St. John’s University

</SJU CYBER>

Network Documentation

SJU-CDC-2017-0001-ND

Document Owner: TEAM CO-LEAD

VERSION	DATE	DESCRIPTION	ORIG	CHK	APPR
1	03/12/17	New Document	Anish Bachu	Matthew Tringone	Anthony Jairam
Review Cycle: 6 months					
This is an electronically generated document which has been reviewed and approved in accordance with SJUCYBER procedure. The screen version of this document is the Controlled Master Copy at all times. A printed copy is considered to be “For Information Only” and as such it is the holder’s responsibility to ensure that they have the current version. Controlled copies of competition documents are available in the Controlled Binder held by team Co-lead.					

PRODUCTION CRITICAL

DOCUMENT DISTRIBUTION PAGE

The Master Copy of this document is available for viewing by contacting Co-Lead

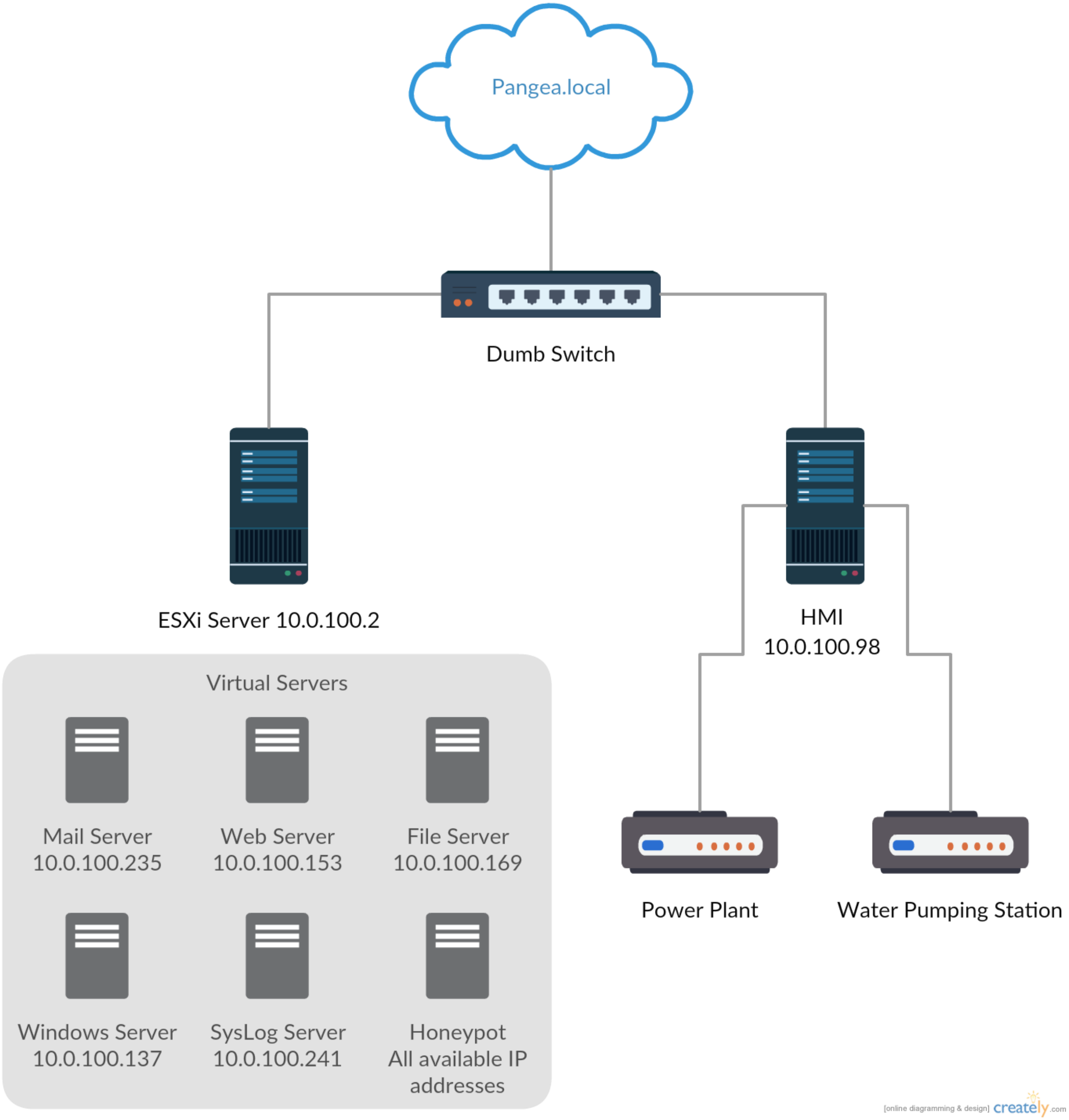
Controlled paper copies of the document have been distributed as follows:

1. Team Lead
2. Team Co-Lead
3. Team Network Administrator
4. White Team (Argonne National Laboratory)

Table of Contents

Network Topology

Network Diagram



Description

Working with the restrictions of the CDC in mind, the network topology reflects and simplistic approach to the structure of the network. The principle of KISS (Keep It Simple, Stupid) was employed when conceptualizing the network diagram – keep the network simple but employ extreme server hardening. The ESXi Server is the home of six (6) virtual servers – Web, Mail, File, Windows, System Log and Honeypot servers – that are logically networked through vSwitch0 (virtual switch zero). The HMI (Human Machine Interface) of the industrial control system sits on its own with the power substation and water pumping station and is connected to the ESXi Server via a dumb (unmanaged) switch – as per CDC restrictions. The ESXi Server and HMI are both contained in the team 10 subnet with Pangea.local being the connection to the CDC router (not under our jurisdiction).

Switch Port Assignments

- Dumb Switch
    - Switch Port 1 – Line in from Pangea
    - Switch Port 2 – ESXi Server vSwitch0
        - Management Network
        - VM Network
    - Switch Port 3 - HMI

Configuration of Network Services

Active Directory

This service is configured on a virtual machine running Windows Server 2008 R2. The domain tree is Pangea.local. It also serves as the central authentication point for the Web, Mail and File servers.

DNS

This service is configured on a virtual machine running Windows Server 2008 R2. It resolves the following IP addresses to the corresponding URL. This service operates on port 53.

IP Address	URL
10.0.100.153	https://web.pangea.local
10.0.100.235	https://mail.pangea.local

FTP

This service operates on port 21. This service resides on the Web, Mail and File Servers

HTTP

This service operates on port 80. This service is enabled but HTTPS is used by default for all connections of this type. This service runs on the Web, Mail and File Servers and the HMI.

HTTPS

This service operates on port 8080. This is the default protocol for connections of this type on the World Wide Web. This service runs on the Web and Mail Servers and the HMI.

LDAP

This service operates on port 389. Search based is ou=Employees,dc=Pangea,dc=local. This protocol is used for streamlined user authentication between Active Directory, the web portal and file server.

NTP

This service operates on port 123. This service runs on all nodes within the network and is used for clock synchronization. This is especially important to ensure the System Log Server receives data with the correct time stamps to enable proper compilation and analysis.

SMTP

This service operates on port 25. This service runs on the mail server on Postfix and is used to send email communications.

IMAP

This service operates on port 993 as it is TLS encrypted IMAP. This service runs on the mail server on Dovecot and is used to receive email communications.

SNMP

This service operates on port 161. Like NTP, this is also especially important to ensure the System Log Server receives data in an efficient manner to enable proper compilation and analysis.

SSH

This service operates on port 53. This service runs on the Web, Mail and File Servers and the HMI. This allows secure and encrypted remote connections to the aforementioned servers by authorized users.

NAT

This service was not employed in our network as it was decided that abundance of honeypots will provided sufficient cover for production critical servers.

Server Information

Active Directory, DNS, NTP Server (Virtualized)

Name:	PangeaWIN
IP Address:	10.0.100.137
Operating System	Windows Server 2008 R2
Operational Level:	Critical
Asset Tag:	SJU-VS-0001

This Windows Server plays as a host to Active Directory (AD), the Domain Name System (DNS) and the Network Time Protocol (NTP). This server is administered and secured by the Windows Server Security Technician. The decision to host AD, DNS and NTP all on one virtual machine was made as the Windows Server Security Technician has a vast wealth of experience to configuring these services. The Pangea security team has recognized that this creates a major point of failure within the network but it also minimizes the number of devices that need to be secured. As such, PangeaWIN is listed as critical to the operations of Pangea Water and Power and several measures have been taken to secure this virtual machine from remote intrusions.

Steps taken to secure Windows Server 2008 R2:

- All outstanding security patches and updates were installed
- Windows Firewall was enabled for all connection types and unicast responses were disabled
- Disabled the last user display option
- Default passwords for administrator and authorized user accounts were changed in accordance with password policy (refer to SJU-CDC-2017-0007-PP)
- Remote Desktop Sharing and Microsoft Peer-to-Peer Networking Services were disabled
- Homegroup capability was disabled
- New user accounts receive the lowest level of privilege
- Session times out after 5 minutes of inactivity and password is required to continue
- Disabled downloading of print drivers over HTTP
- Disallowed anonymous enumeration of SAM accounts and shares
- Disabled IPv6
- The virtual memory pagefile is cleared on shutdown

HTTP - 80	SSH - 22	FTP - 21
LDAP - 389	DNS - 53	NTP - 123

Web Server (Virtualized)

Name:	PangeaWeb
IP Address:	10.0.100.153
Operating System	Debian
Operational Level:	Critical
Asset Tag:	SJU-VS-0002

Debian 7 is the operating system on which the Pangea web server resides. This free and open source operating system serves as the backbone of the user web portal. This asset is administered and secured by the Linux Server Security Technician. In conjunction with Debian, Drupal version 7.4 is the content management framework on which the website is built. Drupal is administered and secured by the Web Application Security Technician. The website serves as the major point of interaction between users and the internal network and as such has been given a high degree of importance as it relates to the business operations of Pangea Water and Power. Several measures have been taken to secure both Debian and Drupal from intrusion and malicious activity.

Steps taken to secure Debian: (Script execution time – under 5 minutes)

- All outstanding updates were installed
- Root password was changed to prevent easy remote access to the system
- The SSH port was changed to 8081 and root access through SSH was disable to prevent unauthorized remote access
- The old SSH key was deleted and a new key was put in place
- The color of the text in the terminal window was changed to black in order to confuse malicious actors that have managed to SSH into the virtual machine
- The size of the listen queue for accepting new TCP packets was increased to 4096 (default 128)
- The maximum number of sockets to be held in TIME-WAIT was increased to order to curb the effects of denial of service attacks
- Core dumps were disabled and ExecShield was enabled
- Packet forwarding was disabled and a log for suspicious packets was set up
- IPv6 was disabled
- IP spoofing protection was put in place where are spoofed packets are logged
- IP source routing was disabled and the system was set to ignore broadcast requests

- Unnecessary directories, folders and software were removed (e.g. telnet, perl, netcat and findutils).

Steps taken to secure Drupal: (Script execution time – under 3 minutes)

- All outstanding updates were installed
- The default Drupal and MySQL passwords were changed
- Files not necessary to production operations were removed
- We removed several hidden shells
- Captcha was installed to eliminate automated data entry processes
- Apache version and OS identity were hidden and supporting manuals were removed
- Apache directory browsing was disabled
- Apache configuration and binaries only viewable from root
- SSL was enabled to encrypt the connection between the server and user browsers

User Permissions on Drupal:

- Default Administrator role was disabled and a new administer role was created (to circumvent the fact that each user was given administrator privileges by default)
- Employee role created for authorized user accounts with the following permissions:
    - Post, view and edit (their own) comments
    - Dashboard only shows logout option (no administrator options)
    - Can only view published content
    - Support tickets can be logged with the option to set ticket priority, assign ticket to another user.
    - Users can only view their tickets
    - Users cannot upload profile pictures
    - Only authenticated employees are allowed to comment on content
- New users can only be added through an official onboarding process (refer to SJU-CDC-2017-0006-BB for onboarding form)
- Anonymous or unauthenticated sites visitors can only view published content.

HTTP - 80	SSH - 8081	FTP - 21
LDAP - 389	DNS - 53	NTP - 123

Mail Server (Virtualized)

Name:	PangeaMail
IP Address:	10.0.100.235
Operating System	CentOS
Operational Level:	High
Asset Tag:	SJU-VS-0003

The mail server consists of Roundcube version 1.2.4 web-based IMAP client and the CentOS version 6 operating system. Roundcube is a free and open source software that is used as the user interface for the Pangea Water and Power email system. CentOS is administered and secured by the Linux Server Security Technician and Roundcube is administered and secured by the Web Application Security Technician. The Roundcube interface was selected due to its intuitive design and because it has the Ajax (Asynchronous JavaScript and XML) scheme built-in which allows the client to exchange data with a server without disrupting the exiting page. The mail server is listed as high on the business operational scale as it is the major method of communication between end users and IT. As such, serval measures have been taken to secure both CentOS and Roundcube from threat agents.

Steps taken to secure CentOS: (Script execution time – under 3 minutes)

- All outstanding updates were installed for CentOS, Roundcube, Apache, Postfix and Dovecot
- Default passwords were changed
- SSL was enabled to encrypt server to browser connection
- The SSH port was changed to 8081 and root access through SSH was disable to prevent unauthorized remote access
- The old SSH key was deleted and a new key was put in place
- Apache, Postfix and Dovecot versions were hidden and supporting manuals were removed
- IPv6 was disabled

HTTP – 80	SSH – 8081	FTP – 21
LDAP - 389	DNS - 53	NTP - 123

File Server (Virtualized)

Name:	PangeaFILE
IP Address:	10.0.100.169
Operating System	Ubuntu
Operational Level:	High
Asset Tag:	SJU-VS-0004

The file server resides on the Ubuntu 10.04 operating system. Ubuntu coupled with Samba form the file server. Samba is a free and open source that provides stable and fast file services. The file server is an important aspect of the business operations of Pangea Water and Power as business critical documents are stored on this server. By storing important files on a central server rather than storing them on various portable devices (laptops, smartphones etc.), business critical information can be secured and access controls employed. This virtual server is administered and secured by the Linux Server Security Technician as the process to secure this machine is similar to that of Debian and CentOS.

Steps taken to secure Ubuntu: (Script execution time – under 5 minutes)

- All outstanding updates were installed
- Root password was changed to prevent easy remote access to the system
- The SSH port was changed to 8081 and root access through SSH was disable to prevent unauthorized remote access
- The old SSH key was deleted and a new key was put in place
- The maximum number of sockets to be held in TIME-WAIT was increased to order to curb the effects of denial of service attacks
- Core dumps were disabled and ExecShield was enabled
- Packet forwarding was disabled and a log for suspicious packets was set up
- IPv6 was disabled
- IP spoofing protection was put in place where are spoofed packets are logged
- IP source routing was disabled and the system was set to ignore broadcast requests
- Unnecessary directories, folders and software were removed (e.g. telnet, perl, netcat and findutils).

HTTP - 80	SSH - 8081	FTP - 21
LDAP - 389	DNS - 53	NTP - 123

Human Machine Interface (HMI)

Name:	PangeaHMI
IP Address:	10.0.100.98
Operating System	Raspbian
Operational Level:	Critical
Asset Tag:	SJU-IS-010

This is a physical device (Raspberry Pi) that plays host to the Human Machine Interface (HMI) and is one part of the larger Industrial Control System (ICS). The HMI is administered and secured by the SCADA (Supervisor Control and Data Acquisition) Security Technician. From the HMI, various production engineers can view the status of the industrial control system. Pangea's control system is broken up into two (2) sections; the water distribution ICS and the power grid ICS. Programmable Logic Controllers (PLCs) control pumps, pressure sensors and the purification process in the water distribution network. In the power distribution network, PLCs control generators, load balancers and the fire and emergency sensors and devices. Due to the major potential fallout as a result of a dysfunctional ICS, the HMI has been listed as critical to the operations of Pangea Water and Power and multiple security measures have been taken to ensure system integrity and functionality.

Steps taken to secure the HMI:

- All outstanding updates were installed
- Root password was changed to prevent easy remote access to the system
- The SSH port was changed to 8081 and root access through SSH was disable to prevent unauthorized remote access
- Internal production logic and safety logic were examined and verified
- Only authorized user accounts were generated
- Enforcement of password policy (refer to SJU-CDC-2017-0007-PP)
- New users will have to go through the official onboarding process (refer to SJU-CDC-2017-0006-BB)

HTTP - 80	SSH - 8081	FTP - 21
LDAP - 389	DNS - 53	NTP - 123

System Log Server (Virtualized)

Name:	PangeaSysLog
IP Address:	10.0.100.241
Operating System	Ubuntu
Operational Level:	Intermediary
Asset Tag:	SJU-VS-0005

The System Log server resides on the Ubuntu 14.04 operating system. The software used to collect and compile the logs from the various machines is called ELK Stack. ELK Stack is a combination of three (3) open source tools; Elasticsearch, Logstash and Kibana. Elasticsearch refer to a log database to store all incoming information. Logstash is a log pipeline that feeds data from the machines being monitored to the system log server. Kibana complies the data and presents it in the form of easy to understand graphs. This virtual machine is administered and monitored by the Log Monitoring Analyst. Minimal security measures were taken to secure this virtual machine.

HTTP - 80	SSH - 22	FTP - 21
LDAP - 389	DNS - 53	NTP - 123

Honeypot (Virtualized)

Name:	PangeaS
IP Address:	All available IP addresses in the subnet (refer to appendix)
Operating System	Ubuntu
Operational Level:	Low
Asset Tag:	SJU-VS-0006

This is a virtualized server that runs Ubuntu 14.04. This minimizes effort due to the fact that two (2) other virtual machines run Ubuntu 10.04 and the method to secure them is the same. The honeypot software being utilized is Honeyd Virtual Honeypot. Honeyd creates virtual hosts on a network that are configured to run services similar to those of legitimate production servers. Two hundred and forty-six (246) honeypots were created within the honeyd daemon to mimic actual machines on the network. ALL IP addresses within the subnet will be link to a honeypot with the exception of 10.0.100.98, 10.0.100.137, 10.0.100.153, 10.0.100.169 and 10.0.100.235, 10.0.100.241. Refer to the appendix to find a complete list of honeypot IP addresses. No effort was made to secure the honeypot virtual machine. Opened service ports available on the honeypot are as shown in the table below.

HTTP - 80	SSH - 8081	FTP - 21
LDAP - 389	DNS - 53	NTP - 123

Appendix

Summary of Servers

Service	Name	Operating System	Applications	IP Address	Patch Level
Web	PangeaWeb	Debian 7	Drupal	10.0.100.153	4
Mail	PangeaMail	CentOS 6.8	Roundcube	10.0.100.235	4
FTP	PangeaFile	Ubuntu 14.04	Samba	10.0.100.169	4
AD	PangeaWIN	Windows Server 2008 R2	-	10.0.100.137	3
DNS	PangeaWIN	Windows Server 2008 R2	-	10.0.100.137	3
NTP	PangeaWIN	Windows Server 2008 R2	-	10.0.100.137	3
Syslog	PangeaSL	Ubuntu 14.04	ELK Stack	10.0.100.241	1
HMI	PangeaHMI	Raspbian	Pangea ICS	10.0.100.98	4
Honey Pot	PangeaS	Ubuntu 14.04	Honeyd	All other IP addresses in the subnet	0

Summary of Port Numbers

	PangeaWeb	PangeaMail	PangeaFile	PangeaWIN	PangeaHMI	PangeaSL	PangeaS
HTTP	80	80	80	80	80	80	80
HTTPS	8080	8080	8080	-	8080	-	8080
FTP	21	21	21	21	21	21	21
SSH	8081	8081	8081	8081	8081	8081	8081
LDAP	389	389	389	389	389	389	389
DNS	53	53	53	53	53	53	53
NTP	123	123	123	123	123	123	123

Responders

Name	Role	Title
Anthony Jairam	Linux Server Security	Lead
Anish Bachu	Business Analysis	Co-Lead
Jeffery Matthews	Windows Server Security	-
Graham Mulvihill	Web Application Security	-
Matthew Tringone	Network Admin	-
Harishikesh Ramprashad	Log Monitoring	-

Honeypot IP Addresses

-
-
10.0.100.3
10.0.100.4
10.0.100.5
10.0.100.6
10.0.100.7
10.0.100.8
10.0.100.9
10.0.100.10
10.0.100.11
10.0.100.12
10.0.100.13
10.0.100.14
10.0.100.15
10.0.100.16
10.0.100.17
10.0.100.18
10.0.100.19
10.0.100.20
10.0.100.21
10.0.100.22
10.0.100.23
10.0.100.24
10.0.100.25
10.0.100.26
10.0.100.27
10.0.100.28
10.0.100.29
10.0.100.30
10.0.100.31
10.0.100.32
10.0.100.33
10.0.100.34
10.0.100.35
10.0.100.36
10.0.100.37
10.0.100.38
10.0.100.39
10.0.100.40
10.0.100.41
10.0.100.42
10.0.100.43
10.0.100.44
10.0.100.45
10.0.100.46
10.0.100.47
10.0.100.48
10.0.100.49
10.0.100.50
10.0.100.51
10.0.100.52
10.0.100.53
10.0.100.54
10.0.100.55
10.0.100.56
10.0.100.57
10.0.100.58
10.0.100.59
10.0.100.60
10.0.100.61
10.0.100.62
10.0.100.63
10.0.100.64
10.0.100.65
10.0.100.66
10.0.100.67
10.0.100.68
10.0.100.69
10.0.100.70
10.0.100.71
10.0.100.72
10.0.100.73
10.0.100.74
10.0.100.75
10.0.100.76
10.0.100.77
10.0.100.78
10.0.100.79
10.0.100.80
10.0.100.81
10.0.100.82
10.0.100.83
10.0.100.84
10.0.100.85
10.0.100.86
10.0.100.87
10.0.100.88
10.0.100.89
10.0.100.90
10.0.100.91
10.0.100.92
10.0.100.93
10.0.100.94
10.0.100.95
10.0.100.96
10.0.100.97
-
10.0.100.99
10.0.100.100
10.0.100.101
10.0.100.102
10.0.100.103
10.0.100.104
10.0.100.105
10.0.100.106
10.0.100.107
10.0.100.108
10.0.100.109
10.0.100.110
10.0.100.111
10.0.100.112
10.0.100.113
10.0.100.114
10.0.100.115
10.0.100.116
10.0.100.117
10.0.100.118
10.0.100.119
10.0.100.120
10.0.100.121
10.0.100.122
10.0.100.123
10.0.100.124
10.0.100.125
10.0.100.126
10.0.100.127
10.0.100.128
10.0.100.129
10.0.100.130
10.0.100.131
10.0.100.132
10.0.100.133
10.0.100.134
10.0.100.135
10.0.100.136
-
10.0.100.138
10.0.100.139
10.0.100.140
10.0.100.141
10.0.100.142
10.0.100.143
10.0.100.144
10.0.100.145
10.0.100.146
10.0.100.147
10.0.100.148
10.0.100.149
10.0.100.150
10.0.100.151
10.0.100.152
-
10.0.100.154
10.0.100.155
10.0.100.156
10.0.100.157
10.0.100.158
10.0.100.159
10.0.100.160
10.0.100.161
10.0.100.162
10.0.100.163
10.0.100.164
10.0.100.165
10.0.100.166
10.0.100.167
10.0.100.168
-
10.0.100.170
10.0.100.171
10.0.100.172
10.0.100.173
10.0.100.174
10.0.100.175
10.0.100.176
10.0.100.177
10.0.100.178
10.0.100.179
10.0.100.180
10.0.100.181
10.0.100.182
10.0.100.183
10.0.100.184
10.0.100.185
10.0.100.186
10.0.100.187
10.0.100.188
10.0.100.189
10.0.100.190
10.0.100.191
10.0.100.192
10.0.100.193
10.0.100.194
10.0.100.195
10.0.100.196
10.0.100.197
10.0.100.198
10.0.100.199
10.0.100.200
10.0.100.201
10.0.100.202
10.0.100.203
10.0.100.204
10.0.100.205
10.0.100.206
10.0.100.207
10.0.100.208
10.0.100.209
10.0.100.210
10.0.100.211
10.0.100.212
10.0.100.213
10.0.100.214
10.0.100.215
10.0.100.216
10.0.100.217
10.0.100.218
10.0.100.219
10.0.100.220
10.0.100.221
10.0.100.222
10.0.100.223
10.0.100.224
10.0.100.225
10.0.100.226
10.0.100.227
10.0.100.228
10.0.100.229
10.0.100.230
10.0.100.231
10.0.100.232
10.0.100.233
10.0.100.234
-
10.0.100.236
10.0.100.237
10.0.100.238
10.0.100.239
10.0.100.240
-
10.0.100.242
10.0.100.243
10.0.100.244
10.0.100.245
10.0.100.246
10.0.100.247
10.0.100.248
10.0.100.249
10.0.100.250
10.0.100.251
10.0.100.252
10.0.100.253
10.0.100.254