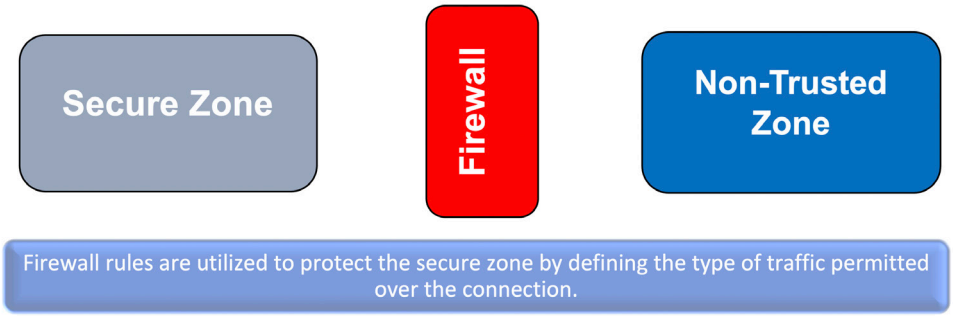
APPLICATION NOTE

Using the RAPTOR® as an ICS/SCADA Firewall

What is a Firewall?

A firewall is a network security device/system that monitors and controls the incoming and outgoing network traffic based on predefined security policies. A firewall typically establishes the barrier between a trusted network and an untrusted network.

Figure 1 - Basic Firewall Architecture



The Firewall used in Industrial Control System / SCADA Environments

Firewalls are a universal part of information technology and information security, especially when only one security measure is selected. Firewalls protect information by monitoring and controlling traffic flow between and within networks, using a set of Policy - access control lists (ACL) to filter traffic appropriately. This is true for industrial and enterprise firewalls, which are generally used alongside ICS/SCADA environments.

Industrial firewalls differ from enterprise firewalls in that they are strengthened for industrial environments, which can be pretty harsh. They rise to the occasion by having higher operating temperature thresholds -40°C to 85°C and robust electrical and mechanical design. For example, the RAPTOR meets the requirements of iEC61850-3 required for use in electric substations. There are also software differences with Industrial Firewalls, e.g. protocol support like SCADA, GOOSE and Modbus traffic and other industrial device's internal communication protocols.

Firewalls Types:

There are mainly three types of network firewalls:

1. Packet Filtering (stateless)
2. Stateful Firewall
3. Application firewall

Packet Filtering / Stateless Firewall

A packet filter, also known as a stateless firewall, analyzes individual network packets without concern for their context. Stateless firewalls decide to deny or allow packets depending on static filtering criteria. The most frequent criteria are:

- Source IP
- Destination IP
- Source protocol
- Destination protocol

The problem with stateless firewalls is that they are easy to spoof by the hacker, which is when the hacker changes their IP address to match an internal application server IP with a commonly used destination port number. Spoofing works because stateless firewalls cannot block inbound communication that does not result from outbound requests.

Stateful Firewall

A stateful firewall tracks the operating condition and the characteristics of the network connection that passes through it. The firewall is configured to classify legitimate packets for different types of connections.

A stateful firewall is cognizant of information exchange paths and can implement several IP Security (IPsec) functionalities, i.e. data encryption and tunnels. From a technical perspective, stateful firewalls can let you know whether a TCP connection is open, open sent, synchronized, synchronization acknowledge status, or established; it can also know if the MTU (Maximum Transmission Unit) has changed or whether packets have fragmented, and so on.

A stateful firewall usually would allow communications only when initiated from the secure zone unless there are exceptions set.

Stateful firewalls are used when connecting a secure zone to a non-secure zone and where zone boundaries can be defined.

Application Firewall

An application firewall is a form of firewall that controls traffic related to applications or services.

Application firewalls, or application layer firewalls, use configured policies to decide whether to allow or block communications to or from an application.

With the control of data flow to and from the CPU, traditional firewalls examine each packet it passes through. Taking it a step further, application firewalls control the execution of files or code by specific applications. That way, even if an intruder gains entry to a network or server, they cannot execute malicious code.

Application firewalls can be active or passive.

Active – Active application firewalls inspect all incoming requests—including the actual message being exchanged—against known vulnerabilities such as SQL injections, parameter and cookie tampering, and cross-site scripting. Only requests deemed "clean" are passed to the application.

Passive – Passive application firewalls act similarly to an intrusion detection system (IDS) in that they also inspect all incoming requests against known vulnerabilities, but they do not actively reject or deny those requests if a potential attack is discovered.

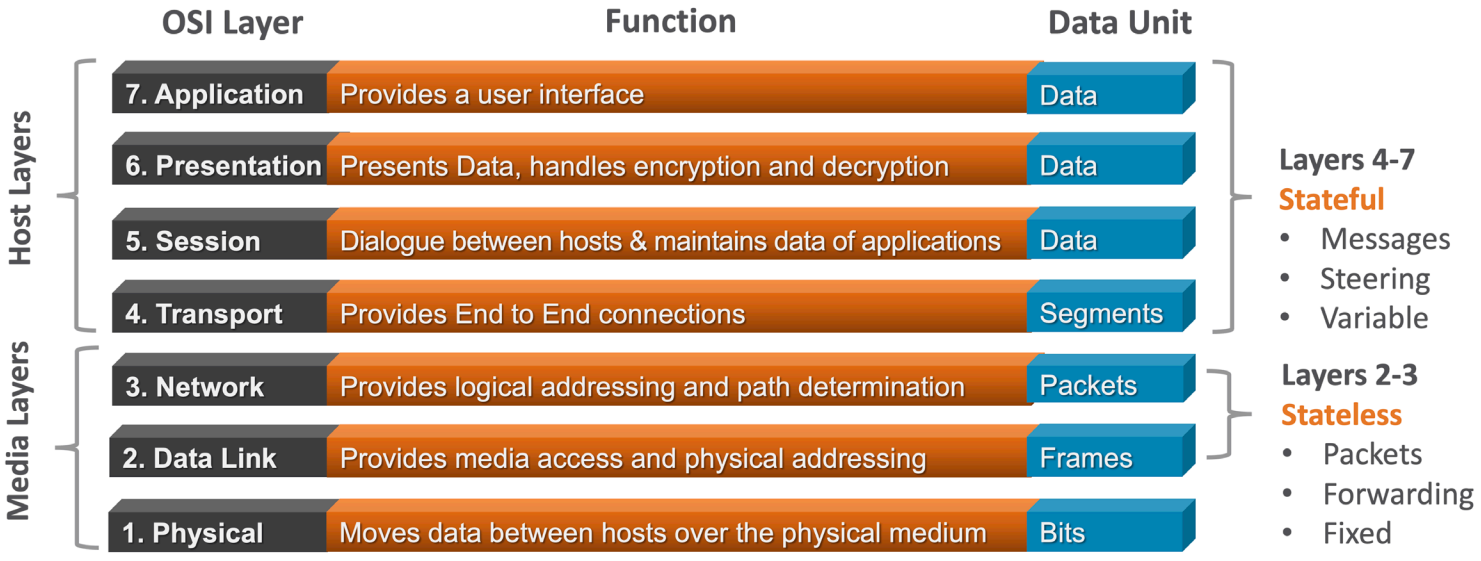
Application firewalls are generally remotely updateable, which allows them to prevent newly discovered vulnerabilities. They are often more up-to-date than specific security-focused code included in applications due to the more extended development and testing cycles required to include such code within applications.

Today, web application firewalls (WAFs) are commonly used to filter, monitor, and block HTTP/S traffic to and from a web application, specifically.

Stateless vs Stateful Firewalls – SCADA Network

To understand what is "state" we need to look at the specifics behind the TCP communication sessions most common in modern-day industrial control systems and SCADA applications. The figure below illustrates the model.

Figure 2 - The data communication layers typically used in TCP/IP communications for ICS and SCADA systems



Stateless vs Stateful firewall in the OSI Layers

RAPTOR iMX950 is an Intelligent Cyber Secure Platform running the iBiome® OS

Designed for future scalability and applications, its modular system of field-replaceable modules, hot-swappable power supplies, and its ability to run third-party software applications makes it a very flexible platform for today and the future.

The iBiome is an all-encompassing operating system that supports switching and routing on a single platform.

Protect and secure critical infrastructures in the harsh environments found in utility and substation applications.

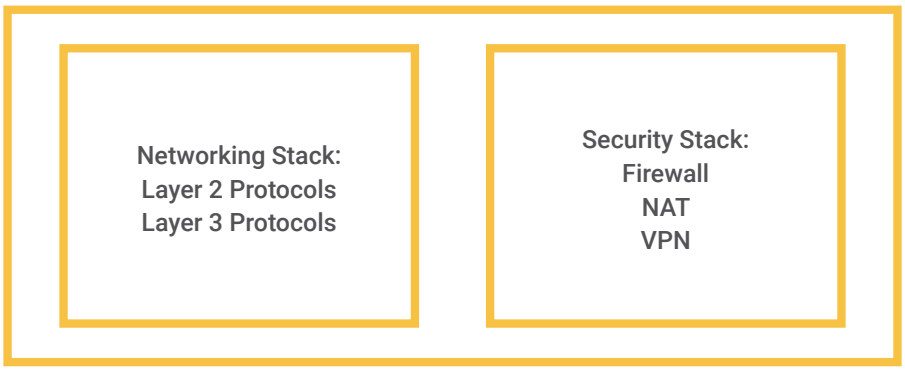
Standards set out in IEC 61850-3 and IEEE 1613 for utility communication equipment in substation environments.

It Supports **a Stateful Firewall, NAT and IPSec capabilities.**

Firewall Architecture on RAPTOR

Two networking stacks are running on the RAPTOR. These networking stacks are for Security and the other for networking protocols.

Figure 3 - *Networking Stacks on the RAPTOR*



Imagine that two routers are running on the RAPTOR hardware. The security networking stack provides **Firewall, NAT and VPN/IPSec** services, while the networking stack provides layer 2 and layer 3 protocols.

The RAPTOR iMX950 logical view, as shown below, when it is configured for firewall applications.

Figure 4 - *Logical view of the RAPTOR internals for the Firewall application*

RAPTOR Device Configuration:

Configuring the Security Application

The RAPTOR requires its internal security stack to be configured, which supports the Firewall application.

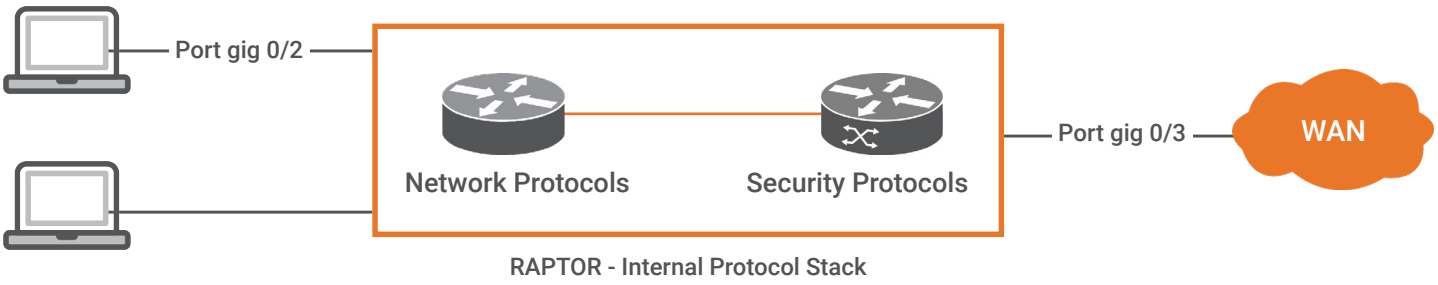
The security application must be configured to use firewall, NAT, and IPSec functionality.

To connect with the internal security stack of the RAPTOR iMX950, we need to create a virtual interface using backplane logical interface of second port of Slot 4 (10 GB Module Slot, 2nd port internal connection and we do not require a 10G module installed in slot 4).

The configuration of the RAPTOR Firewall takes place in two steps:

1. Configuration of connectivity between the RAPTOR Networking and the Security Applications
2. Configuration of the firewall filters

Figure 5 - *RAPTOR- iMX950 Internals for Firewall*



For the configuration example, the following port configuration is in place:

- VLAN 2: interface gigabitethernet 0/2
- WAN port: interface gigabitethernet 0/3
- VLAN 50: interface extreme-ethernet 0/2

1. Login to the RAPTOR as an admin-level user.

NOTE: The prompt may be different if the switch defaults have changed.

The following prompt appears.

iS5com#

2. Establish a VLAN which will later be used between the networking and security applications.

   a. Execute the following commands:

   iS5Comm# configure terminal

   iS5Comm(config)# vlan 50

   iS5Comm(config-vlan)# port add ex 0/2

   iS5Comm(config-vlan)# vlan active

iS5Comm(config-vlan)# exit

iS5Comm(config)# exit

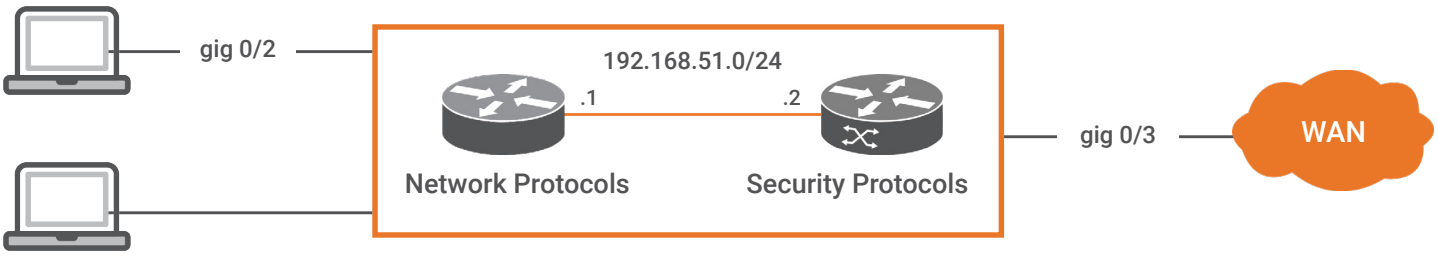
iS5Comm# show vlan id 50

NOTE: For the security application, the port ex 0/2 used

```
iS5Comm# sh vlan id 50

Vlan database
-------------
Vlan ID                 : 50
Member Ports            : Ex0/2
Untagged Ports          : None
Forbidden Ports         : None
Name                    :
Status                  : Permanent
Egress Ethertype        : 0x8100
Service Loopback Status    : Disabled
------------------------------------------------------

iS5Comm#
```

3. Set the IP interfaces for Network and Security applications, and enable the security application. The cybsec command informs the RAPTOR to associate the IP address with the Security Application rather than the networking application.

   The IP scheme for Security configuration:



   a. Execute the following commands:

   iS5Comm# configure terminal

   iS5Comm(config)# set security enable

   iS5Comm(config)# interface vlan 50

   iS5Comm(config-if)# ip address 192.168.51.1 255.255.255.0

   iS5Comm(config-if)# ip address 192.168.51.2 255.255.255.0 cybsec

   iS5Comm(config-if)# no shutdown

   iS5Comm(config-if)# ip proxy-arp cybsec

   iS5Comm(config-if)# exit

   iS5Comm(config)# exit

   iS5Comm# show running-config cybsec

```
iS5Comm# sh running-config cybsec

#Building configuration...
!
!
set security enable
!
```

b. iS5Comm# show running-config vlan 50

```
iS5Comm# show running-config vlan 50

#Building configuration...
!
switch  default
vlan 50
 ports extreme-ethernet 0/2
vlan active
!
end
iS5Comm#
```

c. iS5Comm# show running-config interface vlan 50

```
iS5Comm# sh running-config interface vlan 50

#Building configuration...
!
interface vlan 50
ip address  192.168.51.1 255.255.255.0
no shutdown
!
!
 interface vlan 50
  ip address  192.168.51.2 255.255.255.0 cybsec
  no shutdown
  ip proxy-arp cybsec
!
end
iS5Comm#
```

4. Set up a default route between the networking application and the security application. It could also be viewed as a default route to the WAN interface.

   a. Set up a default route on the Networking application to send traffic to the Security interface.

   iS5Comm# configure terminal

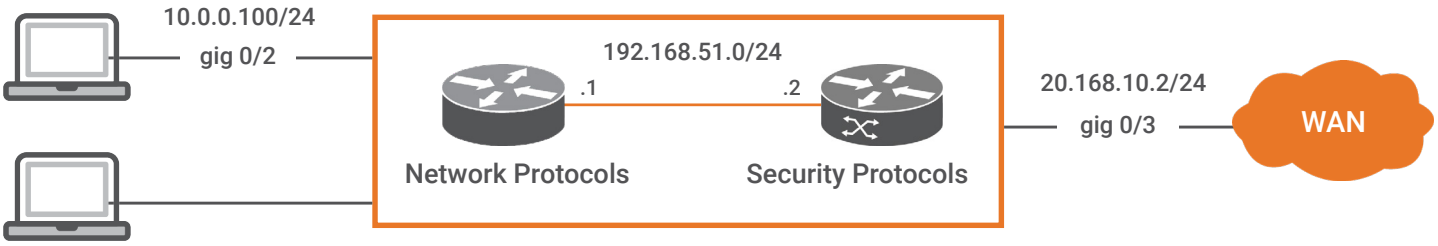
   iS5Comm(config)# ip route 0.0.0.0 0.0.0.0 vlan 50

   iS5Comm(config)# exit

   iS5Comm# show ip route

```
iS5Comm# sh ip route

Codes: C - connected, S - static, R - rip, B - bgp, O - ospf, I - isis, E - ECMP

IA - OSPF inter area, N1 - OSPF NSSA external type 1,
N2 - OSPF NSSA external type 2, E1 - OSPF external type 1,
E2 - OSPF external type 2 L1 - ISIS Level1, L2 - ISIS Level2, ia - ISIS Inter Ar
ea


Vrf Name:           default
---------
S 0.0.0.0/0  is directly connected, vlan50
C 192.168.10.0/24 is directly connected, vlan1
C 192.168.51.0/24 is directly connected, vlan50

iS5Comm#
```

5. Create an IP interface for the WAN. This can be a routed port or a VLAN IP interface. The network IP assignment is now as shown in the following image:



a. Execute the following:

iS5Comm# configure terminal

iS5Comm(config)# interface gigabitethernet 0/3

iS5Comm(config-if)# shutdown

iS5Comm(config-if)# no switchport

iS5Comm(config-if)# ip address 20.168.10.2 255.255.255.0 cybsec

iS5Comm(config-if)# no shutdown

iS5Comm(config-if)# description “WAN Port”

iS5Comm(config-if)# set wan enable

iS5Comm(config-if)# exit

iS5Comm(config)# exit

iS5Comm# show running-config ip

```
iS5Comm# sh running-config interface gigabitethernet 0/3

#Building configuration...
!
interface gigabitethernet 0/3
shutdown
 mac-addr e8:e8:75:90:6e:44
 description "WAN Port"
 shutdown
 no switchport
 no shutdown
no shutdown
!
!
 interface gigabitethernet 0/3
  ip address  20.168.10.2 255.255.255.0 cybsec
  no shutdown
  set wan enable
!
end
iS5Comm#
```

6. Configure a local network port and address.

   a. Execute the following commands:

   iS5Comm# configure terminal

   iS5Comm(config)# interface gigabitethernet 0/2

   iS5Comm(config-if)# shutdown

   iS5Comm(config-if)# no switchport

   iS5Comm(config-if)# ip address 10.0.0.100 255.255.255.0

   iS5Comm(config-if)# no shutdown

   iS5Comm(config-if)# exit

   iS5Comm(config)# exit

7. Establish a route between the network port and the security application.

   a. Execute the following commands:

   iS5Comm# configure terminal

   iS5Comm(config)# ip route 10.0.0.0 255.255.255.0 192.168.51.1 cybsec

   iS5Comm# exit

   iS5Comm# show running-config ip

```
iS5Comm# sh running-config ip

#Building configuration...
!
ip route 0.0.0.0  0.0.0.0  vlan 50
ip route 10.0.0.0  255.255.255.0 20.168.10.2
interface gigabitethernet 0/2
shutdown
 mac-addr e8:e8:75:90:6e:43
 shutdown
 no switchport
 no shutdown
ip address  10.0.0.100 255.255.255.0
no shutdown
!
interface gigabitethernet 0/2
interface gigabitethernet 0/3
shutdown
 mac-addr e8:e8:75:90:6e:44
 shutdown
 no switchport
 no shutdown
no shutdown
!
interface gigabitethernet 0/3
interface vlan 1
ip address  192.168.10.1 255.255.255.0
no shutdown
!
interface vlan 50
ip address  192.168.51.1 255.255.255.0
no shutdown
!
!
 interface vlan 50
  ip address  192.168.51.2 255.255.255.0 cybsec
  no shutdown
  ip proxy-arp cybsec
!
!
 interface gigabitethernet 0/3
  ip address  20.168.10.2 255.255.255.0 cybsec
  no shutdown
  set wan enable
!
end
iS5Comm#
```

The iMX950 has been configured to support a WAN interface and a local interface. Routing has been enabled between these interfaces - Network and Security stack. The RAPTOR is now ready for advanced security applications such as Firewall, NAT, and IPSec.

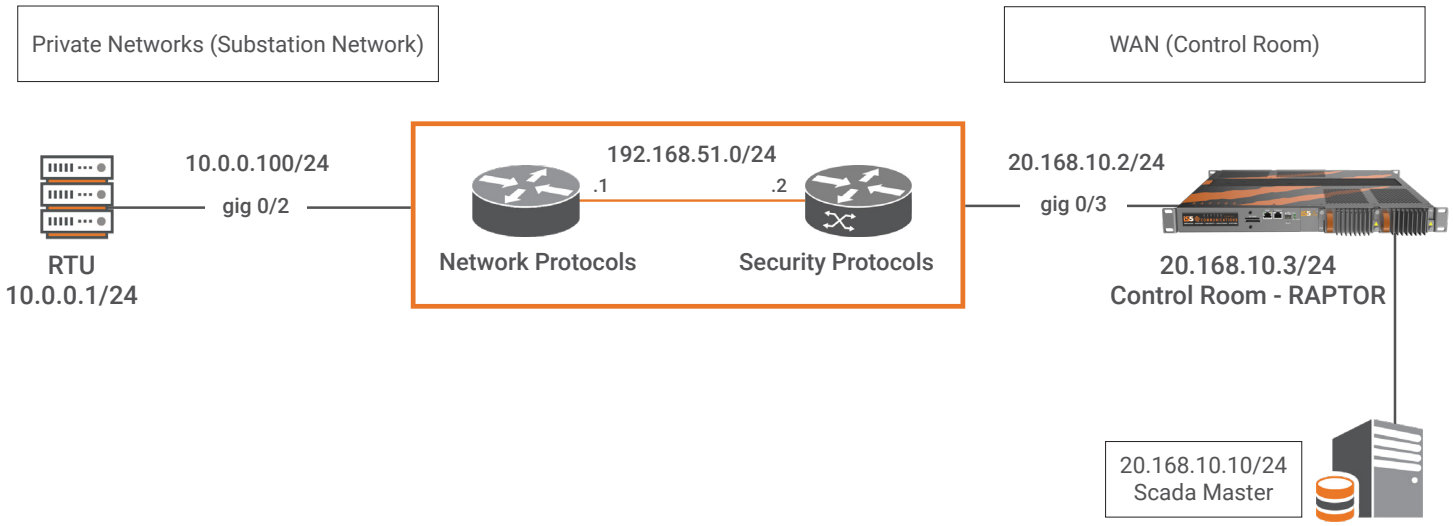
How to configure a simple Firewall

The steps needed to enable the iMX950 security features must have been performed. This document assumes that the steps listed in the **Configuring the Security Application** section were performed.

This section will begin by enabling a simple firewall. Once enabled, rules and complexity will be added as a means of providing a greater understanding of how to use the iMX950s firewall capabilities.

The LAB network diagram that will be used for these exercises will be as shown:

Figure 6 - *LAB Network Diagram for Basic Firewall Configuration*



1. From a host/RTU device on interface gig 0/2, you should be able to ping a host/ devices on the network at gig 0/3.

   a. Control Room RAPTOR switching configuration

   !

   interface vlan 1

   ip address 20.168.10.3 255.255.255.0

   no shutdown

   !

   ip route 10.0.0.0 255.255.255.0 20.168.10.2

   b. From a host/RTU (10.0.0.1) ping 20.168.10.3

   C:\>ping 20.168.10.3

   Pinging 20.168.10.3 with 32 bytes of data:

   Reply from 20.168.10.3: bytes=32 time=3ms TTL=128

   Reply from 20.168.10.3: bytes=32 time=1ms TTL=128

   Reply from 20.168.10.3: bytes=32 time=1ms TTL=128

   Reply from 20.168.10.3: bytes=32 time=1ms TTL=128

   Result: The pings succeed.

2. Enable the Firewall.
   a. Execute the following commands:

   iS5comm# configure terminal

   iS5comm(config)# firewall

   iS5comm(config-firewall)# enable

   iS5comm(config-firewall)# rule blockall deny any any any priority 20

   iS5comm(config-firewall)# access-group from_wan in blockall interface gigabitethernet 0/3

   iS5comm(config-firewall)# exit

   iS5comm(config)# exit

   iS5comm# show run firewall

```
iS5Comm# sh run firewall

#Building configuration...
!
firewall
 enable
 rule blockall deny any any any priority 20
 access-group from_wan in blockall interface gigabitethernet 0/3
!
end
iS5Comm# `
```

3. Test the firewall from the outside to the inside.
   a. Ping from the 20.168.10.0/24 subnet to 10.0.0.100
   b. Step Result: The pings will fail
4. Disable the firewall and repeat Step 3.

   Execute these commands

   iS5comm# configure terminal

   iS5comm(config)# firewall

   iS5comm(config-firewall)# disable

   iS5comm(config-firewall)# exit

   iS5comm(config)# exit

   a. Now ping from the 20.168.10.0/24 subnet to 10.0.0.1
   b. Result: The pings will succeed
5. Reenable the firewall and verify that pings can pass from the Private Network to the WAN.
   a. Execute these commands

   iS5comm# configure terminal

   iS5comm(config)# firewall

   iS5comm(config-firewall)# enable

iS5comm(config-firewall)# exit

iS5comm(config)# exit

b. Ping from the inside host IP 10.0.0.1/24 subnet to 20.168.10.0/24 subnet

C:\>ping 20.168.10.3

Pinging 20.168.10.3 with 32 bytes of data:

Reply from 20.168.10.3: bytes=32 time=2ms TTL=62

Reply from 20.168.10.3: bytes=32 time=1ms TTL=62

Reply from 20.168.10.3: bytes=32 time=1ms TTL=62

Reply from 20.168.10.3: bytes=32 time=2ms TTL=62

Result: The pings succeed.

The priority of the rules are important. As soon as a packet is denied it will be discarded. The lower the number, the higher the priority.

6. Add a rule to permit a host / Device (RAPTOR) on the WAN side to ping the inside host/device (RTU)

   a. Execute the following commands

   iS5comm# configure terminal

   iS5comm(config)# firewall

   iS5comm(config-firewall)# rule from_switch permit 20.168.10.3/32 any any priority 2

   iS5comm(config-firewall)# access-group from_wan in from_switch,blockall interface gigabitethernet 0/3

   iS5comm(config-firewall)# exit

   iS5comm(config)# exit

   iS5comm#show running-config firewall

```
iS5Comm# sh running-config firewall

#Building configuration...
!
firewall
 enable
 rule blockall deny any any any priority 20
 rule from_switch permit 20.168.10.3/32 any any priority 2
 access-group from_wan in from_switch,blockall interface gigabitethernet 0/3
!
end
iS5Comm#
```

7. Ping from the host 20.168.10.3 can ping the 10.0.0.0/24 subnet.

   Result: The pings will be successful.

8. Ping from any host on 20.168.10.0/24 except 20.168.10.3 to the 10.0.0.0/24 subnet.

   Ping from 20.168.10.10 to 10.0.0.1

   Result: The pings will fail.

9. Show command.

   iS5comm# **sh firewall access-group**

```
iS5comm# sh firewall  access-group

                  Firewall Access Groups
                  ----------------------
Access                                  Rule
Group    Interface    Direction    Combination
-------  ----------   ---------   ---------------------
from_wan Gi0/3          in        from_switch blockall
iS5comm#
```

   iS5comm# **sh firewall rule all**

```
iS5comm# sh firewall rule all

                          Firewall Rules
                          --------------
Rule    Prot/   Source              Destination       Src      Dest     Pkt Hit
Name    Action   Address             Address          port     port     Count
------ ------ ------------        -------------     ------   ------   ---------
blockallany/D  0.0.0.0/0           0.0.0.0/0          >1       >1       16
from_switchany/P  20.168.10.3/32      0.0.0.0/0           >1       >1       294
iS5comm#
```

   iS5comm# sh firewall counters

```
iS5comm# sh firewall counters

Rule      Proto/  Access          Source            Destination       Pkt Hit
Name      Action  Group   Bound   Address           Address           Count
------    ------  -------  ------ -----------       -------------     -----------
from_switchany/P   from_wanIN     20.168.10.3/32     0.0.0.0/0         295
blockall any/D   from_wanIN     0.0.0.0/0          0.0.0.0/0         16
iS5comm#
```

CONCLUSION

This application note has provided an overview of firewall usage in industrial control systems, and has explained how to configure the RAPTOR stateful inspection firewall, including:

- Enabling the Firewall
- Applying policies to inbound traffic
- Applying policies to outbound traffic
- Prioritizing rules
- Executing commands to show the state of the Firewall

ABOUT iS5 COMMUNICATIONS INC.

iS5 Communications Inc. (“iS5Com”) is a global provider of integrated services and solutions, and manufacturer of intelligent Industrial Ethernet products. Our products are designed to meet the stringent demand requirements of utility sub-stations, roadside transportation, rail, and industrial applications. iS5Com’s services and products are key enablers of advanced technology implementation such as the Smart Grid, Intelligent Transportation Systems, Intelligent Oil Field, and Internet of Things. All products have the ability to transmit data efficiently without the loss of any packets under harsh environments and EMI conditions.

iS5 COMMUNICATIONS

SERVICES • SUPPORT • SECURITY • SOLUTIONS • SYSTEMS

For more information, visit: is5com.com

toll free: +1-844-520-0588 | fax: +1-289-401-5206 | info@is5com.com
technical support: +1-844-475-8324 | support@is5com.com
Address: 5895 Ambler Dr, Mississauga, ON L4W 5B7