IPAM and VPN

Jared Broyhill

University of Advancing Technology

Author Note

This paper was prepared for NTW216, taught by Professor Mason Galatas.

Abstract

The purpose of this paper is to explain IPAM (Internet Protocol Address Management) and VPN (Virtual Private Network) as they relate to Window Servers, and how to realistically implement them onto such a server.

IPAM and VPN

IPAM and VPN are both things that can be implemented into a Windows Server due to Microsoft providing explicit utilities to do so. Through implementing IPAM, a system administrator can see IP (Internet Protocol) addresses connected to the server, audit activity and changes done through these addresses, automatically discover DHCP (Dynamic Host Configuration Protocol) servers and DNS (Domain Name Server), manage access scopes using PowerShell, and a host of other configuration abilities. VPN, on the other hand, allows an administrator to save cost by circumventing long-distance calls, tunnel information, and encrypt said information to keep it safe. Through use of built-in modules, both IPAM and VPN can be configured and optimized for a variety of uses via Windows Server.

IPAM

IPAM, like many other features in Windows Server 2016, can be installed directly through the Server Manager. By going to Add Roles and Features, a user can select IPAM by installation on their system. Afterwards, IPAM (which will attempt to locate DNS and DHCP servers along with domain controllers) can be provisioned either manually or by using group policy. Next, server discovery can be configured, IP addresses can be blocked, and ranges can be setup. Next, resource records can be enabled and configured through use of the “Add Resource Record” wizard. Following that, DNS zones can be created and edited through the “Monitor and Manage” module along with a DHCP scope. Through the same module, DHCP policies can be setup to as well.

Finally, Role-based Access Control can be configured through the “Access Control” module and auditing can be configured through the Event Catalog. With all of these configurations finished, a system administrator can now monitor, configure, and audit all kinds of access and control to the server through the IPAM module. IPAM is essential enough to be a must-have in any server configuration of any organization that wishes to operate optimally and be taken seriously.

VPN

Just like IPAM, VPNs can be installed through use of the Add Roles and Features node (specifically, DirectAccess and VPN (RAS)). Next, through opening Routing and Remote Access, an Ethernet adapter can be connected and configured for a Remote Access Server. Logging settings for Remote Access can be configured through the Remote Access Logging and Policies folder and then NPS (Network Policy Server). A Network Access Policy can then be created through NPS as well, and specific Day and Time Restrictions can be configured per the administrator’s desires, along with other constraints.

Next, should the administrator wish it, a User Profile can be restricted for Dial-in Access through the Local Users and Groups folder. Following that, Encryption can be configured through NPS. Finally, a VPN network Access Policy can also be configured through NPS.

The configurations on the VPN will allow an administrator to not only offer the VPN itself for a fast access to enterprise infrastructure. Additionally, restrictions can ensure that people who aren’t permitted can’t access the network along with those who shouldn’t be accessing it at certain times. The auditing of network activity will also allow an administrator to monitor what goes on in the network and determine whether or not individuals are following organization policy correctly or not.

References

No references were used in this paper.