Maintaining Remote Services and Resources Over the Internet (and Other Networks)

Thomas L. Wolfe
Jet Propulsion Laboratory
Thomas.L.Wolfe@jpl.nasa.gov

Yin-Chiao Joseph Liu
Jet Propulsion Laboratory
Yhi-Chiao.Liu@jpl.nasa.gov

Hsin-Ping Pat Chang
Jet propulsion Laboratory
Hsin-Ping@jpl.nasa.gov

Abstract

Many organizations are discovering the need to protect themselves with isolation routers, firewalls, and other technologies. Simultaneously they are collaborating more and more with external organizations. When local services and resources must be shared externally, problems arise.

There are many approaches to these problems. For example, a Virtual Private Network (VPN) can provide external users secure access to services and resources maintained by your organization.

In some cases, however, it is necessary to have copies/replicas/shadows of services or resources at remote locations. This presence allows the external organization faster access to your services and resources, and in the event of disrupted communications, continued operations.

A server maintained by your organization at a remote site could provide copies/replicas/shadows of local services and resources. Offering services and resources via remote servers means that your organization must also control access to these services and resources, that all services and resources support secure communications between the remote site and your organization and between all users and themselves (the services and resources) as well.

This paper defines a Remote Node Architecture (RNA) that can house multiple services and resources. The RNA provides secure communications between the remote node and your organization for all services and resources, and between its services and resources and the users thereof.

The RNA proposed in this paper is being prototyped and the configuration will be documented elsewhere. After all, the devil is in the details.

1 Introduction

Many organizations are erecting protective boundaries around themselves. They use isolation routers, firewalls, and other technologies. At the same time the global environment mandates that they collaboration with external organizations. How can these entities maintain security and pool resources? This paper describes several ways of extending your organization's services and resources to remote sites without compromising security.

An example of a remote service is a directory where public PKI certificates are maintained. By providing a replicated copy at the remote site, the external organization can access a local server for public certificates rather than connecting to your directory. This provides faster access to PKI certificates and, in the case of disrupted communications, continued operations.

1.1 VPNs

Virtual Private Networks (VPNs) (see figure 1) may be used to grant remote users access to services and resources within your organization. This is a simple and effective solution to sharing while keeping all of the services and resources within the home organization.

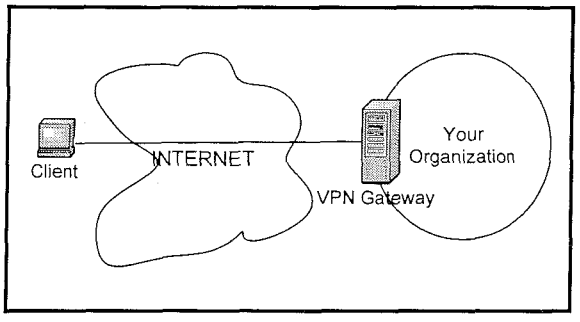

Figure 1: Virtual Private Network architecture

2.2 Remote Servers

There may be a need for some services and resources at remote locations. The use of remote servers (see figure 2) provides copies/shadows/replicas of services and resources at remote locations. Many Commercial Off The Shelf (COTS) products support this method of operation. However, not all provide a method of securing communications between the local and remote servers. Also, many existing systems developed in house fail to provide secure communications and/or replication.

A remote service may also require its own remote auxiliary support services. For example, a remote service may require access to a RADIUS (Remote Authentication Dial In User Service) for user authentication. You may want a copy of the RADIUS server at sites where the remote service is located.

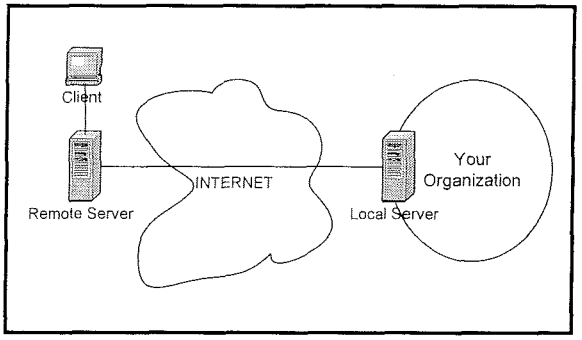

Figure 2: Remote server architecture

1.3 Remote Node Architecture

The Remote Node Architecture (RNA) (see figure 3) described in this paper provides security for many services and resources and limits access to them. For remote clients, a VPN connection to the remote node is provided. With this architecture, the services and resources do not need to provide their own communications security; the RNA provides it for them.

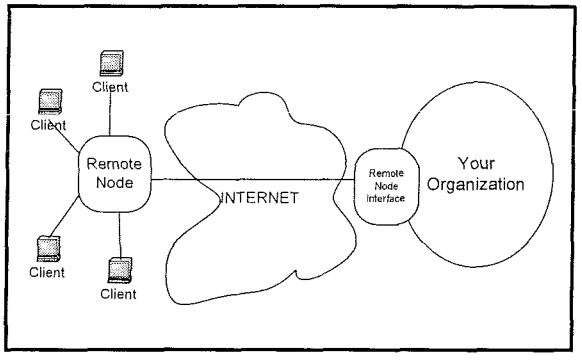

Figure 3: Remote node architecture

2 The Remote Node's (Logical) Architecture

The easiest way to understand the RNA is to first look at the logical components of that make up the architecture and the functions they perform. It should be stressed that these are logical - not actual components. An actual prototype of this architecture will be described in another paper.

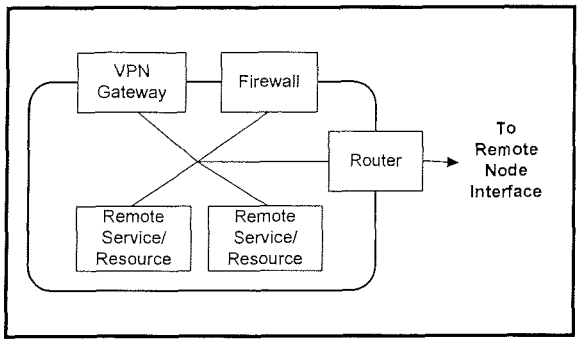

Figure 4: Remote node's (logical) diagram

Figure 4 shows the logical components that a remote node comprises. The functionality provided by each component follows:

VPN Gateway – provides VPN connectivity for remote clients. This allows secure communications between remote clients and the services and resources in the remote node. Remote users must authenticate themselves and be authorized before they are allowed to access the remote node's services and resources.

Firewall - provides protection by limiting communications to those services and resources that unauthenticated users may access.

The firewall also restricts traffic going out of the remote node. Some remote node services and resources may require access to things outside of the remote node; for example, a time service.

Router – provides secure communications (using IPSEC) between the remote node and the remote node's interface located at your organization. This is the only place traffic from inside the remote node is routed.

Remote service/Resource – provides copies/shadows/replicas of services and resources from your organization.

3 The Remote Node's Interface (Logical) Architecture

The easiest way to understand the Remote Node's Interface (RNI) architecture is to first look at its logical components and the functions they perform. It should be stressed that these are logical - not actual components. An actual prototype of this architecture will be described in another paper.

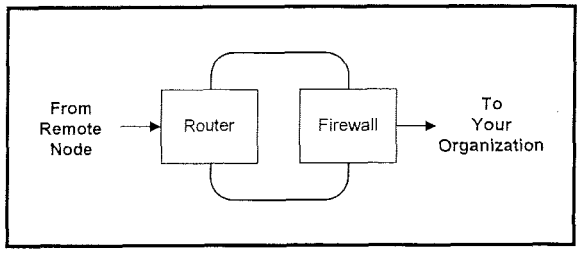

Figure 5: Remote node's interface (logical) diagram

Figure 5 shows the logical components that a remote node's interface comprises. The functionality provided by each component follows:

Firewall – provides limited access to your organization's services and resources. This restricts traffic coming from the remote node to a limited set of protocols, IP addresses, etc.

The firewall also restricts the type of traffic going to the remote node from your organization.

Router – provides secure communications (using IPSEC) between the remote node interface located at your organization and the remote node located at an external organization. This is the only place traffic from the remote node interface is routed.

4 Location, Location, Location

Many organizations scan network traffic going in and out of their organization. They may require that the traffic be transmitted in the clear so that the traffic can be analyzed. These policies will determine if the remote node or remote node interface is inside, outside or in the DMZ of an organization's isolation router, firewall, etc.

5 IP Addresses

All servers within a remote node have three IP addresses. They have an IP address within the Remote Node itself. They also have an IP address in the external organizations address space and an IP address within your organization's address space. Each organization views the server as local and having a local IP address. The internal IP address allows the RNA to route messages internally to the correct location.

6 The Physical Security Issues

The major issue with servers and equipment and especially remote servers and equipment is physical access. Without physical security that limits access to the servers and equipment, there can be no assumption or expectation of security. When working with external organizations that will host your remote node equipment, policies and procedures must be in place that insure physical security. Depending on the sensitivity of the data on the remote node, regular inspections of the servers and equipment are appropriate. To verify that the policies and procedures are being followed, auditing of access logs and other normal security measures are also appropriate.

7 A Digression On Security

Many organizations will purchase leased lines for their network and use them to send data in the clear. They then make statements like, "We have secure communications." Nothing could be further from the truth. They have just (potentially) exposed their data to everyone who works for the carrier from which they leased the lines. This could be a critical problem if the lines go through a foreign country.

The same problem exists within an organization. Statements like "Transmitting of data in the clear is OK because the LAN is switched" are not true. In fact the data is (potentially) exposed to everyone in the organization's networking group, any one who has access to the equipment closets, etc.

By the way, who has keys to almost very room in your organization? The janitor.

8 Conclusion

Collaboration between external organizations and your organization may require access to your internal services and resources. Other factors may require you to maintain copies/replicas/shadows of local services and resources at remote locations. This paper defines a remote node architecture that can provide these remote services and resources in a secure way.

A prototype of the architecture is being built and demonstrated. The implementation will be documented in a later paper.

9 Acknowledgments

The research described in this paper is being carried out at the Jet Propulsion Laboratory, California Institute of Technology, under contract with the National Aeronautics and Space Administration.

10 References

[1] Check Point™ Getting Started Guide
[2] Cisco Secure VPN Client Solutions Guide
[3] Entrust PKI and Check Point™ 2000 Install And Interoperability Guide
[4] Entrust Technical Note TN1058, How Enroll a Cisco Router With Entrust VPNConnector
[5] Entrust/VPNConnector 5.0 User Guide
[6] ISOWan Requirements Document, Jet Propulsion Laboratory