

Abstract

Many organizations are finding the need to protect themselves with isolation routers, firewalls, and other technologies. At the same time they are doing more and more collaboration with external organizations. This creates a problem when local services and resources need to be shared with external organizations.

There are many ways to approach this problem. For Example, a VPN (Virtual Private Network) can give external clients secure access to local services and resources maintained by your organization.

In some case, however, it is necessary to have copies/replicas/shadows of a services or resources at remote locations. This would provide an external organization faster access to your services and resources, and in the case of disrupted communications, continued operations.

A remote server, maintained by your organization, at a remote location could provide copies/replicas/shadows of services and resources. This requires that each service and/or resource support secure communications between your organization and the remote location. Some form of access control must also be maintained. There may also be secure communications requirements between the servers and resources and clients that use them.

This paper defines a remote node architecture that can house multiple services and resources. The architecture provides secure communication between your organization and the remote node for all services and resources. It also provides secure communications between the services and resources and the clients that use them.

A prototype of the remote node architecture was built and tested. This paper describes the design, the hardware and the configuration of the prototype that was built. Key points in the development of the prototype are discussed as well as specific hardware configurations.

Two initial design decisions guided the development of the prototype. COTS products were to be used and an existing PKI implementation was to provide the security infrastructure.