Generic Monitoring platform
Cyber aspects for solution's High Level Design

Contents

1 Introduction

1.1 Purpose

The purpose of this document is to describe the Cyber aspects of a NagiOs based NOC monitoring system, that is going to be used as centralized platform to monitor the systems installed on customer's premises.

The document describes potential threats and the methods to reduce the risk of inter-network connectivity between customers' sites, and between customers to the NOC network.

This document was written where the leading assumption is that cyber security is well defined and control at the organization that implements this monitoring solution, there for deals with the required aspects of interconnecting networks for the sole purpose of monitoring and maintenance.

1.2 Abbreviations

Term	Description
AAA	Authentication, Authorization, and Accounting
ACL	Access List
DOS	Denial of Service
DDoS	Distributed Denial of Service
FW	Firewall
IT	Information Technologies
OT	Operations Technologies
OSS	Operations Support System
NOC	Network Operations Center
SIEM	Security Information & Event Management
SNMP	Simple network Monitoring Protocol
SOC	Security Operations Center

1.3 Document History

Version	Modifications	Editor	Date
Earlier Drafts		Roee Besser	
0.5	•		

2 Functional Requirements

A monitoring system was designed to allow a ... its products installed at their customers' premises. The monitoring ... qiOs system that is based on SNMP and tailored add-ons th... ...es being monitored.

The system should be secured ir... ... one costumer, mistakenly can ac... interconnection between ...

2.1 Basic Net...

1. NOC an... ...y designated clients will be ab... ...he system's GUI.
2. NC... ...at only designated clients will ... to display the system's CLI.
3. ...way that accessing the slave servers ... or transferring files will be through the ...

...separated in a way that only a designated slave ...y ...oe able to connect with each other via the OPS ...

...ot be accessible for each other via the OPS network. ...OC network to customer's sites.

2.2 ...aration and segmentation

1. ...own subnet.
2. O... ...its own subnet.
3. Nagi... Slaves servers for designated customer shall be using its dedicated subnet.
4. NagiOs Master server will be connected to all customers' subnets.
5. Segmentation between subnets will be done over L2 Vlans

2.3 Access control

Initial solution is based on usernames and passwords configured within the various systems themselves. Later phases can be integrated with external AAA or LDAP solutions to authenticate individual and specific users.

2.4 Used protocols

1. HTTPS, SSL and SCP for NagiOs GUI to Master server.
2. Proprietary NagiOs protocols, SSH, SCP and SNMP between Master and slaves servers.
3. SNMP, SSL and SCP between Slaves servers and monitored devices (over VPN tunnels).

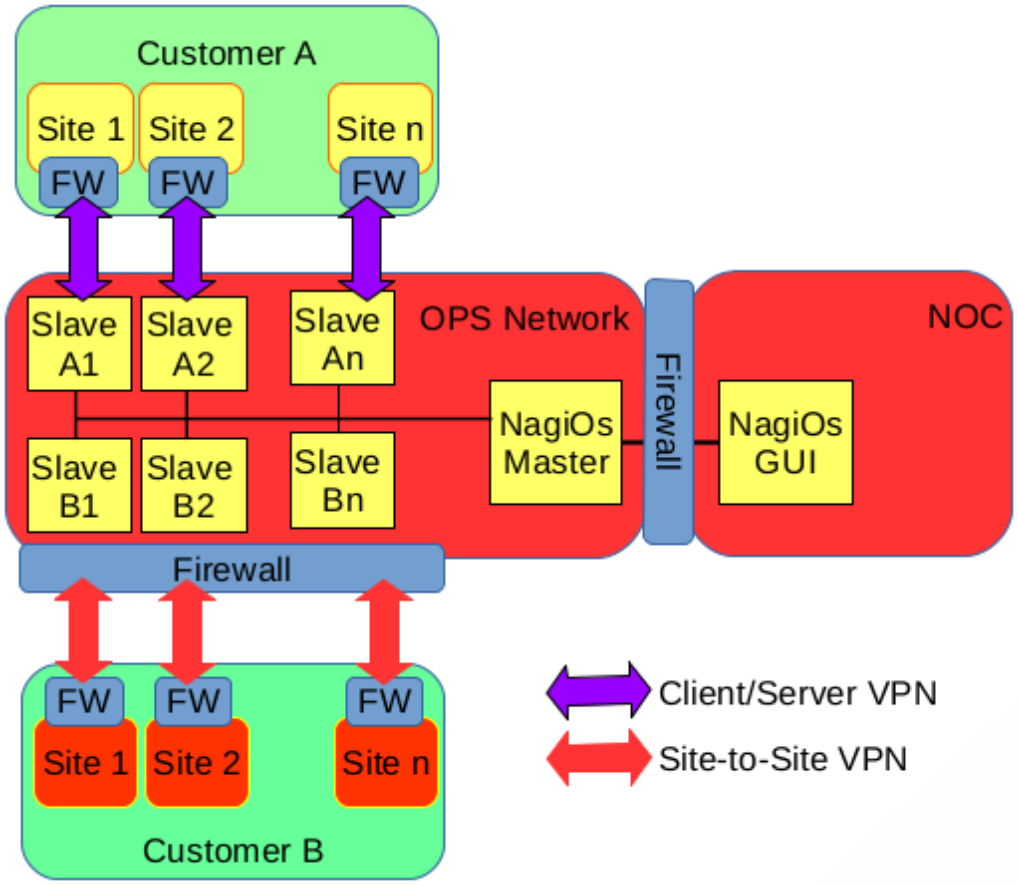
3 High Level Architecture

3.1 Logical Network Architecture – block diagram

For the monitoring platform, there are 3 major components types:

1. One NagiOs Master server
2. Multiple NagiOs Slave servers
3. NagiOs GUI clients

The solution spans over 2 dedicated networks at the control center. First is the NOC that is shared with other systems used to monitor and control and the second is the OPS network where the NagiOs servers are installed.

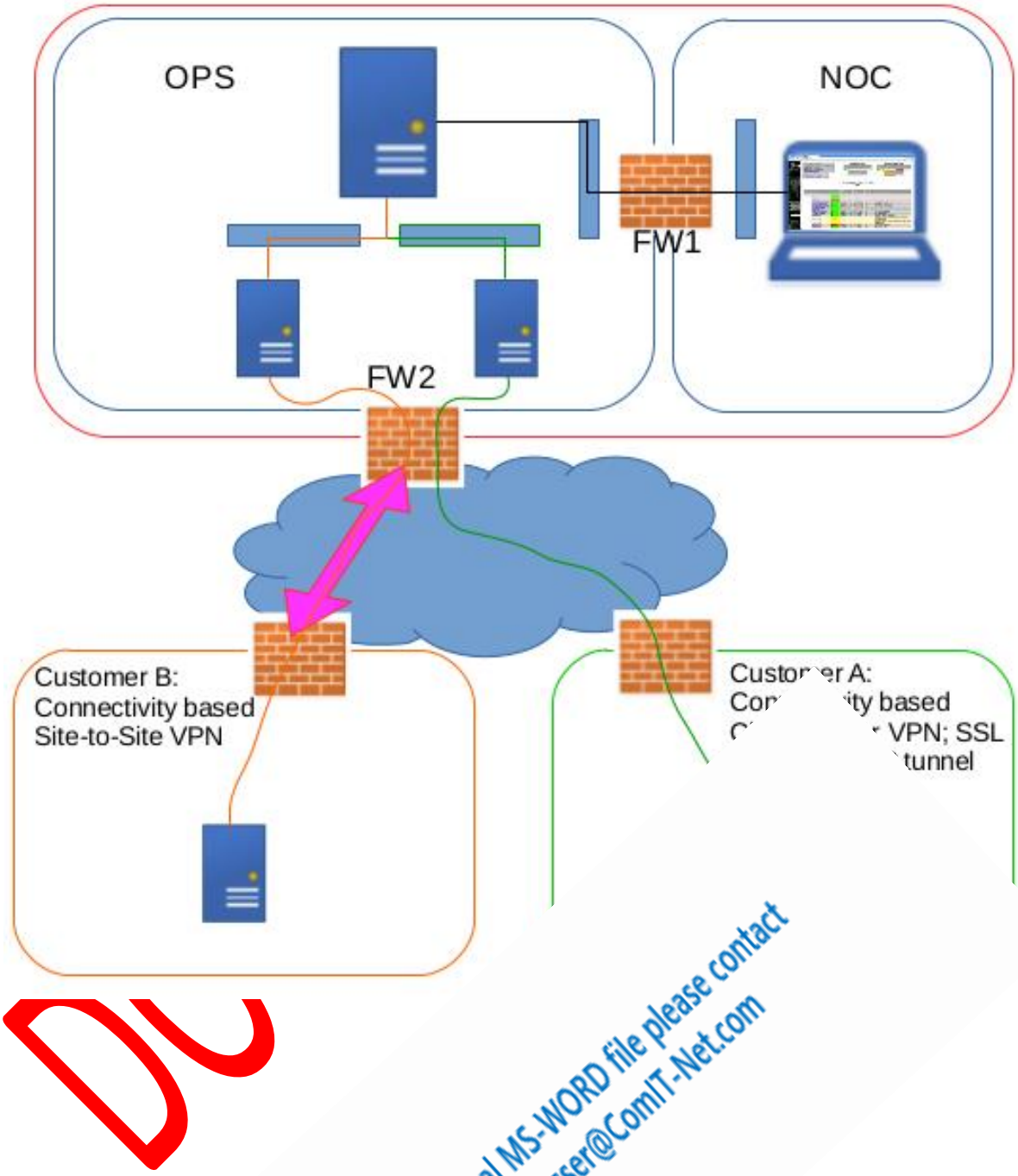


Firewalls are to be used for dividing the various networks (N
allow dedicated connectivity between each slave server ar
site. Connectivity to the site can be over Site-to-Site V
based on the customer guidelines.

3.2 Physical Network Architectu

NagiOs Master Server is the heart of the
isolated as much as possible (with as
from the NOC and rest of IT and C
ders.

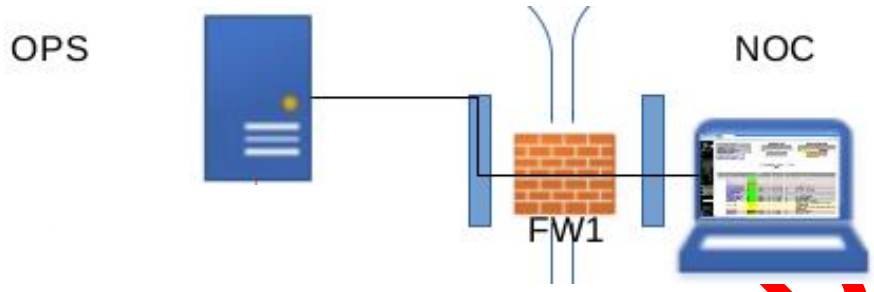
4 Solution Architecture



4.1 Control Plane Data Flow between Components

4.1.1 Data Flow from Nagios Client to Server

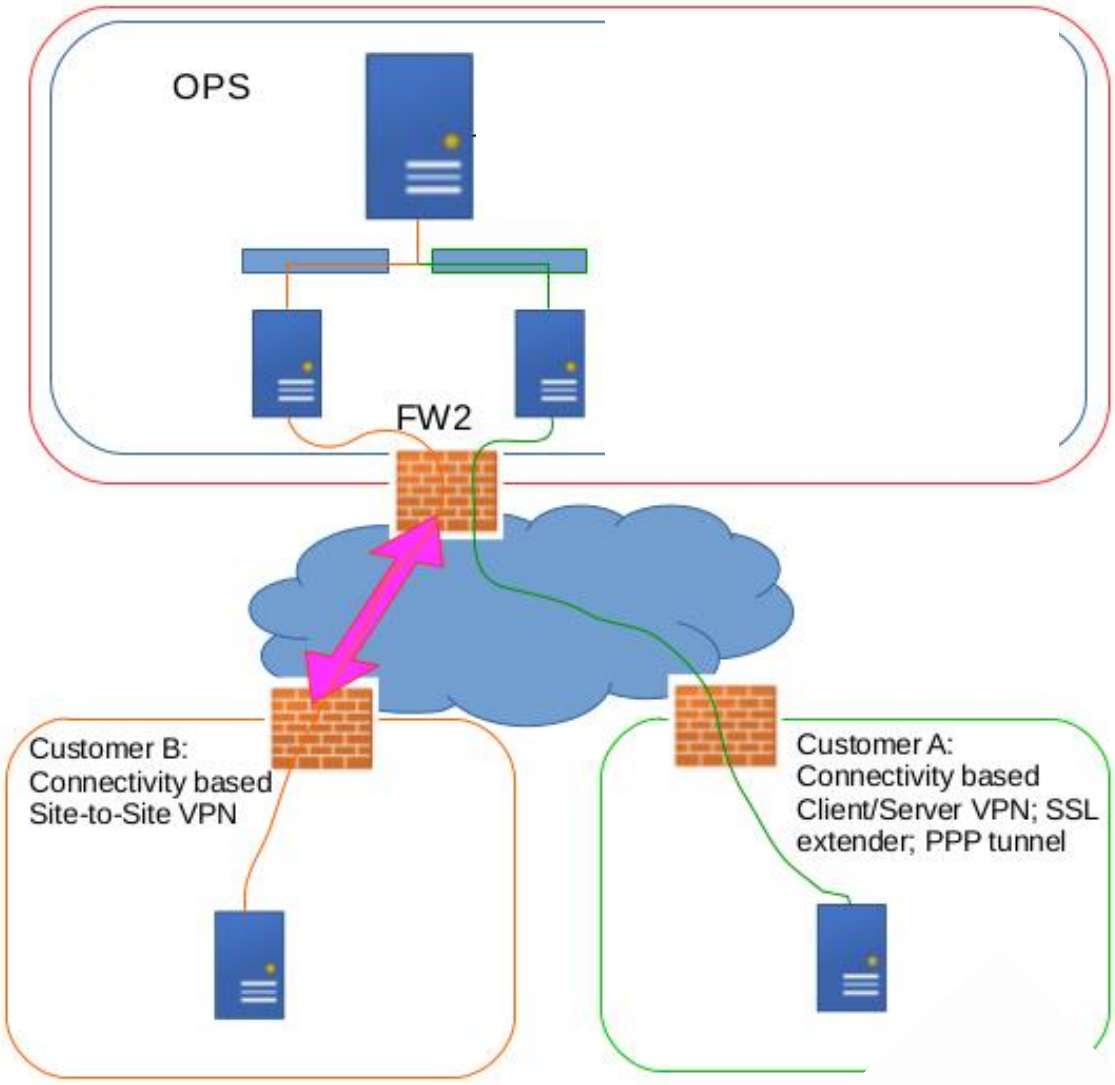
Nagios has Private IP addresses. The Server is being accessible to the NOC network for both GUI (Web based) and SSH access. The following diagrams describe the access protocols.



Source	Destination	Application	Protocol	Port	Comments
NOC (Client)	OPS (Server)	HTTP	TCP	80	To increase security the usage o[illegible]-generic port is [illegible]i.e 1080
NOC	OPS	HTTPS	TCP	443	T[illegible] the
NOC	OPS	SSH	TCP		

4.1.2 Data Flow Nagius s[illegible]

Customer's monitored equip[illegible], that can be site-to-site or clien[illegible], to initiate the connection[illegible] way that for each customer's site[illegible]alled.



Source	Destination	Application	Protocol	Port
OPS Master	Customer	PING	icmp	
OPS Slave	Customer	PING	icmp	
OPS Slave	Customer	SSH		ane neric d, i.e 1022
OPS Slave	Customer			"get" status e, not for traps

4.2 Securing the Control Plane

4.2.1 Nagios servers CLI Access

Each server in the solution, is Linux based. As such it has a command line interface. While most management functions are performed via the Graphic user interface, initial platform configuration must be performed using the CLI. In addition, some additional troubleshooting tools and configuration options are available via CLI.

Accessing the system using CLI will be with individual usernames to keep track on the access and activity done in the servers using CLI

Each server should have 3 different levels of privileges for designated users, each will be limited to its specific tasks.

Login level/group	Password	Available to	Comments
Nagios	NA	Noc operators	NOC operators accessing with individual username & Password will have lowest level. Will allow them to start/stop the service. Read logfiles
OPS	NA	Support	Customer support accessing with individual username & password will have same privileges as above as well as the ability to save files that will be required to be uploaded to customer's network for maintenance
root	NA	Sys admin	Sys admin accessing with individual username & password will have full rights over the system

4.2.2 Nagios GUI Access

The Nagios platform can apply a role to a user that uses the GUI to monitor the customers. There should be minimum two roles set in the system that will allow to distinguish between monitoring agent and support agent.

Role	Privileges
Monitor	NOC agent that access the web interface UI with individual username & password and is capable of monitoring only
Administrator	Support agent that access the web interface UI with individual username & password and is capable to monitor and execute actions

4.3 Securing the Data Plane

4.3.1 VPN connectivity to customers

As a rule, the VPN type and configuration will be dictated by the customer (site-to-site, client/server, PPP etc). when installing the system is is important to set he OPS network Firewall (FW2) to block any connection established at customer's network and aimed to the OPS network.

It is important to disable any routing between same customer's sites to be routed via the OPS firewall or network.

It is must to verify that there is no route between two different customers.

Customer's network should be accessible only from the designated Nagios slave server, that in turn will serve as jump server when as supporter need to troubleshoot an incident.

4.3.2 Nagios servers CLI Access

Nagios slave server should not be able to open CLI connection to other salves or to the muster server. Such interface should be allowed only from the Master to the Slaves

4.3.3 Nagios GUI Access

GUI access will should be available only from NOC network.

END OF DOCUMENT