivity rule you are permitting/denying is relevant to a specific IP physical port, select one of the IP physical ports and click **OK**.
5. If the IP connectivity rule you are permitting/denying is relevant to a specific serial physical port, click **Serial**.

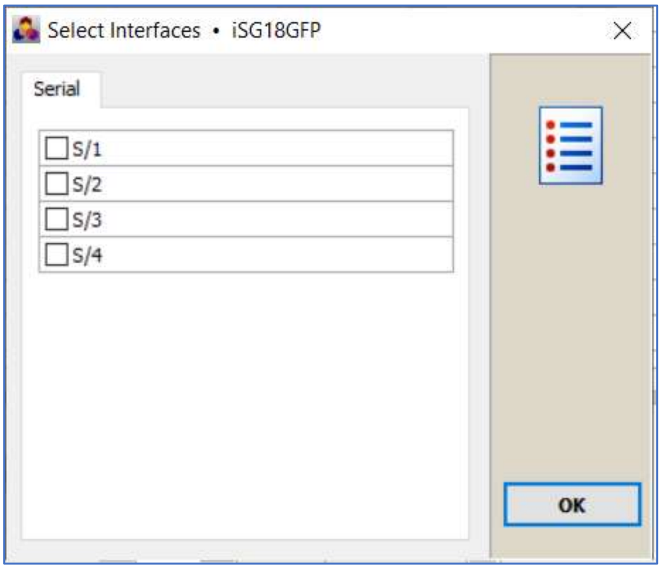
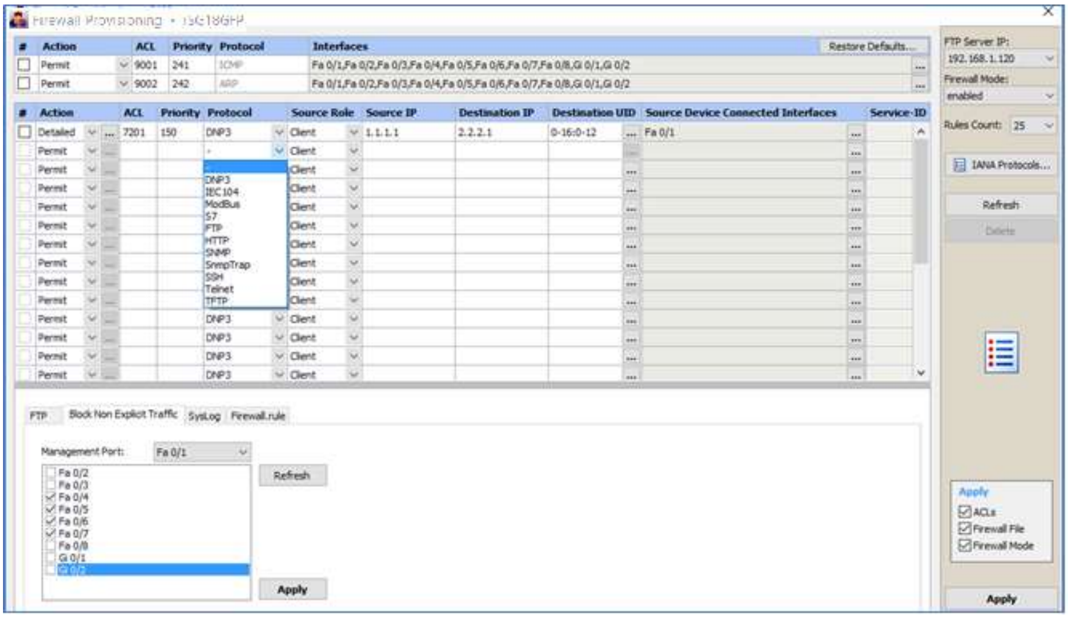


Figure 45 – Select Interfaces, Serial tab

6. Select one of the serial physical ports. Click **OK**.

6.4.7 Firewall Rules

1. Go to **Firewall Provisioning** and then to **Firewall Rules** section (refer to section 8, Figure 31 – Firewall Provisioning Areas). Under **Protocol**, by clicking in the drop-down box, select the specific protocol (DNP3, IEC104, ModBus, S7, FTP, HTTP, SNMP, SNMPTrap, SSH, Telnet, TerminalServer or TFTP) for which a rule will be generated.



#	Action	ACL	Priority	Protocol	Interfaces
☐	Permit	9001	241	ICMP	Fa 0/1,Fa 0/2,Fa 0/3,Fa 0/4,Fa 0/5,Fa 0/6,Fa 0/7,Fa 0/8,Gi 0/1,Gi 0/2
☐	Permit	9002	242	ARP	Fa 0/1,Fa 0/2,Fa 0/3,Fa 0/4,Fa 0/5,Fa 0/6,Fa 0/7,Fa 0/8,Gi 0/1,Gi 0/2

#	Action	ACL	Priority	Protocol	Source Role	Source IP	Destination IP	Destination UID	Source Device Connected Interfaces	Service-ID
☐	Detailed	7201	150	DNP3	Client	1.1.1.1	2.2.2.1	0-16:0-12	Fa 0/1	
	Permit			-	Client					
	Permit				Client					
	Permit				Client					
	Permit				Client					
	Permit				Client					
	Permit				Client					
	Permit				Client					
	Permit				Client					
	Permit				Client					
	Permit			DNP3	Client					
	Permit			DNP3	Client					
	Permit			DNP3	Client					
	Permit			DNP3	Client					

Management Port: Fa 0/1

☐ Fa 0/2
☐ Fa 0/3
☑ Fa 0/4
☑ Fa 0/5
☑ Fa 0/6
☑ Fa 0/7
☐ Fa 0/8
☐ Gi 0/1
☐ Gi 0/2

FTP Server IP: 192.168.1.120

Firewall Mode: enabled

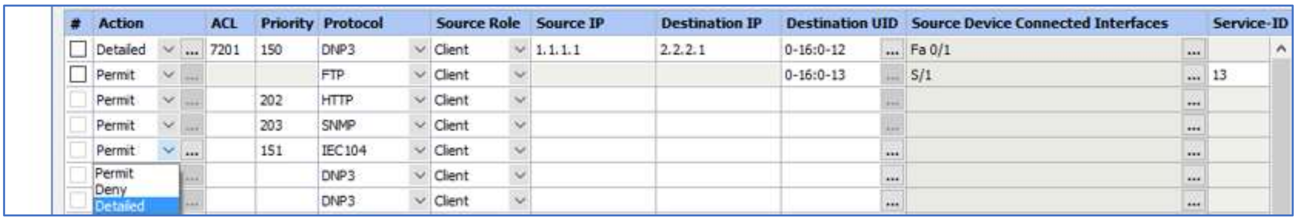
Rules Count: 25

Apply
☑ ACLs
☑ Firewall File
☑ Firewall Mode

Figure 46 – Firewall Rules, Protocol

Only SCADA protocols (DNP3, IEC104, ModBus and S7) have detailed DPI ability, so, only in such cell a Detailed capability can appear. Once Detailed capability is selected, ACL will be between 7201 to 7300 and priority will be between 150 to 199.

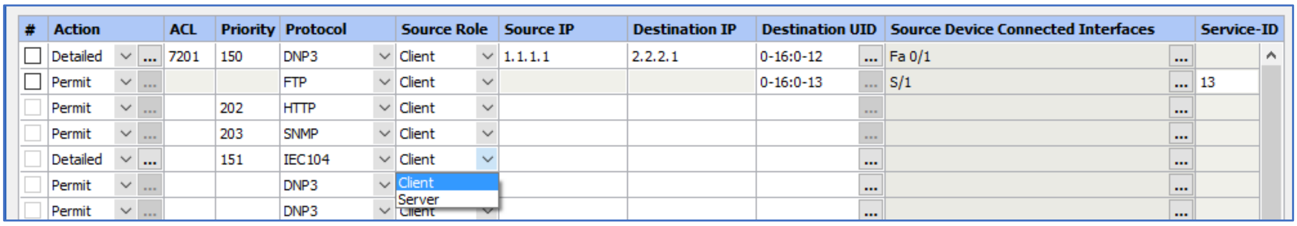
2. In the same area, go to **Action**, select **Permit /Deny /Detailed** (if SCADA protocol was selected), by clicking in the drop-down box for the rule you are generating.



#	Action	ACL	Priority	Protocol	Source Role	Source IP	Destination IP	Destination UID	Source Device Connected Interfaces	Service-ID
□	Detailed	7201	150	DNP3	Client	1.1.1.1	2.2.2.1	0-16:0-12	Fa 0/1	
□	Permit			FTP	Client			0-16:0-13	S/1	13
□	Permit		202	HTTP	Client					
□	Permit		203	SNMP	Client					
□	Permit		151	IEC104	Client					
□				DNP3	Client					
□				DNP3	Client					

Figure 47 – Firewall Rules, Action: Permit /Deny /Detailed

3. In the same area, go to **Source Role**, and from the drop-down menu select **Client/Server**.



#	Action	ACL	Priority	Protocol	Source Role	Source IP	Destination IP	Destination UID	Source Device Connected Interfaces	Service-ID
□	Detailed	7201	150	DNP3	Client	1.1.1.1	2.2.2.1	0-16:0-12	Fa 0/1	
□	Permit			FTP	Client			0-16:0-13	S/1	13
□	Permit		202	HTTP	Client					
□	Permit		203	SNMP	Client					
□	Detailed		151	IEC104	Client					
□	Permit			DNP3						
□	Permit			DNP3	Client					

Figure 48 – Firewall Rules, Source Role, Client/Server

4. Go to **ACL**, and for the rule to be generated, type an ACL number (between 7201 to 7300, for detailed SCADA protocols, and 7301 to 7400, for the rest).

5. Go to **Priority**, and for the rule to be generated, type a priority number (between 150 to 199, for detailed SCADA protocols and 201 to 240, for the rest).

If ACL and priority numbers will be out of their limits, the box will be colored in yellow, to signify a mistake.

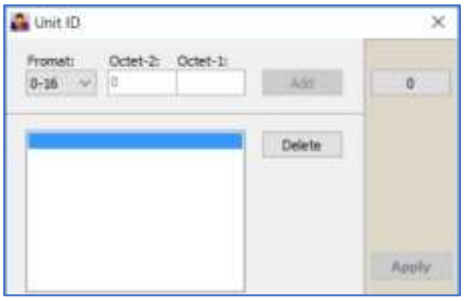
6. Go to **Source IP** header and type a source IP address (IPv4 address format).

7. Go to **Destination IP** and type a **Destination IP** address (IPv4 address format).

If a SCADA protocol (DNP3, IEC104, ModBus, and S7) is set, UID must be entered. If no SCADA protocol has been set, skip to step 8.

DNP3 protocol

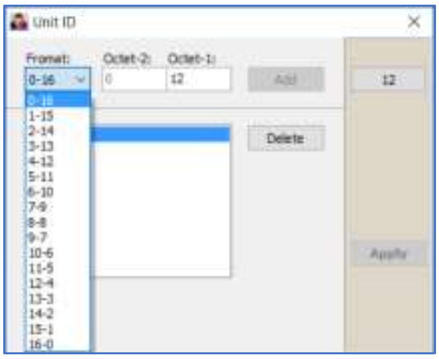
a. If a DNP3 protocol is set, click **UID**. **Unit ID** screen appears.



Fromat: 0-16
Octet-2: 0
Octet-1:

Figure 49 – Unit ID

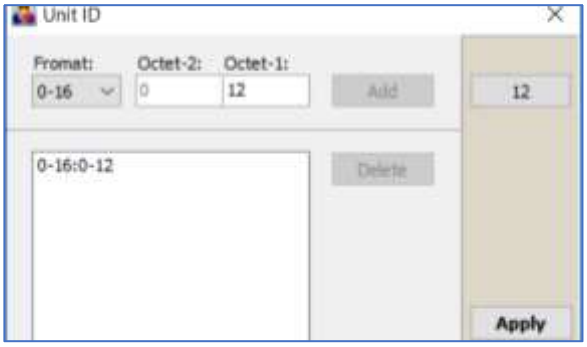
b. Select Unit ID format by choosing it in the drop-down box.



Fromat: 0-16
Octet-2: 0
Octet-1: 12

Figure 50 – Unit ID Drop-down Box

c. Following Unit ID format, type the Unit ID in Octet-2 and Octet-1 fields. Click **Add**. Then, click **Apply**.



Fromat: 0-16
Octet-2: 0
Octet-1: 12

0-16:0-12

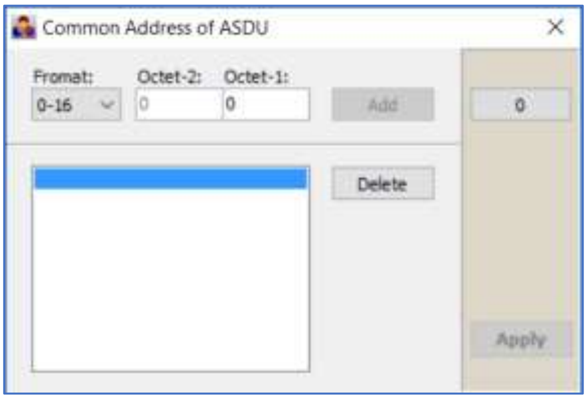
Figure 51 – Unit ID after Typing in Octet-2 and Octet-1

If Unit ID format **0-16** is selected, Octet-2 will be colored gray and set as 0.

If Unit ID format **16-0** is selected, Octet-1 will be colored gray and set as 0.

IEC104 protocol

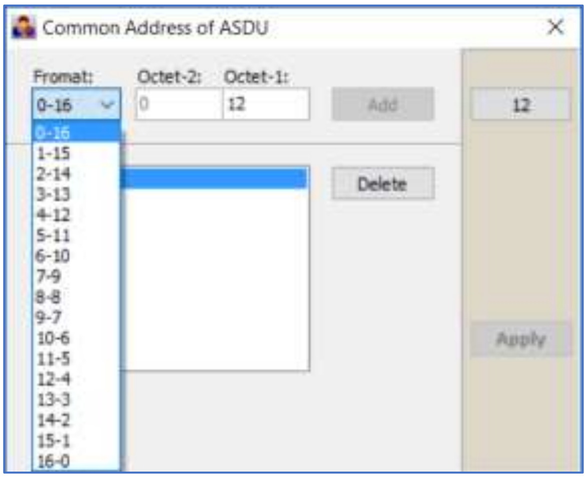
a. If IEC104 protocol is set, go to **UID**. **Common Address of ASDU** screen appears.



Fromat: 0-16
Octet-2: 0
Octet-1: 0

Figure 52 – Common Address of ASDU

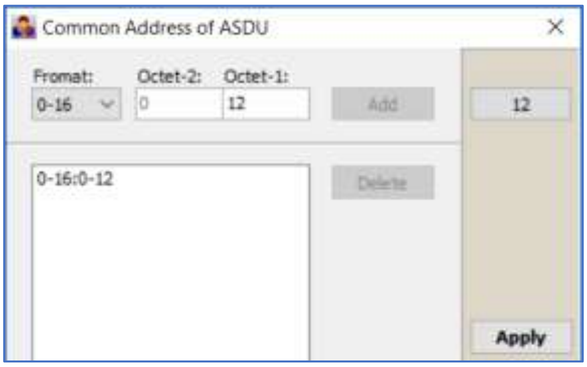
b. Select Common **Address of ASDU** format by choosing from the drop-down box options.



Fromat: 0-16
Octet-2: 0
Octet-1: 12

Figure 53 – Common Address of ASDU Drop-Down Box

c. As per **Common Address of ASDU format**, type the Common Address of ASDU in Octet-2 and Octet-1 fields. Click **Add**. Click **Apply**.



Fromat: 0-16

Octet-2: 0

Octet-1: 12

0-16:0-12

12

Figure 54 – Common Address of ASDU Octet-2 and Octet-1 Completed

✎ If Unit ID format **0-16** is selected, Octet-2 will be colored gray and set as 0.

✎ If Unit ID format **16-0** is selected, Octet-1 will be colored gray and set as 0.

ModBus Protocol

a. If ModBus protocol is set, click **UID**. Unit ID screen appears.

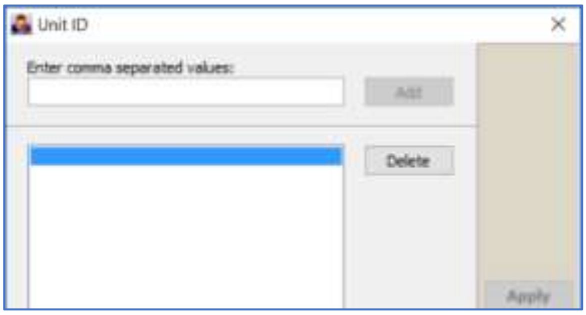


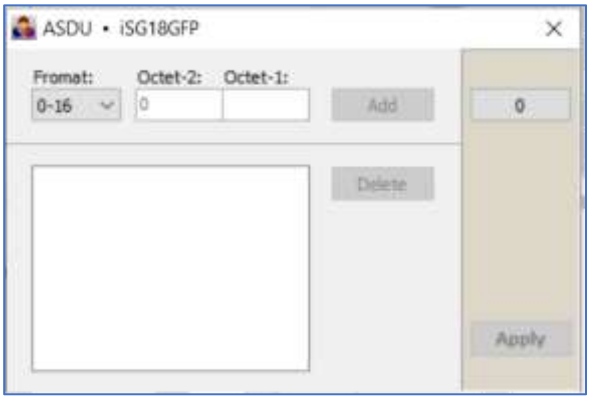
Figure 55 – Unit ID screen for ModBus Protocol

b. According to Unit ID format, type the Unit ID value. If several values are needed, use comma between values, e.g. 11,23,45). Click **Add**. Click **Apply**.

✎ Only decimal numbers can be used for ModBus Unit ID.

S7 protocol

a. If S7 Protocol is set, click UID. ASDU screen appears.



Fromat: 0-16

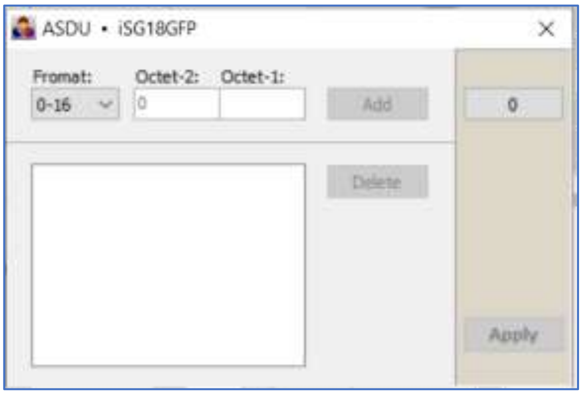
Octet-2: 0

Octet-1:

0

Figure 56 – ASDU screen for S7 Protocol

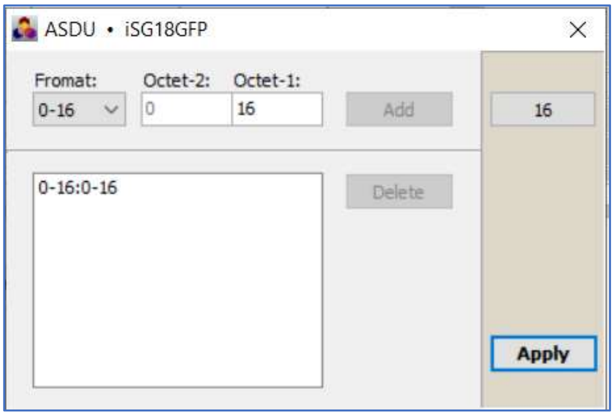
b. Select an ASDU format by choosing from the drop-down box options.



Fromat: 0-16
Octet-2: 0
Octet-1:

Figure 57 – ASDU screen for S7 Protocol with Drop-Down Box Options

c. According to ASDU format, write the ASDU in Octet-2 and Octet-1 fields. Click **Add**. Click **Apply**.



Fromat: 0-16
Octet-2: 0
Octet-1: 16

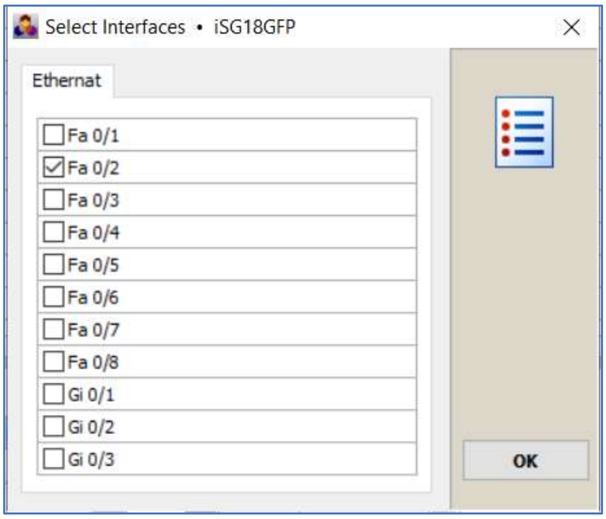
0-16:0-16

Figure 58 – ASDU for S7 Protocol Octet-2 and Octet-1 Completed

If Unit ID format **0-16** is selected, Octet-2 will be colored gray and set as 0.

If Unit ID format **16-0** is selected, Octet-1 will be colored gray and set as 0.

8. Go to **Interfaces**, click **Interfaces**. **Select Interfaces** screen appears.

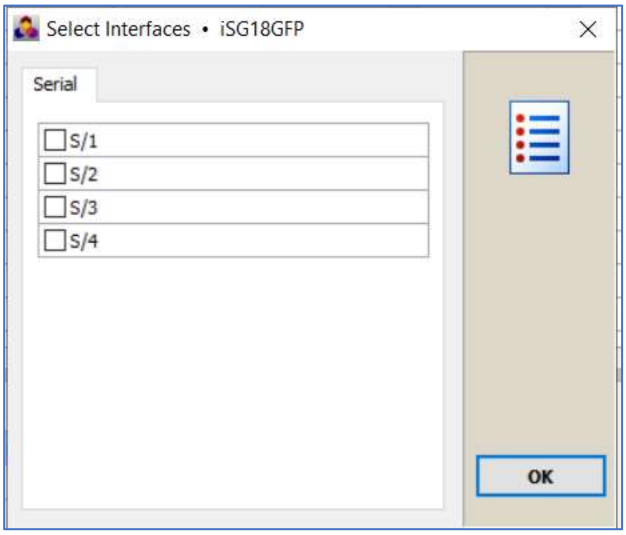


☐ Fa 0/1
☑ Fa 0/2
☐ Fa 0/3
☐ Fa 0/4
☐ Fa 0/5
☐ Fa 0/6
☐ Fa 0/7
☐ Fa 0/8
☐ Gi 0/1
☐ Gi 0/2
☐ Gi 0/3

Figure 59 – Select Interfaces Screen IP Tab

9. IF the rule to be generated is relevant to a specific IP physical port, select one of the IP physical ports and click **OK**.

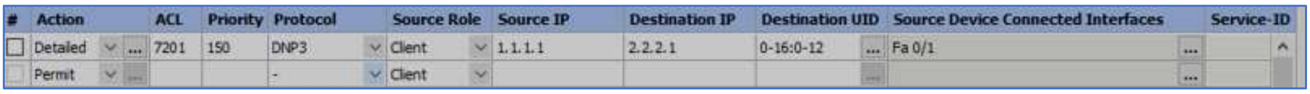
10. IF the rule to be generated is relevant to a specific serial physical port, click **Serial** tab. **Serial Interfaces Serial** screen appears.



□ S/1
□ S/2
□ S/3
□ S/4

Figure 60 – Select Interfaces Screen Serial Tab

11. Select one of the serial physical ports and click **OK**.
12. If serial interface was selected, go to **Service-ID** and type the **Service-ID** in the relevant field.



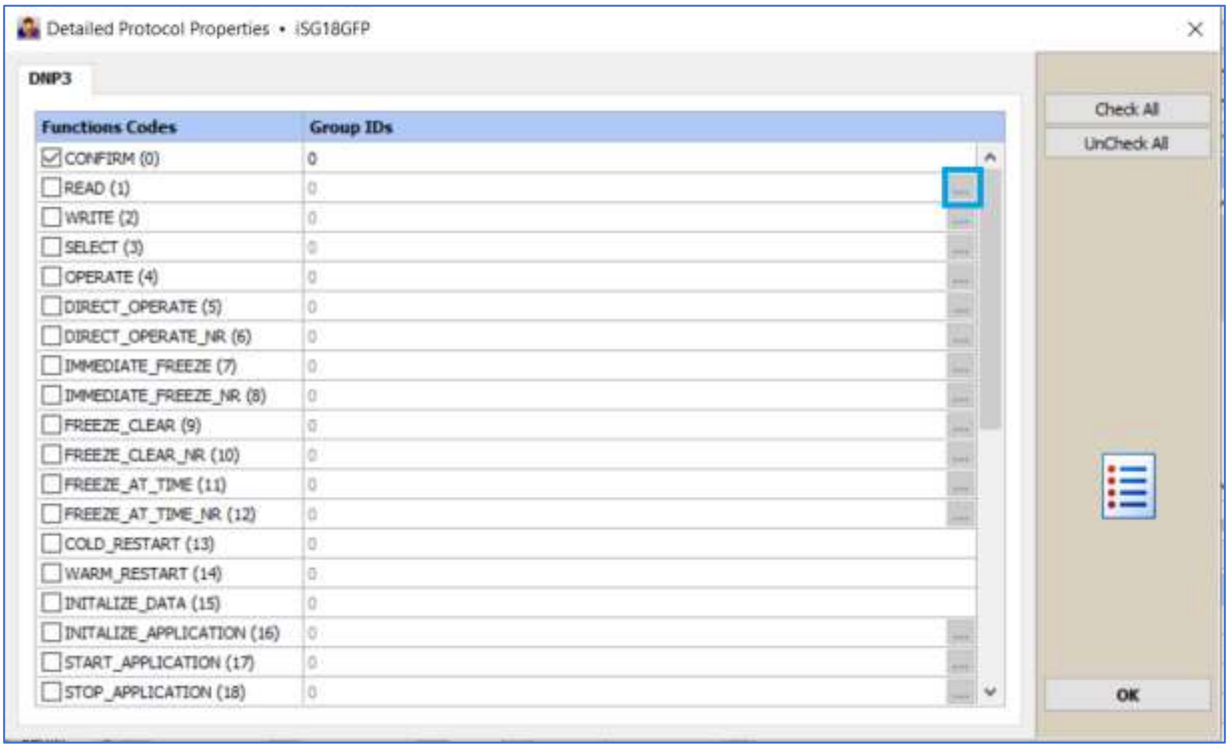
#	Action	ACL	Priority	Protocol	Source Role	Source IP	Destination IP	Destination UID	Source Device Connected Interfaces	Service-ID
□	Detailed	7201	150	DNP3	Client	1.1.1.1	2.2.2.1	0-16:0-12	Fa 0/1	
□	Permit			-	Client					

Figure 61 – Service-ID

13. If a SCADA protocol (DNP3, IEC104, ModBus and S7) is set, it is possible to specify detailed DPI firewall rules. If a SCADA protocol is not necessary, skip to Step 14.

DNP3 protocol

a. If one of the firewall rules is DNP3 protocol and detailed action is set, go to **Action**, click **Detailed** DPI. DNP3 **Detailed Protocol Properties** screen appears.



Functions Codes	Group IDs
☑ CONFIRM (0)	0
□ READ (1)	0
□ WRITE (2)	0
□ SELECT (3)	0
□ OPERATE (4)	0
□ DIRECT_OPERATE (5)	0
□ DIRECT_OPERATE_NR (6)	0
□ IMMEDIATE_FREEZE (7)	0
□ IMMEDIATE_FREEZE_NR (8)	0
□ FREEZE_CLEAR (9)	0
□ FREEZE_CLEAR_NR (10)	0
□ FREEZE_AT_TIME (11)	0
□ FREEZE_AT_TIME_NR (12)	0
□ COLD_RESTART (13)	0
□ WARM_RESTART (14)	0
□ INITALIZE_DATA (15)	0
□ INITALIZE_APPLICATION (16)	0
□ START_APPLICATION (17)	0
□ STOP_APPLICATION (18)	0

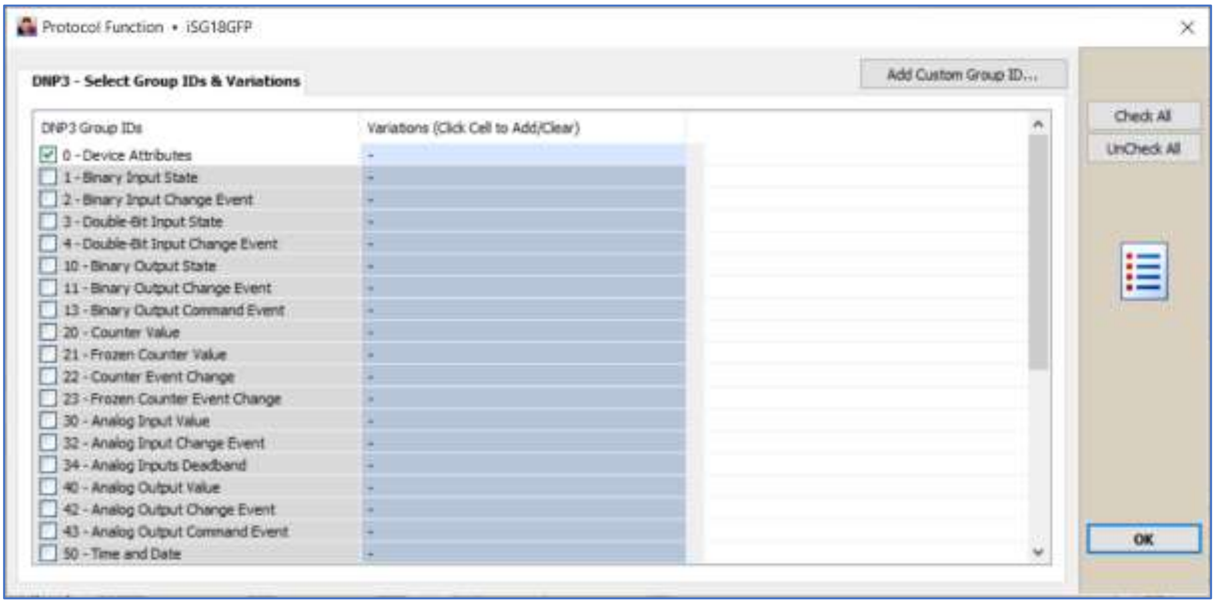
Figure 62 – Detailed Protocol Properties

b. Check/uncheck which groups of DPI detailed rules you want to apply to the firewall rules.

c. If all groups are needed for the firewall rules, click **Check All** button.

d. If you want to clear all groups, click **UnCheck All** button.

e. For DPI detailed functions codes header, go to **Functions Codes** and click DPI detailed functions button ... next to the groups you want to configure. **Select Groups IDs & Variations** screen appears



Protocol Function • iSG18GFP

DNP3 - Select Group IDs & Variations

Add Custom Group ID...

DNP3 Group IDs	Variations (Click Cell to Add/Clear)
☑ 0 - Device Attributes	-
☐ 1 - Binary Input State	-
☐ 2 - Binary Input Change Event	-
☐ 3 - Double-Bit Input State	-
☐ 4 - Double-Bit Input Change Event	-
☐ 10 - Binary Output State	-
☐ 11 - Binary Output Change Event	-
☐ 13 - Binary Output Command Event	-
☐ 20 - Counter Value	-
☐ 21 - Frozen Counter Value	-
☐ 22 - Counter Event Change	-
☐ 23 - Frozen Counter Event Change	-
☐ 30 - Analog Input Value	-
☐ 32 - Analog Input Change Event	-
☐ 34 - Analog Inputs Deadband	-
☐ 40 - Analog Output Value	-
☐ 42 - Analog Output Change Event	-
☐ 43 - Analog Output Command Event	-
☐ 50 - Time and Date	-

Figure 63 – Select Groups IDs & Variations

f. Check/uncheck which **DNP3 Group IDs** of DPI detailed rules to be applied to the firewall rules.

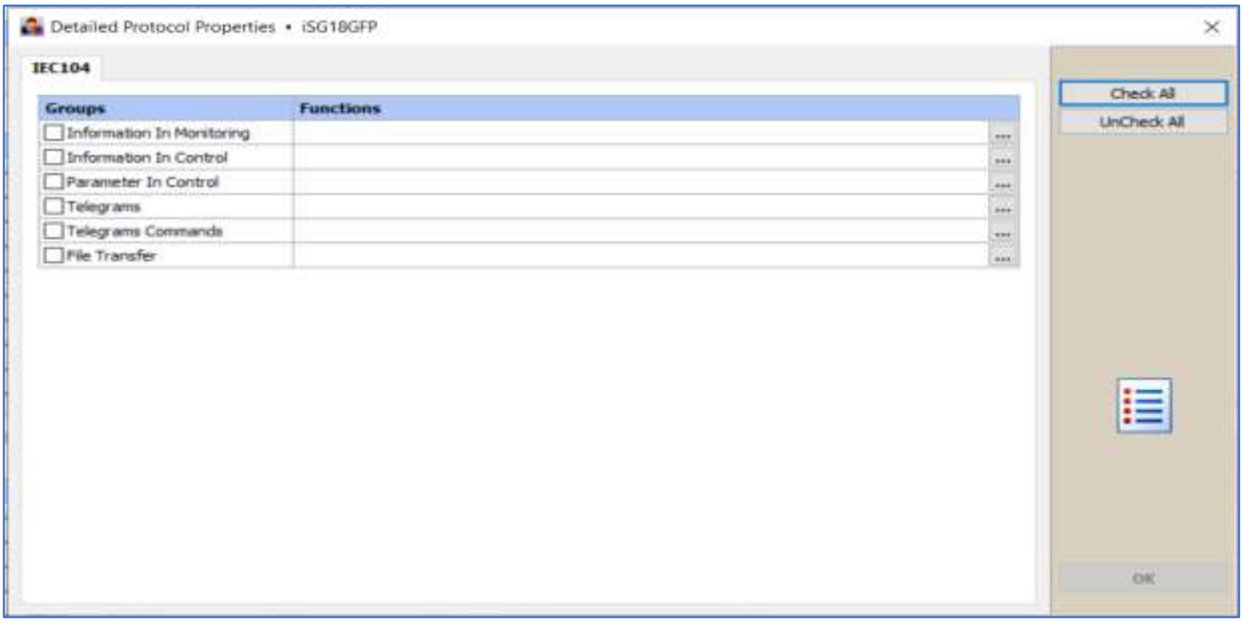
g. If all Group IDs are needed for the firewall rules, click **Check All**. To clear all Group IDs, click **UnCheck All**.

h. Under each specific Group IDs variations, insert a decimal number for range. Click **OK** to save the firewall rules and verify that Groups IDs & Variations screen closes.

i. Click **OK** to save all firewall rules in DNP3 Detailed Protocol Properties screen (see Figure 62 – Detailed Protocol Properties)

IEC104 protocol

a. If one of the firewall rules is IEC104 protocol and detailed action is set, go to **Action** (see Figure 46 – Firewall Rules, Protocol) and click detailed DPI. IEC104 **Detailed Protocol Properties** screen appears.



Detailed Protocol Properties • iSG18GFP

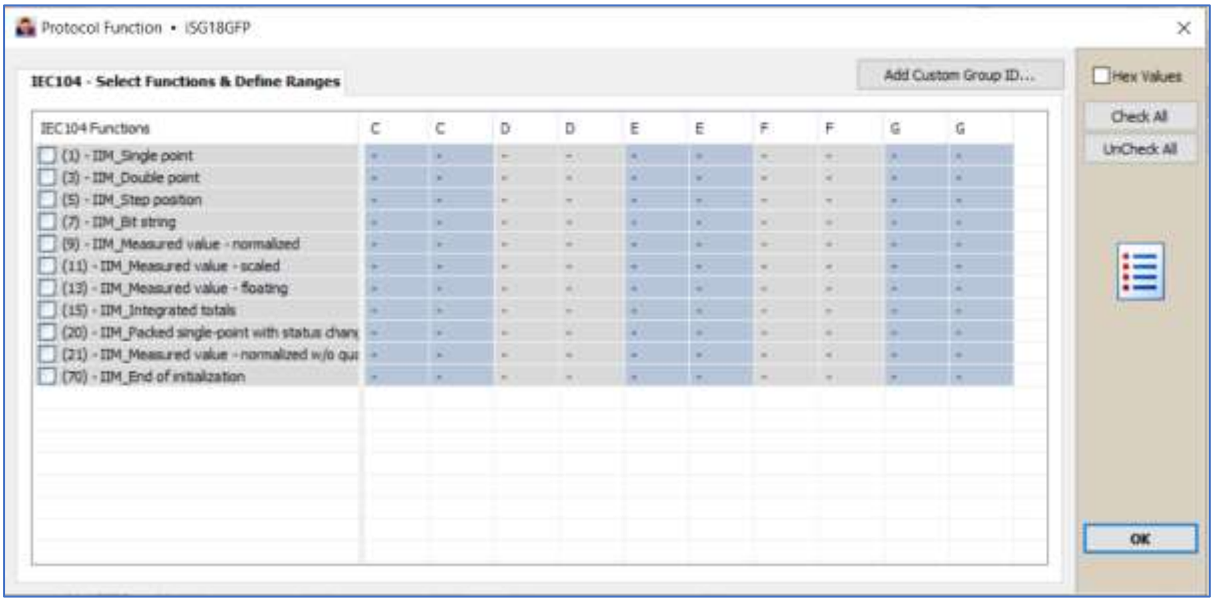
IEC104

Groups	Functions
☐ Information In Monitoring	...
☐ Information In Control	...
☐ Parameter In Control	...
☐ Telegrams	...
☐ Telegrams Commands	...
☐ File Transfer	...

Figure 64 – IEC104 Detailed Protocol Properties

b. Go to **Groups**, and check/uncheck which groups of DPI detailed rules to be applied to the firewall rules. If all groups are needed for the firewall rules, click **Check All**. If all groups are to be cleared, click **UnCheck All**.

c. For **DPI Detailed Functions**, go to **Functions** and click DPI detailed functions button ⋯ next to the groups you want to configure. **Select Functions & Define Ranges** screen appears.


Protocol Function • iSG18GFP
IEC104 - Select Functions & Define Ranges
Add Custom Group ID...
□ Hex Values
Check All
UnCheck All
OK

IEC104 Functions	C	C	D	D	E	E	F	F	G	G
□ (1) - IIM_Single point	-	-	-	-	-	-	-	-	-	-
□ (3) - IIM_Double point	-	-	-	-	-	-	-	-	-	-
□ (5) - IIM_Step position	-	-	-	-	-	-	-	-	-	-
□ (7) - IIM_Bit string	-	-	-	-	-	-	-	-	-	-
□ (9) - IIM_Measured value - normalized	-	-	-	-	-	-	-	-	-	-
□ (11) - IIM_Measured value - scaled	-	-	-	-	-	-	-	-	-	-
□ (13) - IIM_Measured value - floating	-	-	-	-	-	-	-	-	-	-
□ (15) - IIM_Integrated totals	-	-	-	-	-	-	-	-	-	-
□ (20) - IIM_Packed single-point with status chan	-	-	-	-	-	-	-	-	-	-
□ (21) - IIM_Measured value - normalized w/o qu	-	-	-	-	-	-	-	-	-	-
□ (70) - IIM_End of initialization	-	-	-	-	-	-	-	-	-	-

Figure 65 – IEC104 Select Functions & Define Ranges

d. Check/uncheck which functions of DPI detailed rules are to be applied to the firewall rules. If all functions are needed for the firewall rules, click **Check All** button. To clear all functions, click **UnCheck All**.

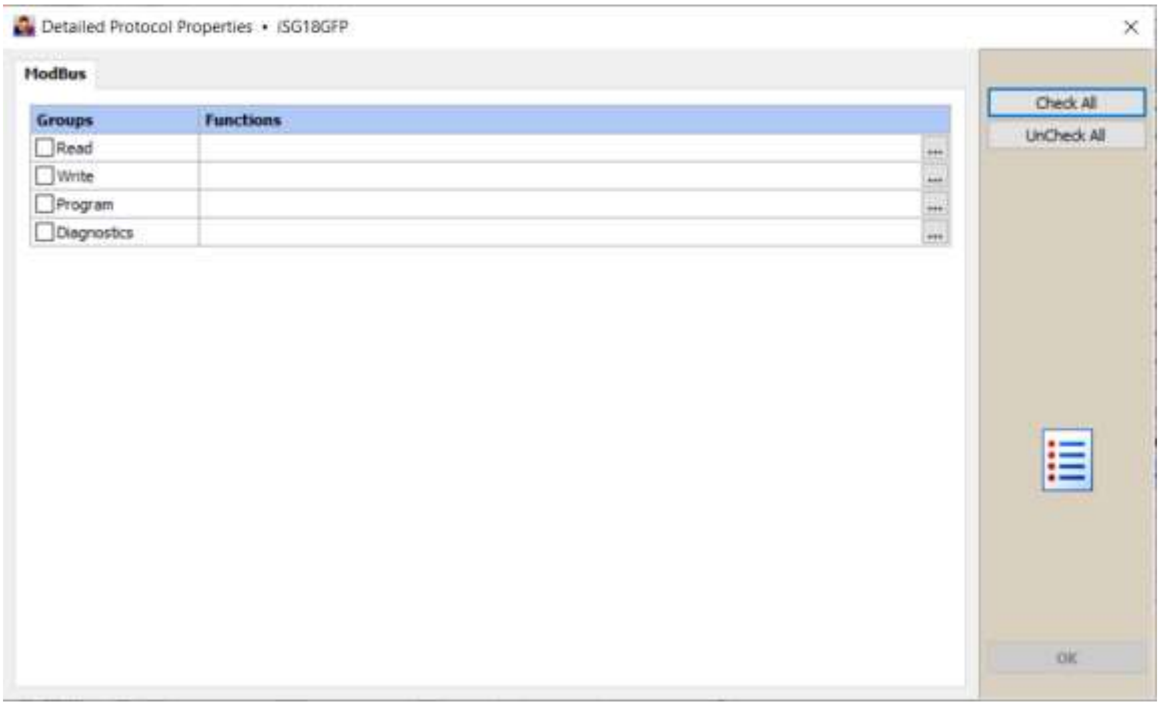
e. Under each specific functions variations, insert a decimal number for range. If **Hex Values** checkbox is selected, a hexadecimal number can be inserted under each specific functions variations.

f. In the **IEC104 Select Functions & Define Ranges** screen, Click **OK** to save the firewall rules and verify that Select Functions & Define Ranges screen closes.

g. In the **IEC104 Detailed Protocol Properties**, Click **OK** to save all firewall rules.

ModBus Protocol

a. If one of the firewall rules is ModBus protocol and detailed action is set, go to Action (see Figure 46 – Firewall Rules, Protocol) and click detailed DPI. ModBus **Detailed Protocol Properties** screen appears.



Detailed Protocol Properties • iSG18GFP

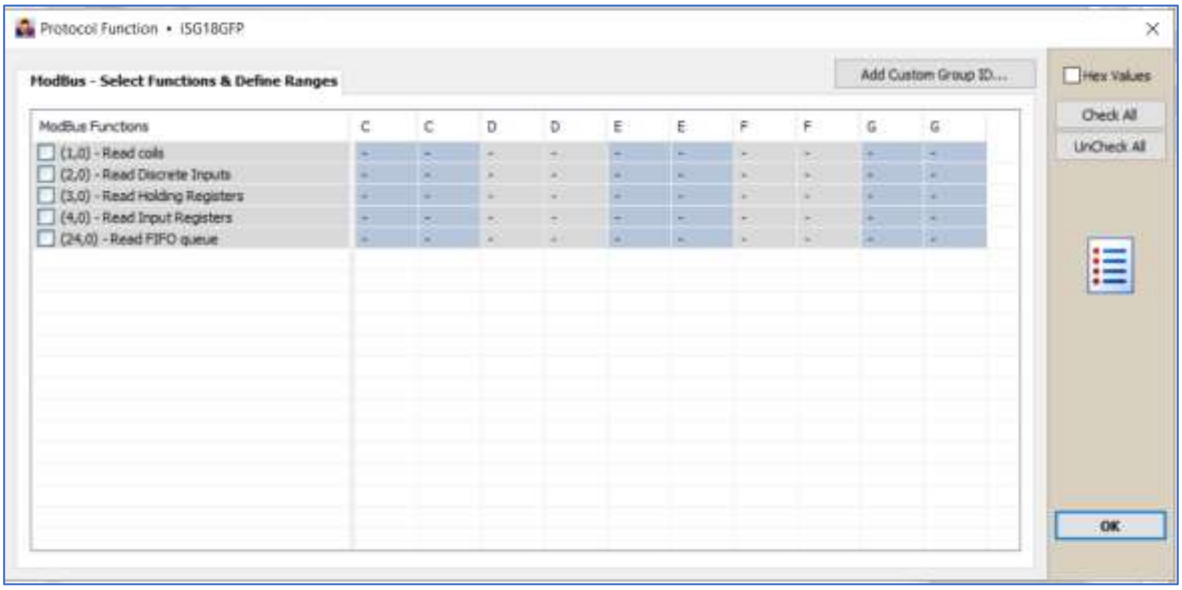
ModBus

Groups	Functions
□ Read	...
□ Write	...
□ Program	...
□ Diagnostics	...

Figure 66 – ModBus Detailed Protocol Properties

b. Check/uncheck which groups of DPI detailed rules you want to apply to the firewall rules. If all groups are needed for the firewall rules, click **Check All** button. If you want to clear all groups, click **UnCheck All** button.

c. For DPI Detailed Functions, go to Functions, click DPI detailed functions button next to the groups you want to configure. **Select Functions & Define Ranges** screen appears.



Protocol Function • iSG18GFP

ModBus - Select Functions & Define Ranges

□ Hex Values

ModBus Functions	C	C	D	D	E	E	F	F	G	G
□ (1,0) - Read coils	-	-	-	-	-	-	-	-	-	-
□ (2,0) - Read Discrete Inputs	-	-	-	-	-	-	-	-	-	-
□ (3,0) - Read Holding Registers	-	-	-	-	-	-	-	-	-	-
□ (4,0) - Read Input Registers	-	-	-	-	-	-	-	-	-	-
□ (24,0) - Read FIFO queue	-	-	-	-	-	-	-	-	-	-

Figure 67 – ModBus Select Functions & Define Ranges

d. Check/uncheck which functions of DPI detailed rules to be applied to the firewall rules. If all functions are needed for the firewall rules, click **Check All**. To clear all functions, click **UnCheck All**.

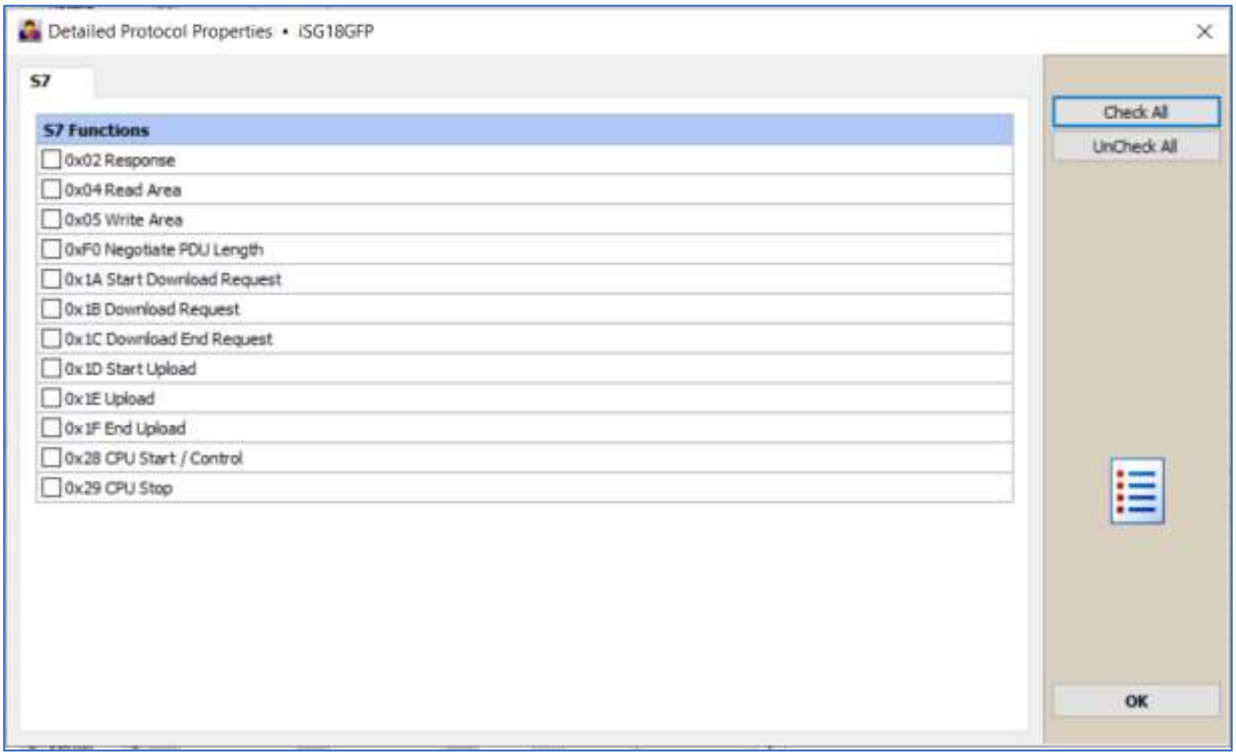
e. Under every specific functions variations, insert a decimal number for range. If Hex Values checkbox is selected, insert a hexadecimal number under each specific functions variations.

f. In the **ModBus Select Functions & Define Ranges** screen, click **OK** to save the firewall rules and verify that select functions & define ranges screen closes.

g. In the ModBus Detailed Protocol Properties screen, click **OK** to save all firewalls.

S7 Protocol

a. If one of the firewall rules is S7 protocol and detailed action is set, go to Action (see Figure 46 – Firewall Rules, Protocol) and click detailed DPI. S7 detailed protocol properties screen appears.



Detailed Protocol Properties • iSG18GFP

S7

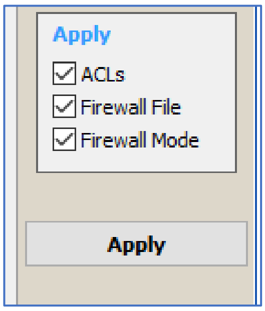
S7 Functions
- □ 0x02 Response
- □ 0x04 Read Area
- □ 0x05 Write Area
- □ 0xF0 Negotiate PDU Length
- □ 0x1A Start Download Request
- □ 0x1B Download Request
- □ 0x1C Download End Request
- □ 0x1D Start Upload
- □ 0x1E Upload
- □ 0x1F End Upload
- □ 0x28 CPU Start / Control
- □ 0x29 CPU Stop

Figure 68 – S7 Detailed Protocol Properties

b. Check/uncheck which functions of DPI detailed rules you want to apply to the firewall rules. If all functions are needed for the firewall rules, click **Check All** button. If you want to clear all functions, click **UnCheck All** button.

c. Click **OK** to save all firewall rules in **S7 Detailed Protocol Properties** Screen.

14. Go to # (see Figure 46 – Firewall Rules, Protocol) and check all rules to be applied to the firewall.
15. If GCE **ACLs** rules are needed to be applied, check if the **ACLs** checkbox is selected.
16. If ACE **Firewall Rules** are needed to be applied, check if the **Firewall File** checkbox is selected.
17. If **Firewall Mode** is needed to be changed, check if the **Firewall Mode** checkbox is selected.



Apply
- ☑ ACLs
- ☑ Firewall File
- ☑ Firewall Mode

Figure 69 – ACLs, Firewall Rules, and Firewall Mode Checkboxes

18. Click **Apply**.

6.5 Example of an IP firewall

Below is an example of configuration made by iDMS.

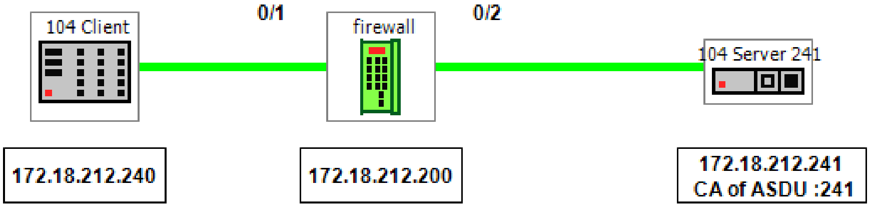


Figure 70 – Example of IP Firewall

1. Set VLAN for the service. Tag the target ports and the application firewall port Gi 0/4.

```
configure terminal

vlan 3500

port add Fa 0/1 untagged Fa 0/1

port add Fa 0/2 untagged Fa 0/2

port add Gi 0/4

exit
```

2. Create ACL to allow ARP between the stations.

```
mac access-list extended 1001

permit any 0x0806 priority 10

exit
```

3. Create ACL to allow ICMP between the stations.

```
ip access-list extended 1006

permit icmp any priority 10

exit
```

4. Create ACL to direct IEC 104 (destination TCP port 2404) traffic sourced from the Client towards the Server to the firewall (Gi 0/4).

```
ip access-list extended 2001

permit tcp host 172.18.212.240 host 172.18.212.241 eq 2404 priority 20 redirect interface Gi 0/4 sub-action modify-vlan 3500

exit
```

5. Create ACL to direct IEC 104 (source TCP port 2404) traffic sourced from the Server towards the Client to the firewall (Gi 0/4).

```
ip access-list extended 2003

permit tcp host 172.18.212.241 eq 2404 host 172.18.212.240 priority 30 redirect interface Gi 0/4 sub-action modify-vlan 3500
```

```
exit
```

6. Deny any other traffic at the Client and Server ports.

```
mac access-list extended 2998
deny any priority 250
exit
```

7. Place the ACLs on the Client port.

```
interface Fa 0/1
ip access-group 2001 in
ip access-group 1006 in
mac access-group 1001 in
mac access-group 2998 in
exit
```

8. Place the ACLs on the Server port.

```
interface Fa 0/2
ip access-group 2003 in
ip access-group 1006 in
mac access-group 1001 in
mac access-group 2998 in
exit
end
write startup-cfg
```

9. Create the firewall.rules file.

Done only in iDMS, not available in CLI

10. Import the firewall.rules file to the switch

```
firewall-rules import tftp://172.18.212.240/firewall.rules
```

11. Activate the firewall.rules file

```
application connect
firewall profile import filename firewall.rules
firewall tcp activate mode enabled
exit
```

6.6 Firewall Commands Hierarchy

```
+ root
        - learning-results-export {tftp://ip-address/filename | sftp://<user-name>:<password>@ip-address/filename | flash:filename}
        - firewall-rules import {tftp://ip-address/filename | sftp://<user-name>:<password>@ip-address/filename | flash:filename}
        + config terminal

                –   monitor session <name> source interface <type>/<ID>

                –   monitor session <name> destination interface gigabitethernet 0/4

+  application connect

+ learn-mode

        + mode

- set mode {none| count| matrix| log| log_matrix| count_matrix}

- set max_file_ram_size (bytes 999,<371-65535>)

- show

        - counters [show| clear}

        - file {create| export}

- show

- status show

+  firewall

+ profile

- show

- import filename <name>

- log {show [lines-to-show(1000,<>)] |clear}

+ tcp

- show

- counters [show| clear}

- activate mode {disabled | enabled | simulate| learn}

+ serial

+ modbus_gw

+ terminal-server
```

+ serial-tunnel

  - counters {clear| show}

  - dnp3 db {clear| show}

  - iec101 db {clear| show}

  - hash {clear| show}

  - modbus {clear| show}

- show

- activate service-id <id> mode {disabled | enabled | simulate}

6.7 Firewall Commands Description

Table 7 – Firewall Commands Description

Command	Description
learning-results-export	Export the file of the learning mode results to a TFTP/SFTP server or to the USB. The file should be ready in advance.
firewall-rules import	Import the firewall.rules file from a TFTP/SFTP server. The file should be created by iDMS and ready in advanced at the server to be downloaded.
configure terminal	
monitor session	When learning mode enabled, traffic mirroring is to be set. The source interfaces would be the ones where the service devices are connected at. The destination interface is always gigabitethernet 0/4.
application connect	Enter the industrial application menu.
Learn-mode	Access the learning mode.
mode	**Set mode:** Set how the learning results are presented. • Matrix - a table format. • Log - log format. • log_matrix - table and log. **Show:** information about current mode.
Counters	• **Show:** display counter values. • **Clear:** clear counters.
status show	Information about the learning mode operation state enabled | disabled.
firewall	• Enter the configuration mode for the Cellular application. • **Enable:** enable application. • **Disable:** disable application.

Command	Description
Profile	**Show:** indicates the file name used by the firewall. import filename <>: after the firewall.rules file was imported at the GCE ('firewall-rules import'), have it imported to the ACE firewall profile.
Log show	**show:** display the firewall log. **clear:** clears the log.
Tcp	**Show:** status of the firewall is displayed.
activate	**Mode:** • **Disabled:** firewall is disabled. Packets are not inspected. • **Enabled:** packets are inspected and blocked in case of violation. Violations are logged. • **Simulate:** packets are inspected but are not blocked in case of violations. Violations are logged. • **Learn:** learning mode is enabled. Traffic is learned to provide information on the service traffic.
Counters	**Show:** display counter values. **Clear:** clear counters.
Serial	
activate	**Service-id <>:** the serial service id number for which to enable the firewall on. Mode: • **Disabled:** firewall is disabled. Packets are not inspected. • **Enabled:** packets are inspected and blocked in case of violation. Violations are logged. • **Simulate:** packets are inspected but are not blocked in case of violations. Violations are logged.
serial-tunnel	
Counters	**Show:** display counter values. **Clear:** clear counters.
dnp3 db	**Show:** display the firewall database of the dnp3 serial tunneling service. **Clear:** clear the database.
iec101 db	**Show:** display the firewall database of the iec101 serial tunneling service. **Clear:** clear the database.
modbus	**Show:** display the firewall database of the Modbus serial tunneling service. **Clear:** clear the database.
Show	Status of the firewall is displayed.