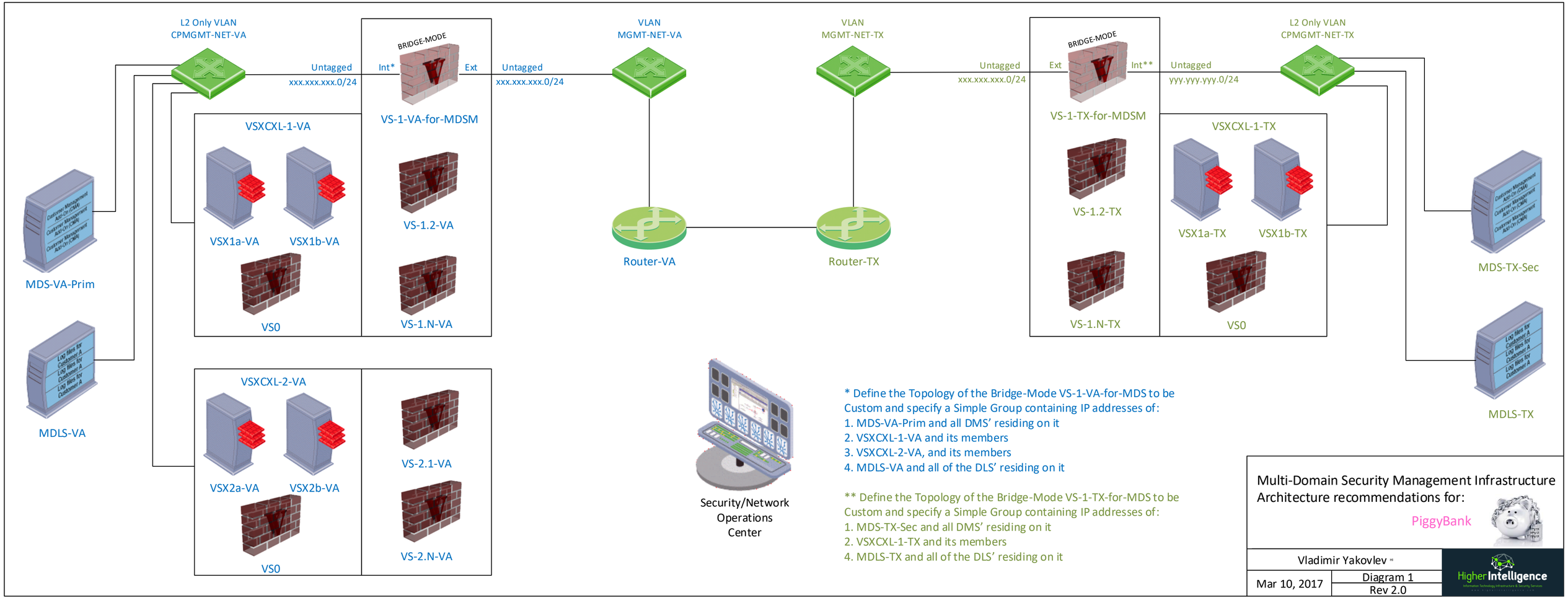
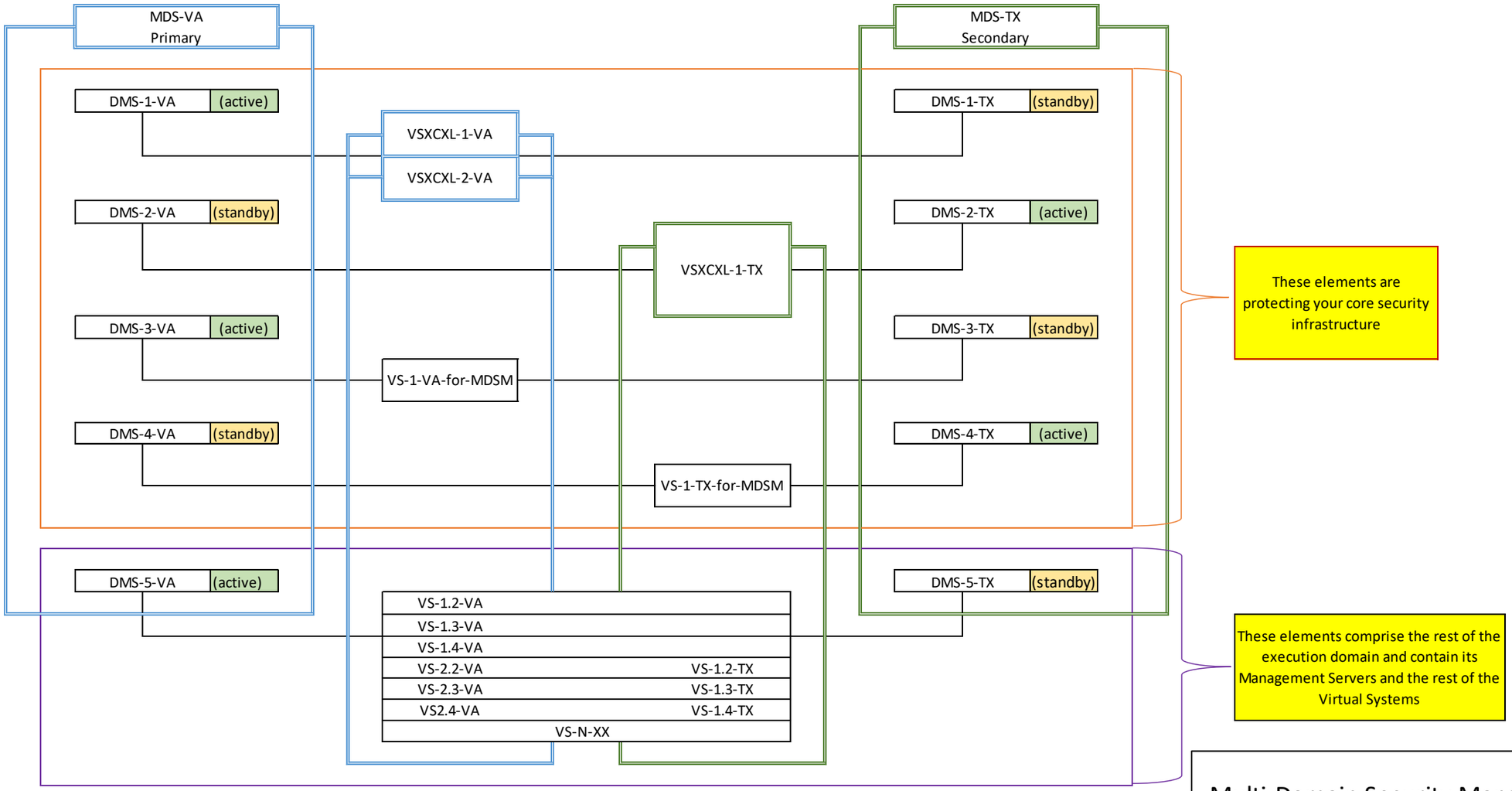

L2 Only VLAN
CPMGMT-NET-VA
Untagged
xxx.xxx.xxx.0/24
BRIDGE-MODE
Int*
Ext
VS-1-VA-for-MDSM
VSXCXL-1-VA
VSX1a-VA
VSX1b-VA
VS-1.2-VA
VS0
VS-1.N-VA
MDS-VA-Prim
MDLS-VA
VSXCXL-2-VA
VSX2a-VA
VSX2b-VA
VS-2.1-VA
VS0
VS-2.N-VA
VLAN
MGMT-NET-VA
Untagged
xxx.xxx.xxx.0/24
Router-VA
VLAN
MGMT-NET-TX
Router-TX
Untagged
xxx.xxx.xxx.0/24
BRIDGE-MODE
Ext
Int**
VS-1-TX-for-MDSM
VS-1.2-TX
VS-1.N-TX
L2 Only VLAN
CPMGMT-NET-TX
Untagged
yyy.yyy.yyy.0/24
VSXCXL-1-TX
VSX1a-TX
VSX1b-TX
VS0
MDS-TX-Sec
MDLS-TX
Security/Network
Operations
Center
* Define the Topology of the Bridge-Mode VS-1-VA-for-MDS to be
Custom and specify a Simple Group containing IP addresses of:
1. MDS-VA-Prim and all DMS' residing on it
2. VSXCXL-1-VA and its members
3. VSXCXL-2-VA, and its members
4. MDLS-VA and all of the DLS' residing on it
** Define the Topology of the Bridge-Mode VS-1-TX-for-MDS to be
Custom and specify a Simple Group containing IP addresses of:
1. MDS-TX-Sec and all DMS' residing on it
2. VSXCXL-1-TX and its members
4. MDLS-TX and all of the DLS' residing on it
Multi-Domain Security Management Infrastructure
Architecture recommendations for:
PiggyBank
Vladimir Yakovlev
Mar 10, 2017
Diagram 1
Rev 2.0
HigherIntelligence

Check Point MDSM Architecture



These elements are protecting your core security infrastructure

These elements comprise the rest of the execution domain and contain its Management Servers and the rest of the Virtual Systems

Multi-Domain Security Management Infrastructure Architecture recommendations for:

PiggyBank

Vladimir Yakovlev

Mar 10, 2017

Diagram 2

Rev 2.0

Higher Intelligence

VA

Cluster or Gateway	Log to: Send logs and alerts to these log servers: 1	2	In case one of the above servers is unreachable, send logs to: 1	2
VSXCXL-1-VA	DMS-1-VA		DMS-1-TX	
VSXCXL-2-VA	DMS-1-VA		DMS-1-TX	
VS-1-VA-for-MDSM	DMS-3-VA		DMS-3-TX	
VS-1.2-VA	DMS-5-VA		DMS-5-TX	
VS-1.3-VA	DMS-5-VA		DMS-5-TX	
VS-1.4-VA	DMS-5-VA		DMS-5-TX	
VS-2.2-VA	DMS-5-VA		DMS-5-TX	
VS-2.3-VA	DMS-5-VA		DMS-5-TX	
VS-2.4-VA	DMS-5-VA		DMS-5-TX	

Log forwarding from Log or Management Servers:

DLS-1-VA	(active)	forward logs to:	DMS-1-TX
DLS-2-VA	(standby)	forward logs to:	DMS-2-TX
DLS-3-VA	(active)	forward logs to:	DMS-3-TX
DLS-4-VA	(standby)	forward logs to:	DMS-4-TX
DLS-5-VA	(active)	forward logs to:	DMS-5-VA

TX

Cluster or Gateway	Log to: Send logs and alerts to these log servers: 1	2	In case one of the above servers is unreachable, send logs to: 1	2
VSXCXL-1-TX	DMS-2-TX		DMS-2-VA	
VS-1-TX-for-MDSM	DMS-4-TX		DMS-4-VA	
VS-1.2-TX	DMS-5-TX		DMS-5-VA	
VS-1.3-TX	DMS-5-TX		DMS-5-VA	
VS-1.4-TX	DMS-5-TX		DMS-5-VA	

Log forwarding from Log or Management Servers:

DLS-1-TX	(standby)	forward logs to:	DMS-1-VA
DLS-2-TX	(active)	forward logs to:	DMS-2-VA
DLS-3-TX	(standby)	forward logs to:	DMS-3-VA
DLS-4-TX	(active)	forward logs to:	DMS-4-VA
DLS-5-TX	(standby)	forward logs to:	DMS-5-VA

Multi-Domain Security Management Infrastructure
Architecture recommendations for:

Logging
MDS' only

PiggyBank

Vladimir Yakovlev HI

Mar 10, 2017

Table 1
Rev 2.0

Higher Intelligence
Information Technology, Infrastructure & Security Services
www.higherintelligence.com

VA

Cluster or Gateway	Log to: Send logs and alerts to these log servers: 1	2	In case one of the above servers is unreachable, send logs to: 1	2
VSXCXL-1-VA	DLS-1-VA		DLS-1-TX	
VSXCXL-2-VA	DLS-1-VA		DLS-1-TX	
VS-1-VA-for-MDSM	DLS-3-VA		DLS-3-TX	
VS-1.2-VA	DLS-5-VA		DLS-5-TX	
VS-1.3-VA	DLS-5-VA		DLS-5-TX	
VS-1.4-VA	DLS-5-VA		DLS-5-TX	
VS-2.2-VA	DLS-5-VA		DLS-5-TX	
VS-2.3-VA	DLS-5-VA		DLS-5-TX	
VS-2.4-VA	DLS-5-VA		DLS-5-TX	

Log forwarding from Log or Management Servers:

DLS-1-VA	(active)	forward logs to:	DLS-1-TX
DLS-2-VA	(standby)	forward logs to:	DLS-2-TX
DLS-3-VA	(active)	forward logs to:	DLS-3-TX
DLS-4-VA	(standby)	forward logs to:	DLS-4-TX
DLS-5-VA	(active)	forward logs to:	DLS-5-VA

TX

Cluster or Gateway	Log to: Send logs and alerts to these log servers: 1	2	In case one of the above servers is unreachable, send logs to: 1	2
VSXCXL-1-TX	DLS-2-TX		DLS-2-VA	
VS-1-TX-for-MDSM	DLS-4-TX		DLS-4-VA	
VS-1.2-TX	DLS-5-TX		DLS-5-VA	
VS-1.3-TX	DLS-5-TX		DLS-5-VA	
VS-1.4-TX	DLS-5-TX		DLS-5-VA	

Log forwarding from Log or Management Servers:

DLS-1-TX	(standby)	forward logs to:	DLS-1-VA
DLS-2-TX	(active)	forward logs to:	DLS-2-VA
DLS-3-TX	(standby)	forward logs to:	DLS-3-VA
DLS-4-TX	(active)	forward logs to:	DLS-4-VA
DLS-5-TX	(standby)	forward logs to:	DLS-5-VA

Multi-Domain Security Management Infrastructure
Architecture recommendations for:

Logging
MDS' and MDLS'

PiggyBank

Vladimir Yakovlev

Mar 10, 2017

Table 2

Rev 2.0

Higher Intelligence
Information Technology, Infrastructure & Security Services

VA

Cluster or Gateway	Log to: Send logs and alerts to these log servers: 1	2	In case one of the above servers is unreachable, send logs to: 1	2
VSXCXL-1-VA	DLS-1-VA	DLS-1-TX		
VSXCXL-2-VA	DLS-1-VA	DLS-1-TX		
VS-1-VA-for-MDSM	DLS-3-VA	DLS-3-TX		
VS-1.2-VA	DLS-5-VA	DLS-5-TX		
VS-1.3-VA	DLS-5-VA	DLS-5-TX		
VS-1.4-VA	DLS-5-VA	DLS-5-TX		
VS-2.2-VA	DLS-5-VA	DLS-5-TX		
VS-2.3-VA	DLS-5-VA	DLS-5-TX		
VS-2.4-VA	DLS-5-VA	DLS-5-TX		

Log forwarding from Log or Management Servers:

DLS-1-VA	(active)	forward logs to:	SIEM-VA
DLS-2-VA	(standby)	forward logs to:	SIEM-TX
DLS-3-VA	(active)	forward logs to:	SIEM-VA
DLS-4-VA	(standby)	forward logs to:	SIEM-TX
DLS-5-VA	(active)	forward logs to:	SIEM-VA

TX

Cluster or Gateway	Log to: Send logs and alerts to these log servers: 1	2	In case one of the above servers is unreachable, send logs to: 1	2
VSXCXL-1-TX	DLS-2-TX	DLS-2-VA		
VS-1-TX-for-MDSM	DLS-4-TX	DLS-4-VA		
VS-1.2-TX	DLS-5-TX	DLS-5-VA		
VS-1.3-TX	DLS-5-TX	DLS-5-VA		
VS-1.4-TX	DLS-5-TX	DLS-5-VA		

Log forwarding from Log or Management Servers:

DLS-1-TX	(standby)	forward logs to:	SIEM-VA
DLS-2-TX	(active)	forward logs to:	SIEM-TX
DLS-3-TX	(standby)	forward logs to:	SIEM-VA
DLS-4-TX	(active)	forward logs to:	SIEM-TX
DLS-5-TX	(standby)	forward logs to:	SIEM-VA

Multi-Domain Security Management Infrastructure
Architecture recommendations for:

Logging
Single Site

PiggyBank

Vladimir Yakovlev

Mar 10, 2017

Table 3
Rev 2.0

Higher Intelligence
Information Technology, Infrastructure & Security Services

VA

Cluster or Gateway	Log to: Send logs and alerts to these log servers: 1	2	In case one of the above servers is unreachable, send logs to: 1	2
VSXCXL-1-VA	DLS-1-VA	SIEM-VA	DLS-1-TX	SIEM-TX
VSXCXL-2-VA	DLS-1-VA	SIEM-VA	DLS-1-TX	SIEM-TX
VS-1-VA-for-MDSM	DLS-3-VA	SIEM-VA	DLS-3-TX	SIEM-TX
VS-1.2-VA	DLS-5-VA	SIEM-VA	DLS-5-TX	SIEM-TX
VS-1.3-VA	DLS-5-VA	SIEM-VA	DLS-5-TX	SIEM-TX
VS-1.4-VA	DLS-5-VA	SIEM-VA	DLS-5-TX	SIEM-TX
VS-2.2-VA	DLS-5-VA	SIEM-VA	DLS-5-TX	SIEM-TX
VS-2.3-VA	DLS-5-VA	SIEM-VA	DLS-5-TX	SIEM-TX
VS-2.4-VA	DLS-5-VA	SIEM-VA	DLS-5-TX	SIEM-TX

Log forwarding from Log or Management Servers:

DLS-1-VA	(active)	forward logs to:	DLS-1-TX
DLS-2-VA	(standby)	forward logs to:	DLS-2-TX
DLS-3-VA	(active)	forward logs to:	DLS-3-TX
DLS-4-VA	(standby)	forward logs to:	DLS-4-TX
DLS-5-VA	(active)	forward logs to:	DLS-5-VA

TX

Cluster or Gateway	Log to: Send logs and alerts to these log servers: 1	2	In case one of the above servers is unreachable, send logs to: 1	2
VSXCXL-1-TX	DLS-2-TX	SIEM-TX	DLS-2-VA	SIEM-VA
VS-1-TX-for-MDSM	DLS-4-TX	SIEM-TX	DLS-4-VA	SIEM-VA
VS-1.2-TX	DLS-5-TX	SIEM-TX	DLS-5-VA	SIEM-VA
VS-1.3-TX	DLS-5-TX	SIEM-TX	DLS-5-VA	SIEM-VA
VS-1.4-TX	DLS-5-TX	SIEM-TX	DLS-5-VA	SIEM-VA

Log forwarding from Log or Management Servers:

DLS-1-TX	(standby)	forward logs to:	DLS-1-VA
DLS-2-TX	(active)	forward logs to:	DLS-2-VA
DLS-3-TX	(standby)	forward logs to:	DLS-3-VA
DLS-4-TX	(active)	forward logs to:	DLS-4-VA
DLS-5-TX	(standby)	forward logs to:	DLS-5-VA

Multi-Domain Security Management Infrastructure Architecture recommendations for:

Logging
MDLS' and SIEM

PiggyBank

Vladimir Yakovlev

Mar 10, 2017

Table 3

Rev 2.0

Higher Intelligence
Information Technology, Infrastructure & Security Services

VA

Cluster or Gateway	Use the following Management Stations for fetch and install:	
	1	2
VSXCXL-1-VA	DMS-1-VA	DMS-1-TX
VSXCXL-2-VA	DMS-1-VA	DMS-1-TX
VS-1-VA-for-MDSM	DMS-3-VA	DMS-3-TX
VS-1.2-VA	DMS-5-VA	DMS-5-TX
VS-1.3-VA	DMS-5-VA	DMS-5-TX
VS-1.4-VA	DMS-5-VA	DMS-5-TX
VS-2.2-VA	DMS-5-VA	DMS-5-TX
VS-2.3-VA	DMS-5-VA	DMS-5-TX
VS-2.4-VA	DMS-5-VA	DMS-5-TX

TX

Cluster or Gateway	Use the following Management Stations for fetch and install:	
	1	2
VSXCXL-1-TX	DMS-2-TX	DMS-2-VA
VS-1-TX-for-MDSM	DMS-4-TX	DMS-4-VA
VS-1.2-TX	DMS-5-TX	DMS-5-VA
VS-1.3-TX	DMS-5-TX	DMS-5-VA
VS-1.4-TX	DMS-5-TX	DMS-5-VA

Multi-Domain Security Management Infrastructure Architecture recommendations for:

Policy Sources PiggyBank

Vladimir Yakovlev

Mar 10, 2017

Table 3

Rev 2.0

Higher Intelligence