

IPsec: Securing Your Network Today to Prepare for Tomorrow

By Ian Hameroff, CISSP

Product Manager, Windows Server Core Networking
Microsoft Corporation



Microsoft

It was no surprise that security was a hot topic at last month's US IPv6 Summit. The new opportunities and risks that have been introduced by today's nearly ubiquitous network connectivity appear to only grow in scope with the adoption of IPv6. These sentiments were certainly present during the full-day security tutorial at the Summit.

Common questions like, "Do I really want my data center to be globally addressable?" or "how do I enable true end-to-end connectivity without giving up the IP address obscurity provided by my NAT?" have been echoed by many IT professionals during their IPv6 deployment planning. Compounding these challenges are regulatory requirements for greater data privacy protection which appear, on the surface, to be counter to the "seamless networking" vision that IPv6 can help make a reality.

These are important questions to ask, but they need not become roadblocks to IPv6 adoption.

The good news is there are tools and solutions already available to you — in the IPv4 world — that can help you prepare for a more secure IPv6 transition. One in particular is IPsec (Internet Protocol security) and a solution based on it called, "Server and Domain Isolation."

When most people hear the term IPsec, they tend to think of it as part of a VPN solution, like the Routing and Remote Access Service in Windows Server 2003. However, there are a series of IPsec-based scenarios that do not employ its tunneling and encryption capabilities, but, instead, leverages its end-to-end authentication features to protect IP communications between trusted hosts. Microsoft has created a solution based on this approach called "Server and Domain Isolation."

Server and Domain Isolation enables administrators to dynamically segment their networked infrastructure into more secure, isolated virtual networks. These "virtual LANs" are created by policies on the host, rather than through the networking equipment. These policies are enforced by the IPsec capabilities of the platform, at the network layer, which removes the need for changes to network topology or existing applications.

As part of an overall defense-in-depth strategy, Server and Domain Isolation adds another safeguard against common security threats, such as worms, denial-of-service attacks and, most importantly, unauthorized access to trusted networked resources .

Security Defense-in-Depth Model

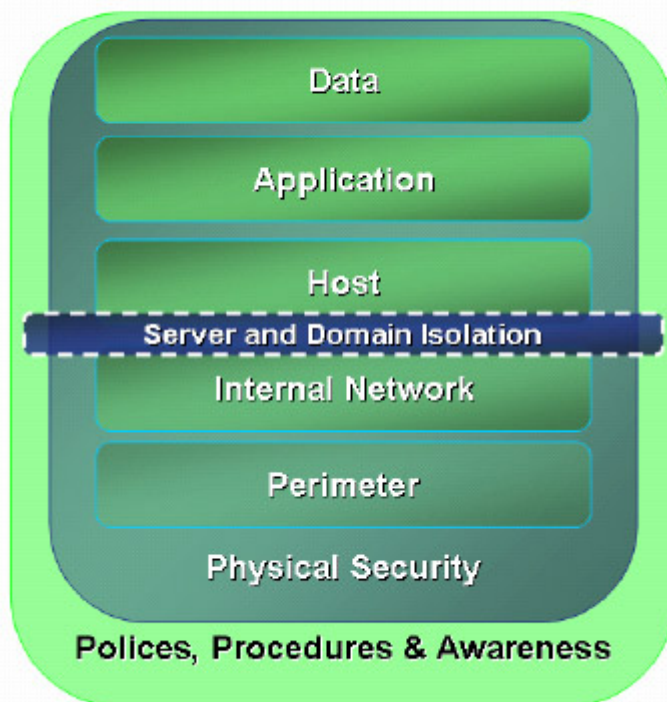


Figure 1. Server and Domain Isolation is part of an overall defense-in-depth approach, employed at the network-layer between the host and the physical network.

This is made possible through the IPsec's ability to mutually authenticate hosts that are attempting to communicate and ensure the integrity of packets sent between them. In technical terms, this approach utilizes IPsec transport mode (for end-to-end protection between hosts) and Encapsulating Security Payload (ESP) without encryption (for integrity checking, even across NATs).

Before two hosts can communicate, they must first engage in a security negotiation using the Internet Key Exchange (IKE) protocol. The IKE conversation provides the first safeguard, by requiring each side to have an explicit policy to communicate with the other and the appropriate credential to authenticate itself. In the Microsoft implementation of IPsec, this can be either a Kerberos ticket generated for the computer by Active Directory, an x.509 PKI certificate or a pre-shared key.

Once the IKE negotiation completes, each packet sent between the two hosts is encapsulated and cryptographically signed to ensure it has not been manipulated in transit. This continues until the communications end and the connection is torn down.

If either host fails to successfully negotiate this exchange, the other host effectively appears invisible. This greatly reduces the risk of an authorized compromise of a trusted host. For example, a common propagation tactic used by computer worms is to scan the network for hosts with a vulnerability it can exploit to infect its next victim.

Since the malicious computer, say a contractor's laptop without the latest antivirus signatures or patches, does not have the proper IPsec policy or credential, the IKE negotiation fails. The worm cannot communicate with the target host and the trusted host is protected from infection.

Server and Domain Isolation is based on this approach. More specifically, Server Isolation creates an isolated, virtual network around high-value servers (and its data) and the hosts that have a requirement to connect to it. For example, you can create an isolated network around your servers with HR data and

the HR department's desktops. Domain Isolation extends this approach to an entire managed domain. In Microsoft parlance, this would be hosts joined to an Active Directory domain.

You can easily nest more restrictive Server Isolation policies within a larger Domain Isolation deployment. Microsoft does this inside our own network. Our network has more than 275,000 hosts in its Domain Isolation implementation, while a more restrictive Server Isolation within it limits access to our source code servers to only to the development teams. Employing this network-level protection of our source code has helped us achieve compliance with the Sarbanes-Oxley Act which requires us to safeguard our most important intellectual property.

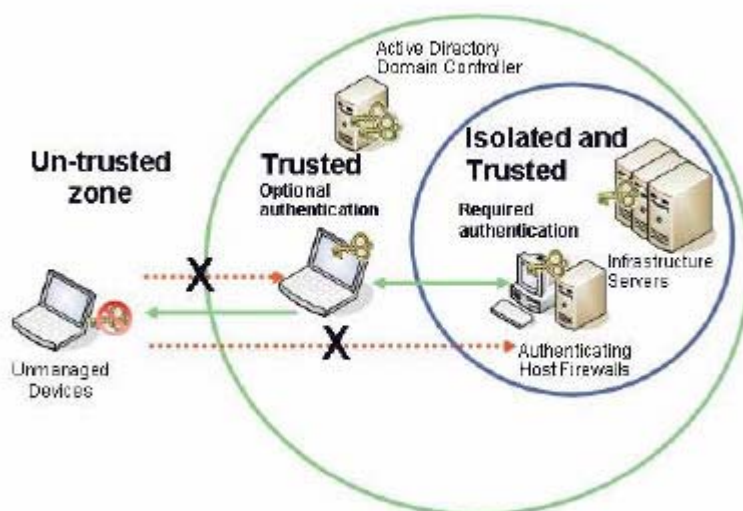


Figure 2. Server and Domain Isolation's policy-based dynamic segmentation enables you to create tiered access to trusted resources with your network without changes to the topology or applications.

So, how does this help address the risks potentially introduced by IPv6, such as the global addressability of IPv6 hosts? Since every computer participating in the Server and/or Domain Isolation policy mutually authenticates with the other before any network communications, you are able to mitigate the risk of unauthorized access by rouge or unmanaged devices. The flexibility of these IPsec isolation scenarios means you can easily create virtual trust boundaries and better protect your network.

For example, you can create a restrictive policy that isolates your data center so it only communicates hosts on your network. Anyone outside the network, even if the data center servers are globally addressable, will not have the appropriate IPsec policy or credential to establish a connection to these trusted resources.

Server and Domain Isolation easily translate to IPv6. By deploying this solution in your IPv4 environment today, you can more confidentially transition to IPv6 since you have the network-layer protections in place to reduce the risk of unauthorized network access.

Finally, this whole solution builds upon your existing infrastructure investments. In a Microsoft Windows environment, for example, Server and Domain Isolation utilizes Active Directory Group Policy for centralize policy management, Active Directory credentials for authentication and Windows IPsec for enforcement. This is among the many reasons why a large number of our customers have embraced Server and Domain Isolation to protect tens of thousands hosts.

For more information about Server and Domain Isolation, including prescriptive deployment guidance, visit <http://www.microsoft.com/sdisolation>.

