]HackingTeam[

Remote Control System

Technical Requirements

Revision	Author (s)	Release Date
2.2.3	FAE Team	2013, October 31th

Contents

1 Objectives

The present document details requirements needed for Galileo installation.

The document includes:

- Galileo architecture high level overview
- Galileo hardware specifications
- Galileo network configuration

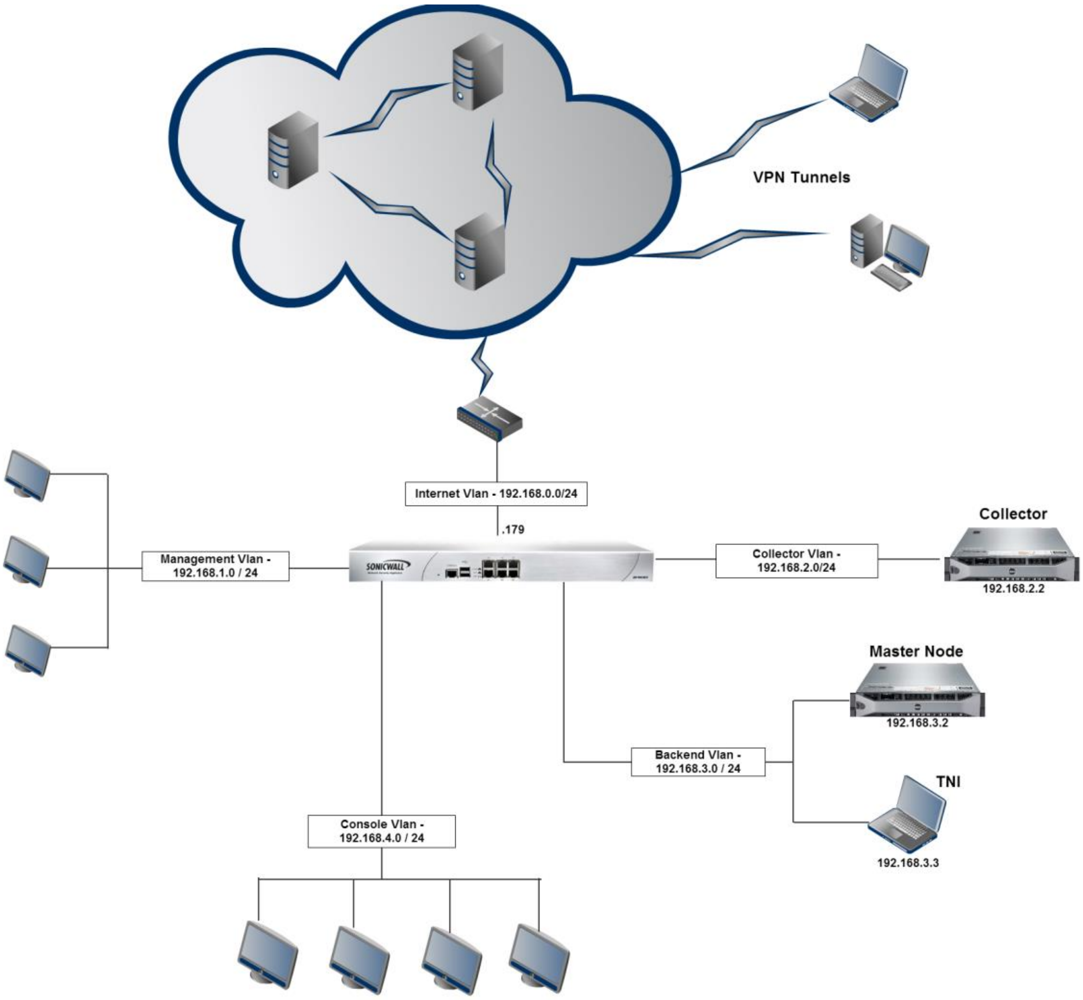
2 Environment

2.1 Requirements

The following system requirements must be present:

1. Rack cabinet
2. KVM or separated items (monitor + USB keyboard + USB mouse)
3. UPS and power strips to cover all production systems
4. Network switch and Firewall as specified in the Hardware Requirements section
5. Wired high-speed Internet connection with Static public IP Address

2.2 Network Diagram


VPN Tunnels
Internet Vlan - 192.168.0.0/24
.179
Collector
Collector Vlan - 192.168.2.0/24
192.168.2.2
Management Vlan - 192.168.1.0 / 24
SONICWALL
Master Node
192.168.3.2
Backend Vlan - 192.168.3.0 / 24
TNI
192.168.3.3
Console Vlan - 192.168.4.0 / 24

3 Hardware Requirements

3.1 Master Node

Masternode is the central server implementing system core features. It manages all other components and is directly accessed by the Console. It also implements core database functionalities.

3.1.1 System Requirements

The following must be present:

1. 96 GB of RAM minimum
2. 2 x 146GB SAS HD RAID1 (for O.S.)
3. 4 x 600GB SAS HD RAID 10 (for data)
4. Windows Server 2008 R2 SP1 Enterprise Edition 64 Bit (English)

3.1.2 Disk Configuration

The following table details how disks must be configured:

Qty	Disk	RAID	Partitioning	Notes
2	146 GB	RAID 1	NTFS, single partition	Install O.S. here
4	600 GB	RAID 10	NTFS, single partition	Mount as C:\RCS

3.1.3 Suggested Hardware Specifications

Below you can find a recommended hardware configuration for Master Node.

Dell PowerEdge R720
CPU : Intel Xeon E5-2660 2.20Ghz, 20MB Cache
RAM : 12 x 8GB RDIMM, 1600Mhz
HD (OS) : 2 x 146GB SAS 6Gbps 15k 2.5” HD Hot Plug (RAID1)
HD (Data) : 4 x 600GB SAS 6Gbps 10k 2.5” HD Hot Plug (RAID10)
RAID : PERC H710p Integrated RAID Controller
Network : Broadcom 5720 QP 1Gb Network Card
Optical : 16X DVD+/-RW Drive SATA

3.1.4 Additional Configurations

Enable the NTP Synchronization towards the NTP server on the Collector.

3.2 Shard

Shard is an additional module needed to add database power to the system. It is hot-pluggable and its workload is automatically balanced by the Masternode.

NOTE: This is an optional module and can be skipped according to customer’s license.

3.2.1 System Requirements

The following must be present according to the purchased license:

1. 96 GB of RAM minimum
2. 2 x 146GB SAS HD RAID1 (for O.S.)
3. 4 x 600GB SAS HD RAID 10 (for data)
4. Windows Server 2008 R2 SP1 Enterprise Edition 64 Bit (English)

3.2.2 Disk Configuration

The following table details how disks must be configured:

Qty	Disk	RAID	Partitioning	Notes
2	146 GB	RAID 1	NTFS, single partition	Install O.S. here
4	600 GB	RAID 10	NTFS, single partition	Mount as C:\RCS

3.2.3 Suggested Hardware Specification

Below there is a recommended hardware configuration for Shard.

Dell PowerEdge R720
CPU : Intel Xeon E5-2660 2.20Ghz, 20MB Cache
RAM : 12 x 8GB RDIMM, 1600Mhz
HD (OS) : 2 x 146GB SAS 6Gbps 15k 2.5” HD Hot Plug (RAID1)
HD (Data) : 4 x 600GB SAS 6Gbps 10k 2.5” HD Hot Plug (RAID10)
RAID : PERC H710p Integrated RAID Controller
Network : 2 x Broadcom 5720 QP 1Gb Network Card
Optical : 16X DVD+/-RW Drive SATA

3.2.4 Additional Configurations

Enable the NTP Synchronization towards the NTP server on the Collector.

3.3 Collector

Collector is the infrastructure endpoint on the internet. It is contacted by agents and is responsible to gather their collected evidences and forward them to the Masternode. A collector must be attached with an Anonymizer to prevent its IP address disclosure.

3.3.1 System Requirements

The following must be present:

1. 16 GB of RAM minimum
2. 2 x 300GB SAS HD RAID1 (for O.S. and data)
3. Windows Server 2008 R2 SP1 Standard Edition (or above) 64 Bit (English)

3.3.2 Disk Configuration

The following table details how disks must be configured:

Qty	Disk	RAID	Partitioning	Notes
2	300 GB	RAID 1	NTFS, single partition	Install O.S. here

3.3.3 Suggested Hardware Specifications

Below you can find a recommended hardware configuration for Collector.

Dell PowerEdge R210 II
CPU : Intel Xeon E3-1230 3.20Ghz, 8MB Cache
RAM : 2 x 8GB DDR3, 1333Mhz
HD (OS) : 2 x 300GB SAS 6Gbps 15k 2.5” HD Hot Plug (RAID1)
RAID : PERC H200 RAID Controller
Network : 2 x Broadcom 5720 QP 1Gb Network Card
Optical : 16X DVD+/-RW Drive SATA

3.3.4 Additional Configurations

Enable the NTP Synchronization towards the closest public NTP server.

3.4 Anonymizer

The Anonymizer is a component which prevents the disclosure of the Collector IP address.

3.4.1 Virtual Private Server

The Anonymizer software must run on a server deployed on the Internet with a public static IP address. The best way to provide yourself with such requirement is renting a Virtual Private Server (VPS) from an online provider. In paragraph 3.4.3 a suggested list of VPS provider is given.

3.4.2 System Requirements

The following must be present on the VPS:

1. 256 MB of RAM minimum
2. 10GB HD
3. Linux CentOS 6 32 Bit
4. Static public IP address
5. 2 Mbit/s Internet connection

NOTE: Due to company policies and to protect customer’s confidentiality requirements, Hacking Team is not allowed to provide accounts on VPS services.

3.4.3 Suggested VPS List

The following table list examples of possible VPS providers:

Name	Web site	Locations
Linode	http://www.linode.com	USA and many other locations
Host Europe	http://www.hosteurope.de	Germany and other locations

3.5 Console

The Console is used by operators as a point of access to the entire system. It connects directly to the Masternode, but all components can be managed using the Console. It can be installed on any personal Windows laptop.

NOTE: A VPN connection is suggested when connecting to Master Node from external network.

3.5.1 System Requirements

The following must be present:

1. 4 GB of RAM minimum
2. 320GB SATA HD
3. Windows or OS X
4. Display capable of 1280x800 pixel minimum resolution

3.5.2 Suggested Hardware Specifications

Below you can find a recommended hardware configuration for Console.

Dell PowerEdge R210 II
CPU : Intel Core i3-3120M 2.50Ghz, 3MB Cache
RAM : 1 x 4GB DDR3, 1600Mhz
HD : 1 x 320GB SATA 7.2k 2.5” HD
Video : Intel HD Graphics 4000
Network : 1 x 1Gb Network Card, 1 x Dell Wireless 1901 802.11 a/b/g/n
Optical : 8X DVD+/-RW Drive SATA

3.5.3 Additional Configurations

Adobe Air runtime must be installed on the system (download it from get.adobe.com/air)

3.6 Backup

NOTE: The backup unit is a SAN (Storage Area Network) or a NAS (Network Attached Storage) device that is responsible for all data backup.

3.6.1 System Requirements

The following must be present:

1. 64 GB of RAM minimum
2. 6 x 1TB SAS HD RAID6 (for data)

3.6.2 Disk Configuration

The following table details how disks must be configured:

Qty	Disk	RAID	Partitioning	Notes
6	1 TB	RAID 6	NTFS, single partition	Mount as Z:\

3.6.3 Suggested Hardware Specifications

Below you can find a recommended hardware configuration for backup unit.

DELL PowerVault MD3200i
HD : 6 x 1TB SAS 6Gbps 7.2k HD Hot Plug

3.7 Firewall

3.7.1 System Requirements

The following must be present:

1. Support for VPN connection client to site (SSL or IPSEC)
2. Stateful throughput of 1 Gbps
3. IMIX performance of 235 Mbps
4. Maximum connections of 225000
5. VPN throughput of 300 Mbps

3.7.2 Suggested Hardware Specifications

Below you can find a recommended hardware configuration for firewall.

SonicWall NSA 2400MX Network Security Appliance
IPSEC VPN Connections Client to Site: Up to 10
Stateful Throughput: 775 Mbps
IMIX Performance: 235 Mbps
Maximum Connections: 225000
VPN Throughput: 300 Mbps

3.8 Switch

3.8.1 System Requirements

The following must be present:

1. 24 ports
2. Support for 10/100/1000 Mbps

3.8.2 Suggested Hardware Specifications

Below you can find a recommended hardware configuration for the switch.

Dell PowerConnect 2800
Ports : 24 at least
Speed: 10/100/1000 Mbps

4 Network Configuration

4.1 VLANs Configuration on Switch

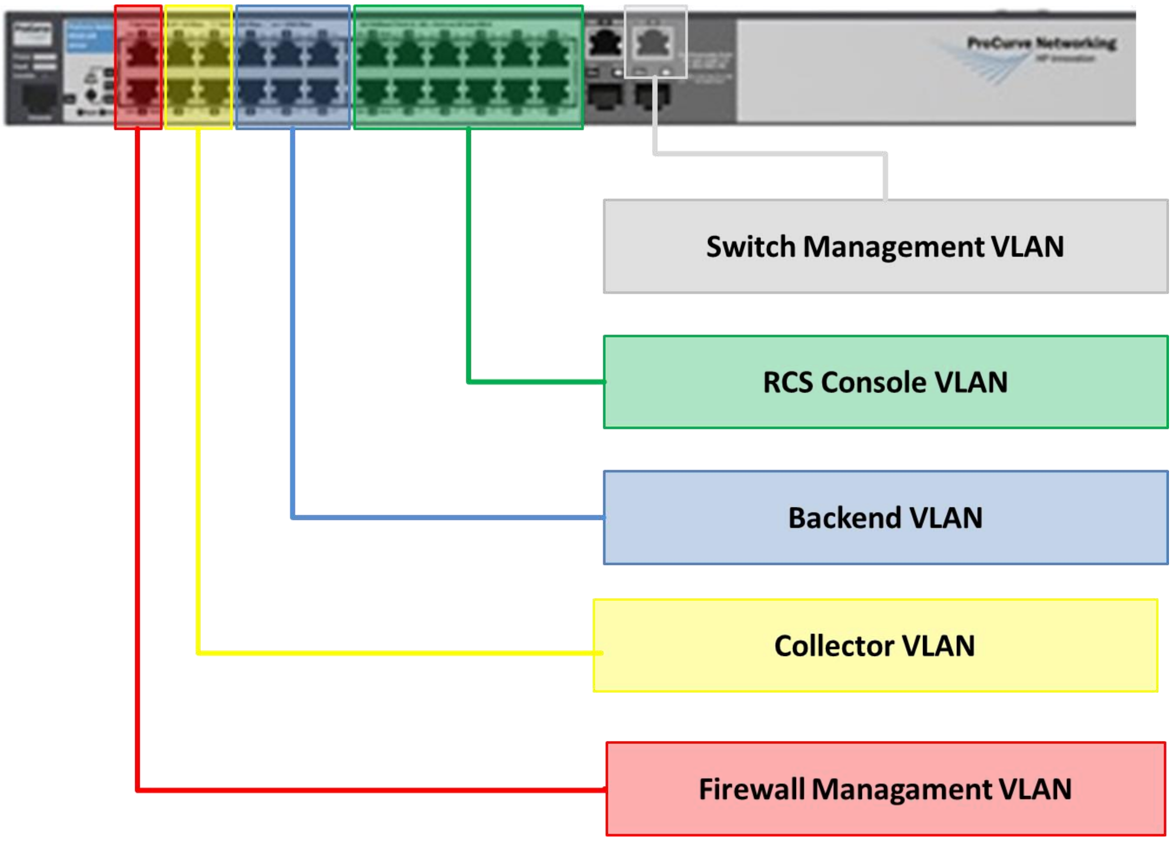
The environment requires 5 VLANs on a switch.

These VLANs create different logical LAN for each component and for devices management.

On the switch you can create there VLANs:

- Backend VLAN
- Collector VLAN
- Console VLAN
- Firewall Management VLAN
- Switch Management VLAN

The assigned ports on the switch for each VLAN could be 2 or more, depending on the architecture.



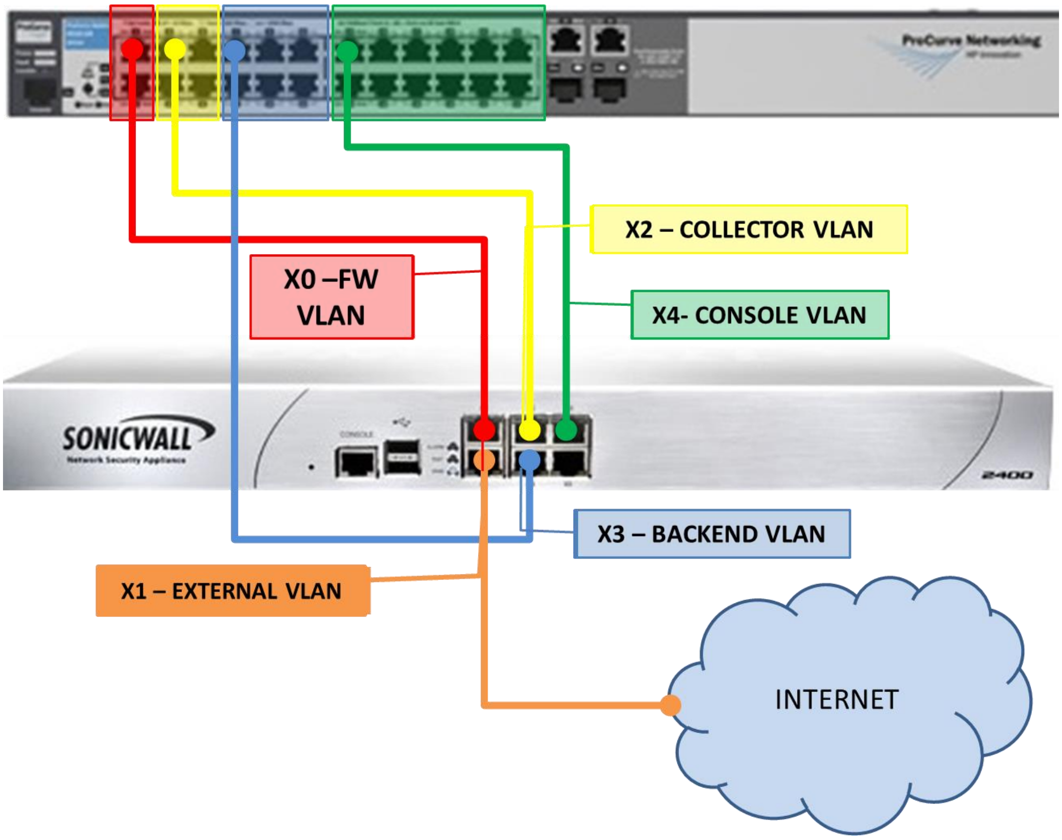
4.2 Firewall → Switch Interconnection

The firewall is used to regulate communication between VLANs.

Five zones are configured on the firewall:

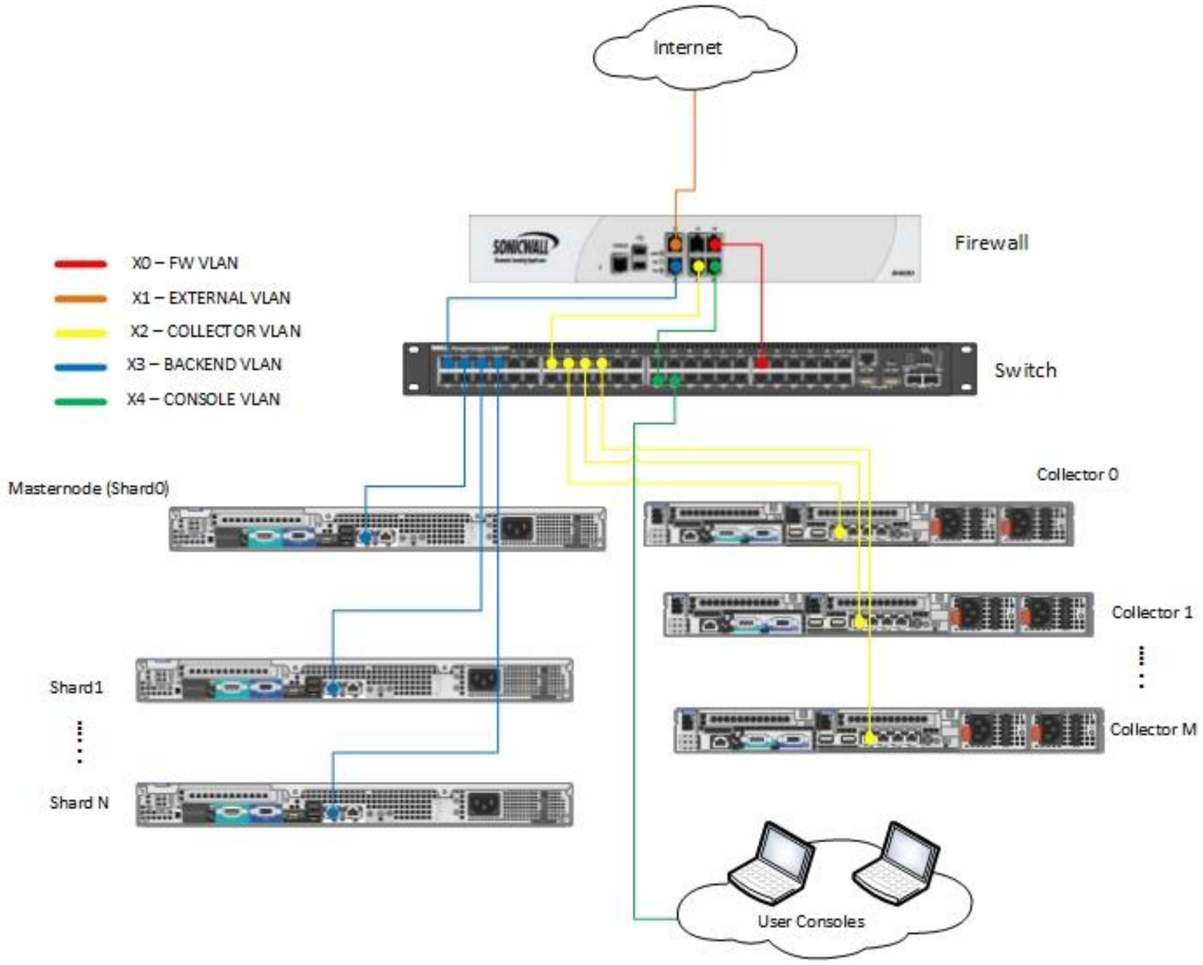
- Backend VLAN
- Collector VLAN
- Console VLAN
- Firewall Management VLAN
- External VLAN (Internet)

Zones on the firewall and VLANs on the switch must be connected according to the picture below.



4.3 Hardware Interconnection Schema

Following is represented the whole system architecture with its interconnections. As described in the picture, final infrastructure may include additional Collectors and Shards.



4.4 Firewall Rules Setup

The following rules must be implemented on the firewall to allow the system to work correctly.

Table's colors reflect the colors used in previous pictures.

Source	Destination	Service	Protocol	Port
Backend	Any	DNS	UDP	53
Backend	Any	NTP	UDP	123
Backend	TNI	HTTPS	TCP	443
Backend	Collector	HTTPS	TCP	443
Backend	Collector	HTTP	TCP	80
Console	Any	HTTPS	TCP	443
Console	Any	HTTP	TCP	80
Console	Any	DNS	UDP	53
Console	Any	ICMP	ICMP	
Console	Collector	RDP	TCP	3389
Console	Backend	RDP	TCP	3389
Console	Backend	HTTPS	TCP	443
Console	Backend	TCP_444	TCP	444
Collector	Any	DNS	UDP	53
Collector	Any	HTTP	TCP	80
Collector	Any	HTTPS	TCP	443
Collector	Any	NTP	UDP	123
Collector	Backend	HTTPS	TCP	443
Anonymizer(s)	Collector	HTTP	TCP	80