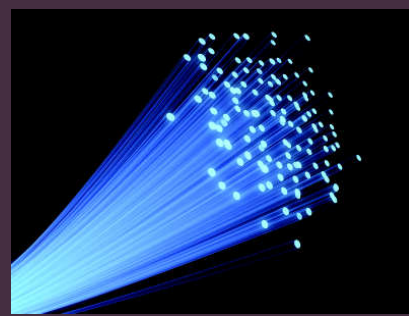


WHITE PAPER

Secure Routing Features in Thinklogical's VX Router



A Thinklogical White Paper

By Greg Goblirsch

Senior Systems Engineer - Thinklogical

Evaluating and deploying the right infrastructure solutions are important steps for protecting the confidentiality, integrity and availability of critical data. This white paper will outline how to limit security risks with Thinklogical's VX Router solution, which includes a comprehensive overview of key product features and how to implement them in your existing system security landscape.

Introduction

When mission-critical applications are in play, system integrators and administrators understand that it is essential to provide users with a secure system that leaves little room for downtime. Consider users in a military command-and-control center, where they must react swiftly to urgent event information and a system slow down or fault could potentially have disastrous consequences. In addition, accessing sensitive data is of paramount importance in these types of environments. In many instances, end users need to switch between two or more computers, possibly at different classification levels, thus introducing data vulnerability. In these types of environments, strict security rules for the protection of classified information apply, specifically in what is known as red and black networks. For example, where networks with different security classifications are connected, it must be absolutely certain that classified information processed solely in trustworthy red networks is never transferred to black networks, where unauthorized personnel would have access to it. Therefore, a routing and extension system that is deployed in the most stringent of secure environments must not only have fail proof security features, but also meet a variety of security regulations.

What Sets Thinklogical Apart

For over a decade Thinklogical's products have been engineered and designed with secure computing applications in mind. Our products and solutions play a critical role in helping military and government departments and agencies overcome security infrastructure concerns, as well as collaboration and information sharing issues. Therefore, Thinklogical is the only provider in the marketplace today that has established an Information Assurance (IA) methodology across its entire line of VX routing products. This in turn has enabled Thinklogical to achieve the prestigious accreditation for Common Criteria EAL-4 certification.

Common Criteria is an internationally recognized set of guidelines which define a common framework for evaluating security features and capabilities of Information Technology products. The standard consists of several predetermined evaluation assurance levels, each one more stringent than the last. Once completed, Common Criteria certifications are accepted by NATO through the Common Criteria Recognition Agreement (CCRA).

Common Criteria EAL-4 accreditation confirms that the unique and proprietary VX technology provides secure data separation in restricted switching environments where secure access between source and destination end points is critical. This provides the ability to establish "Red/Black" levels of access within a single system, which is critical in complex, multi-layered secure military and government environments. In addition, the VX Router product line also meets the regulatory and security demands for the Energy and Utilities markets.

A New Secure Architecture – Partitioning and Restricted Switching

Thinklogical's VX Router uses two methods for secure routing. Method one is what is known as partitioning and method two is restricted switching. These methods can be deployed singularly or jointly depending on security parameters and requirements.

Partitioning

Partitions allow VX Router sources and destinations to be segregated. Therefore, destination workstations will only receive signals that are transmitted from source computers in the same partition. In addition, it is impossible for a source computer to be inadvertently routed outside of its designated partition; the signals simply will not be transmitted.

The following example shows a VX80 Router with four distinct partitions.

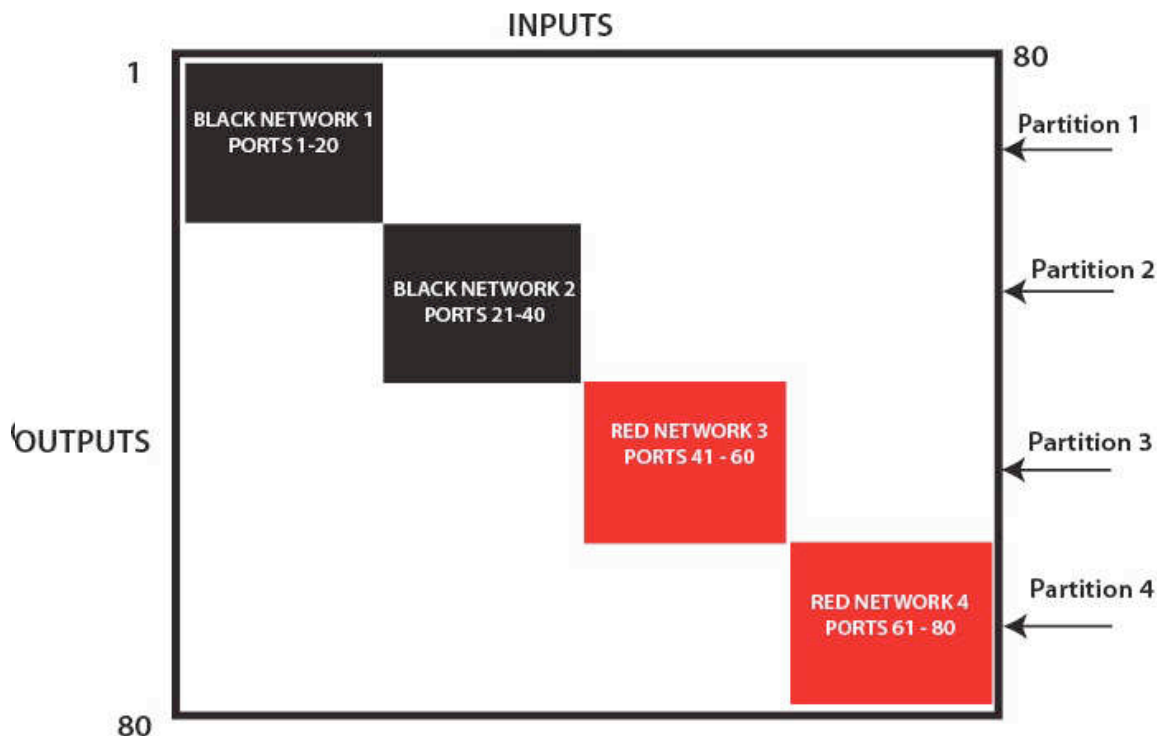


Figure 1: Four partitions set up for secure routing and extension applications. Signals are only capable of transmitting and receiving within a single partition, not across partitions.

The maximum number of partitions is the number of ports that make up the VX Router (80, 160, 320). A VX40 or VX80 Router could potentially be configured with up to 80 partitions, a VX160 up to 160, and so forth. There are also a number of possible overlapping partition configurations.

The following example shows a VX80 Router with an overlapping partition.

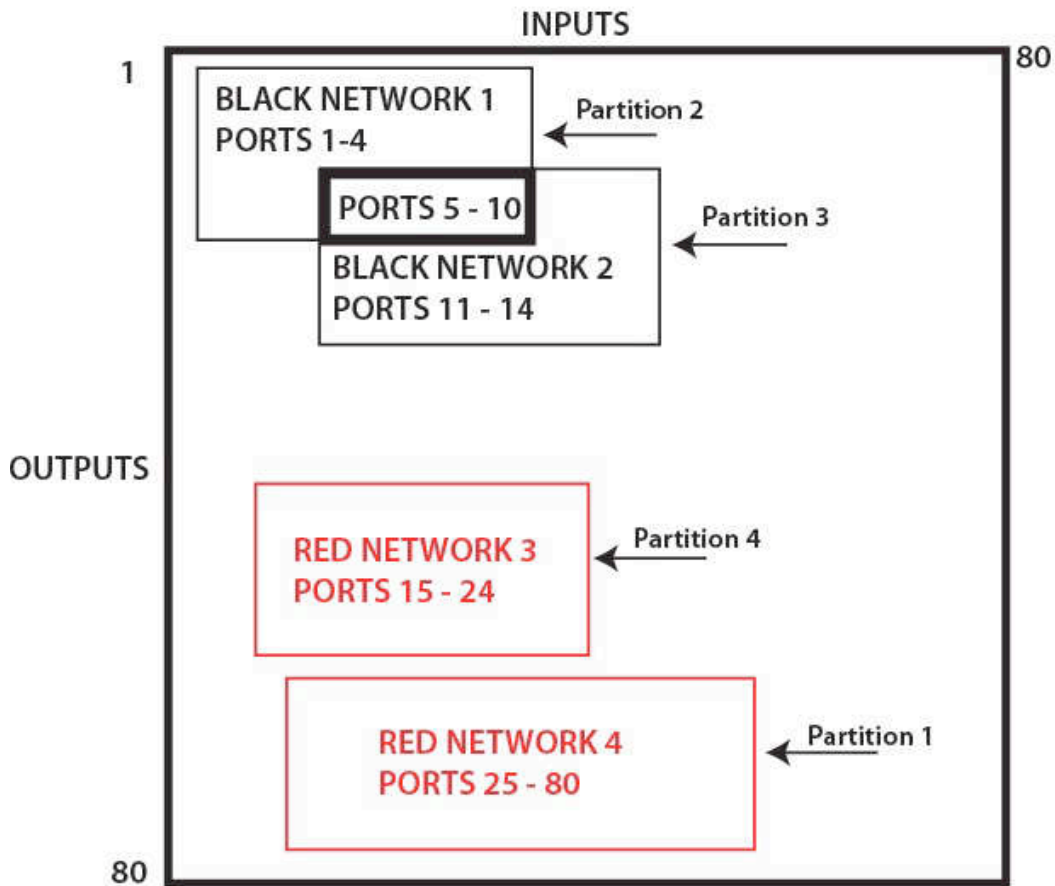


Figure 2: In this diagram the VX80 has four partitions, with ports 5 – 10 accessible to both partition 2 and 3.

The user must provide a table defining the partitions. This table is in the form of a comma separated value (csv) file located in `/var/local/router/partition` on the VX Router. This file contains the port number and partitions it belongs to. The configuration file for the above scenario would look like this:

```
"Port", "Partition"  
1, 2  
2, 2  
3, 2  
4, 2  
5, 2,3  
6, 2,3  
7, 2,3  
8, 2,3  
9, 2,3  
10, 2,3  
11, 3  
12, 3  
13, 3  
14, 3  
15, 4  
16, 4  
17, 4  
18, 4  
19, 4  
20, 4  
21, 4  
22, 4  
23, 4  
24, 4
```

NOTE: All ports not listed default to partition 1. Ports can be explicitly added to partition 1.

The VX router will interpret the Partition Table csv file during boot-up. The csv file must be located in /var/local/router/partition on the VX Router. Any errors that occur during the Partition Table interpretation process will be logged to /var/log/messages.

It is recommended that the messages file be reviewed and any errors in the Partitioning Table be corrected. It is also recommended that Partitioning be fully tested before implementing multiple partitions on the same VX Router.

The VX40 or VX80 Router can support up to 80 partitions. They require one table named upstream.csv. This table can have up to 80 ports and 80 partitions. The VX160 Router can support 160 partitions for upstream to downstream paths and another 160 partitions for downstream to upstream paths. Two tables are required named upstream.csv and downstream.csv. The tables can have up to 160 ports and 160 partitions. The VX320 Video Router can support 320 partitions. One table is required named upstream.csv. The table can have 320 ports and 320 partitions. Lastly, the VX320 Router can support 320 partitions for the upper card cage and 320 partitions for the lower card cage. Two tables are required named upstream.csv and downstream.csv. The tables can have up to 320 ports and 320 partitions.

Partitioning is disabled when the Partitioning Table files are removed. By default, when there are no Partitioning Table files, all input and output ports are in partition 1. All VX Routers are shipped without Partitioning Table files stored on the controller card and therefore do not restrict connections.

NOTE: When using a Back-up Controller configuration, both controllers must have the same Partitioning Table files.

Restricted Switching

Restricted Switching is used to provide for multiple levels of security classifications within the same VX Router. Each destination needs to ensure that no unauthorized content is displayed or accessed. Therefore, each input and output needs to be prioritized. Priorities can range from 1 to the number of ports in a VX Router. An output can connect to an input with a priority less than or equal to its priority. Thus, a priority level of 1 on an output can connect to any input (priority 1,2,3,...).

The user must provide a table defining the priorities for each input and output of the switch matrix. This table is in the form of a comma separated value (csv) file. This file contains the values in three columns, Port Direction (i=input, o=output), Port Number, Port Priority. See figure 3 on the following page for an example of a Restricted Switching scheme.

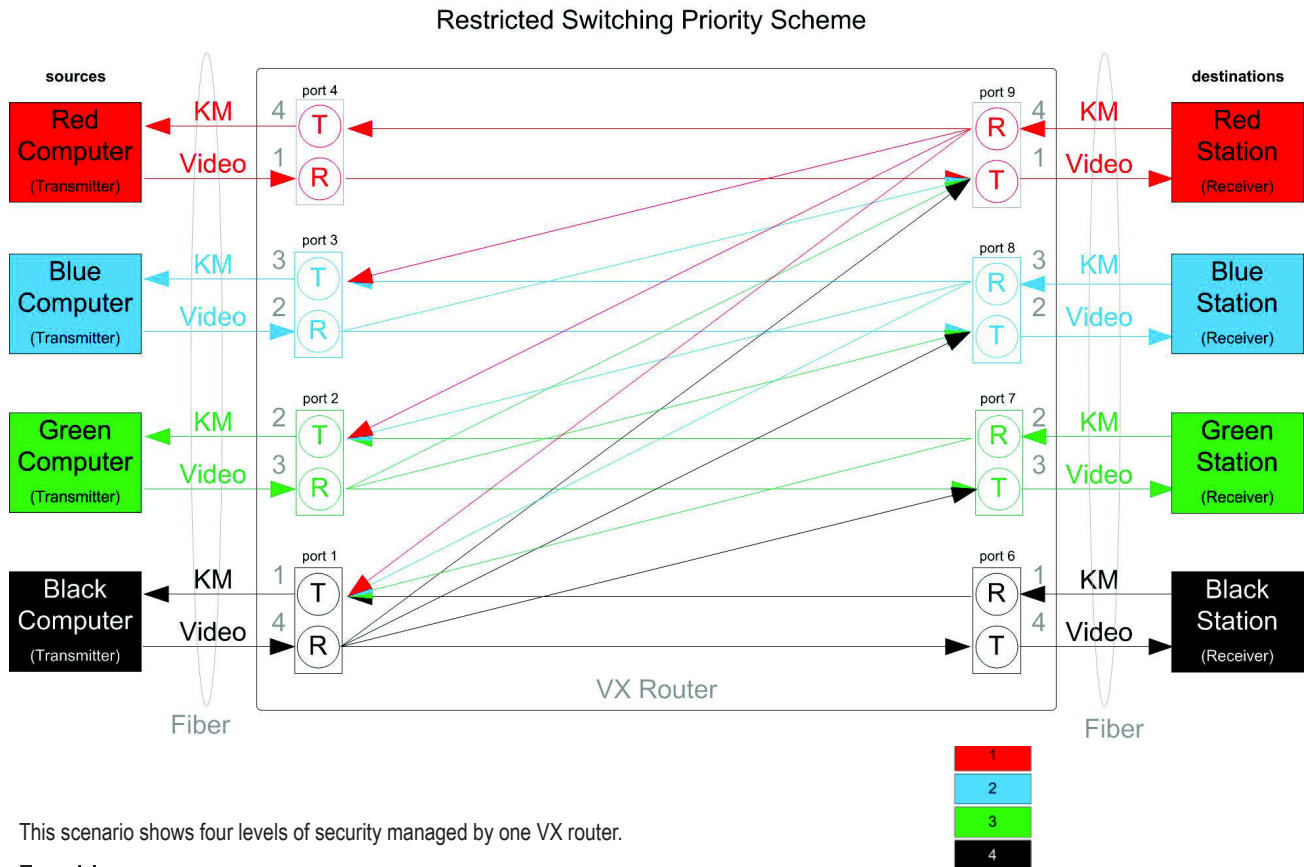
The VX Router will interpret the Restricted Switching Table csv file during boot-up. The csv file must be located in `/var/local/router/restrict` on the VX Router. Any errors that occur during the Restricted Switching Table interpretation process will be logged to `/var/log/messages`.

It is recommended that the messages file be reviewed and any errors in the Restricted Switching Table be corrected. It is also recommended that Restricted Switching be fully tested before implementing multiple levels of security classification domains on the same VX Router.

The VX40 and VX80 Routers contains a single 80 by 80 matrix switch. It requires 1 table named `upstream.csv` listing priority levels of input ports 1-80 and output ports 1-80. Any input or output ports that are not listed in the table will default to a priority of 1.

The VX160 Router contains a single 160 by 160 matrix switch for the upstream to downstream switching paths and another 160 by 160 matrix switch for the downstream to upstream switching paths. The first table named `upstream.csv` lists priority levels of upstream input ports 1-160 and downstream output ports 1-160. The second table named `downstream.csv` lists priority levels of downstream input ports 1-160 and upstream output ports 1-160. Any input or output ports that are not listed in the tables will default to a priority of 1.

Restricted Switching with VX Routers



This scenario shows four levels of security managed by one VX router.

For video:

- destination workstations in the **red** network can see what is transmitted by source computers in the **black, green, blue, and red** networks
- destination workstations in the **blue** network can see what is transmitted by source computers in the **black, green, and blue** networks
- destination workstations in the **green** network can see what is transmitted by source computers in the **black and green** networks
- destination workstations in the **black** network can see what is transmitted by source computers in the **black** network only

For keyboard and mouse:

- destination workstations in the **red** network can control source computers in the **black, green, blue, and red** networks
- destination workstations in the **blue** network can control source computers in the **black, green, and blue** networks
- destination workstations in the **green** network can control source computers in the **black and green** networks
- destination workstations in the **black** network can control source computers in the **black** network only

Restricted switching is configured via firmware loaded to the VX router. The configuration file for this scenario would look like (where the first value is "i" for input or "o" for output, the second value is the port number, and the third value is the priority level).

Important Notes:

- In this scenario, ports 1, 2, 3, 4 in card 1 and ports 6, 7, 8, 9 in card 2 are used; however, any ports on any cards could be used. (Each card has five ports numbered 1–5 bottom to top.)
- The number of priority levels you can manage by one VX router is the same as the number of ports in that VX router: a VX40 or VX80 can support 80 priority levels, a VX160 can support 160 priority levels, a VX320 or VX320 Video can support 320 priority levels.

"i",1,4
 "i",2,3
 "i",3,2
 "i",4,1
 "i",6,1
 "i",7,2
 "i",8,3
 "i",9,4
 "o",1,1
 "o",2,2
 "o",3,3
 "o",4,4
 "o",6,4
 "o",7,3
 "o",8,2
 "o",9,1

Figure 3: Example of Restricted Switching scheme

The VX320 Video Router contains a single 320 by 320 matrix switch. It requires 1 table named upstream.csv listing priority levels of input ports 1-320 and output ports 1-320. Any input or output ports that are not listed in the table will default to a priority of 1.

The VX320 Router contains a single 320 by 320 matrix switch located in the upper card cage and another 320 by 320 matrix switch located in the lower card cage. The first table named upstream.csv lists priority levels of upper card cage input ports 1-320 and upper card cage output ports 1-320. The second table named downstream.csv lists priority levels of lower card cage input ports 1-320 and lower card cage output ports 1-320. Any input or output ports that are not listed in the tables will default to a priority of 1.

Restricted switching is disabled when Restricted Switching Table files are removed. By default, when there are no Restricted Switching Table files, all input and output ports will have a priority of 1. All VX Routers are shipped without Restricted Switching Table files stored on the Controller card and therefore do not restrict connections.

NOTE: When using a Back-up Controller configuration, both controllers must have the same Restricted Switching Table files.

Administration Access

There are only two methods by which the administrator can access the VX Router Controller Configurations:

1. Using the serial console directly connected to the VX Router.

It should be noted that while no administrator password is required to use the serial console, physical access to the router is required. Therefore, the router should be stored in a physically secure location to avoid unauthorized access which may lead to the router being placed in an unsecured state.

2. Using SSH access

The router allows SSH connections to the router for management purposes. SSH sessions are authenticated using an encrypted password file.

Secure Application Examples

The secure application diagrams that follow depict a VX Router in secure application designs. The highly secure networks are described as the Red Network and the other lower security networks are described as the Black Network. The Red Network containing the computers (sources) are shown in a physically secure environment along with the VX Router, the computer server used to manage the Router, and the Network Hub. The Network Hub is on a dedicated network that is only used to connect the VX Router to the computer server. This dedicated network does not connect to any other components and does not extend beyond the physically secure environment. The dedicated network connection could be replaced by a direct serial connection (RS-232) between the VX Router and the computer server.

Note that the VX Router and the computer server used to manage the Router must be protected according to the highest security classification of any component in the entire network application. In addition, the optical connections and DESTINATION receiver designated as the Red Network must be physically secure.

The configuration of the VX Router should be reviewed on a regular basis to ensure that the configuration continues to meet the organizational security policy in the face of the following:

- Changes in the VX Router configuration
- Changes in the organizational security policy
- Changes in the threats presented from the untrusted network interfaces
- Changes in the administration and operation staff or the physical environment of the VX Router application

The VX Router can be configured to prevent accidental connection from the Red Network to the Black Network using the Restricted Switching feature. For example, the VX40 Matrix Router Network in figure 4 would be configured with the following .csv file:

```
I,1,2  
I,2,2  
O,2,2  
I,42,2  
O,41,2  
O,42,2  
I,5,1  
O,5,1  
I,45,1  
O,45,1
```

So that the following connection rules will apply:

SOURCE 2 can be connected only to DESTINATION 2.

SOURCE 1 can be connected to both DESTINATION 1 and DESTINATION 2.

Restricted Switching within Partitions

Restricted Switching can also be configured within VX Router partitions for an additional level of security and control. In figure 4 putting ports 1, 2, 5, 41, 42, and 45 into a unique partition ensures no other ports other than those listed can be connected regardless of priority.

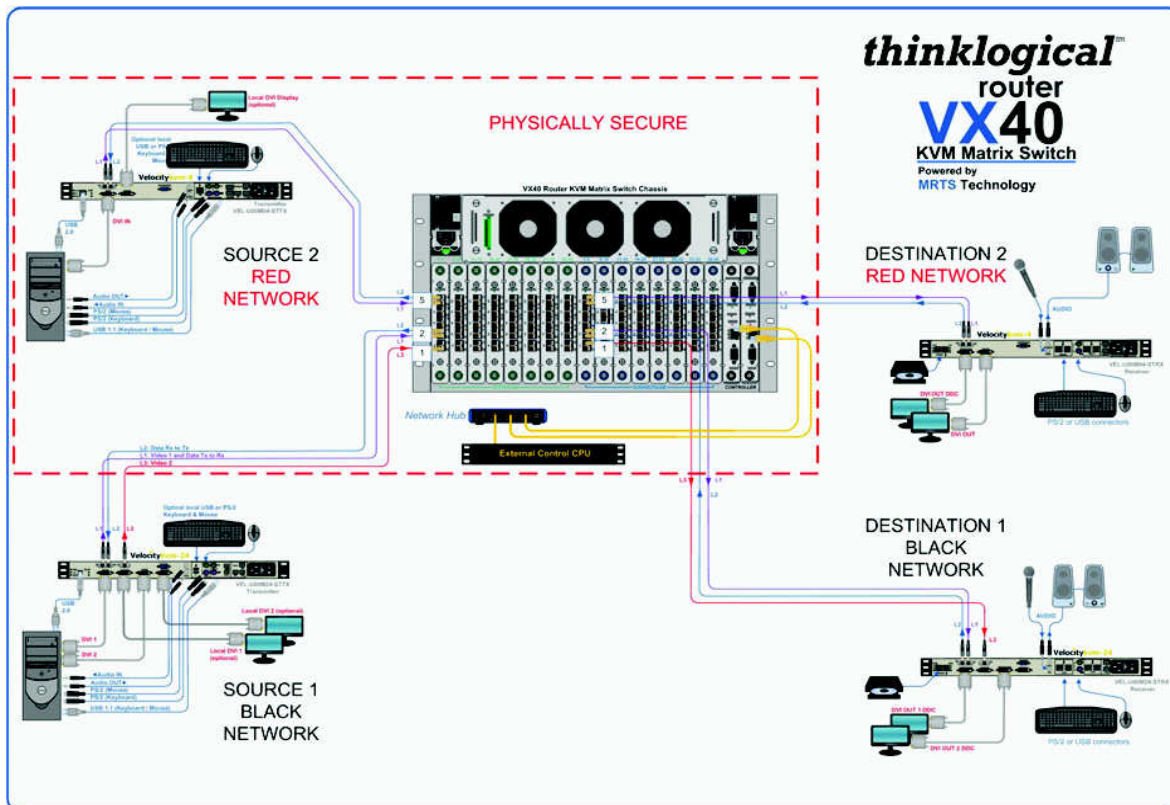


Figure 4: VX40 secure application using both partitioning and Restricted Switching

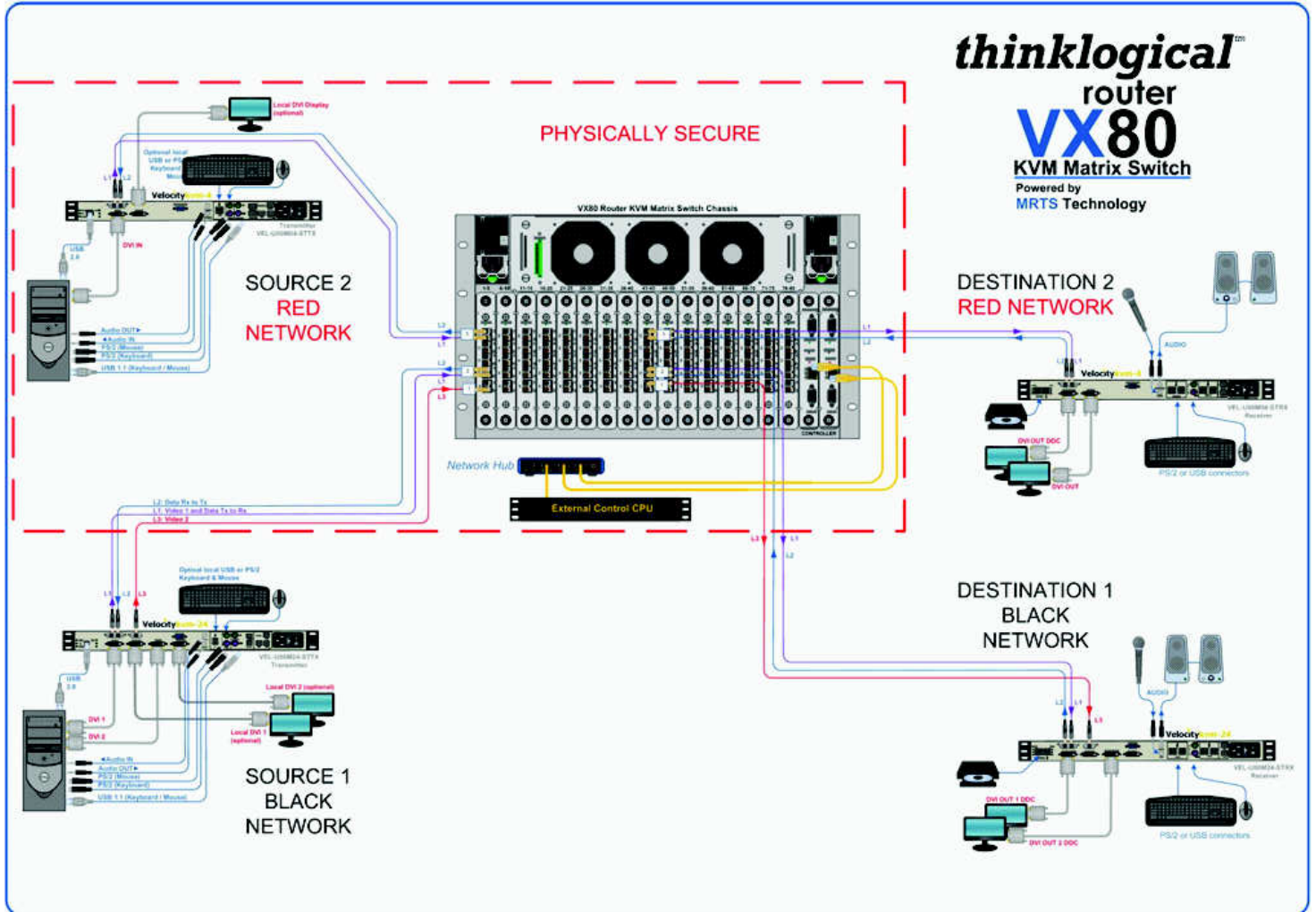


Figure 5: VX80 secure application

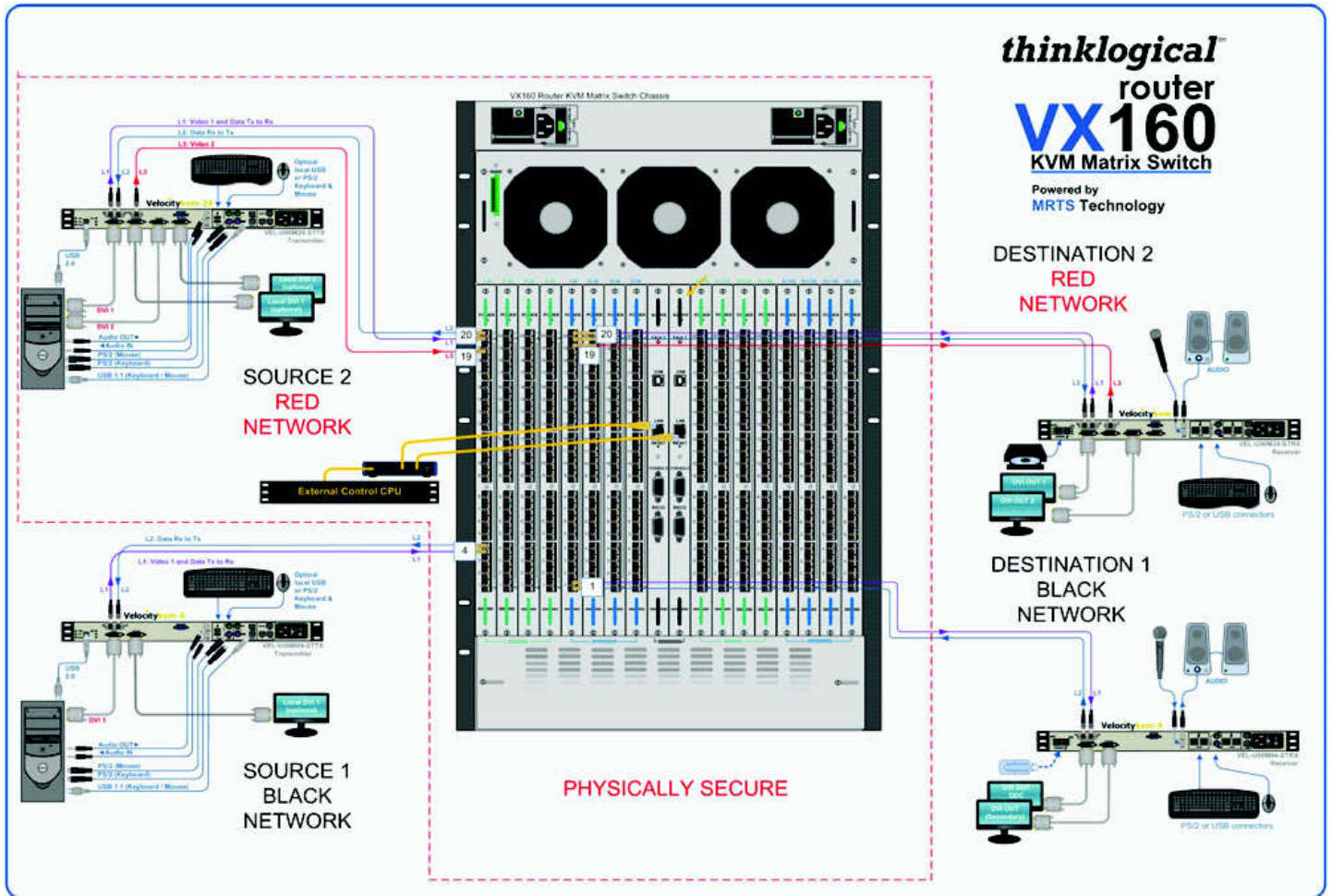


Figure 6: VX160 secure application

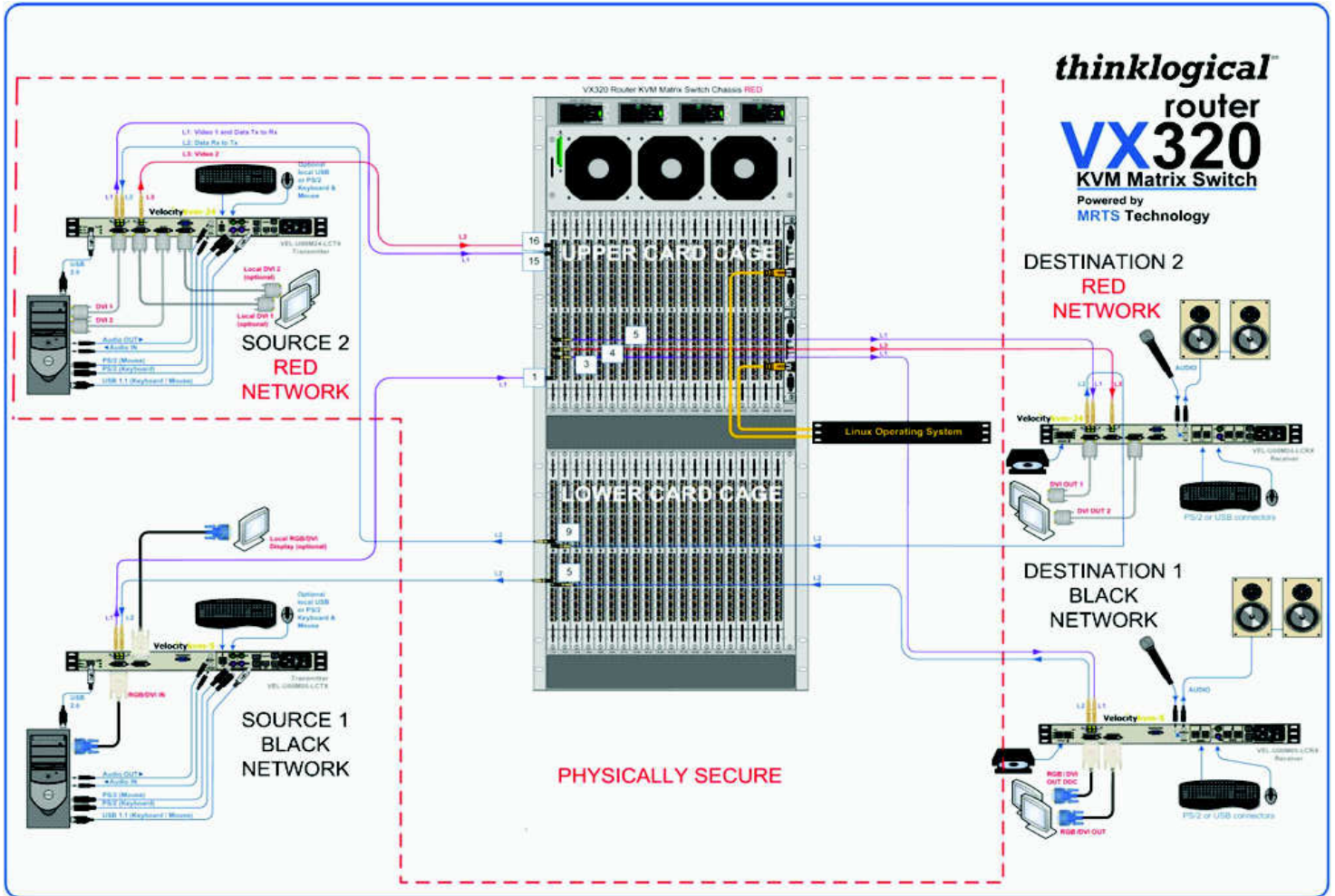


Figure 7: VX320 secure application



thinklogical[®]
Extend • Distribute • Innovate

October 2011

© 2011 Thinklogical. All rights reserved.

Thinklogical claims or other product information contained in this document are subject to change without notice. This document may not be reproduced, in whole or in part, without the express written consent of Thinklogical.