TECHNICAL WHITE PAPER

IP Security Features

Intel® Ethernet Server Adapters and Microsoft® Windows Server® 2008

TABLE OF CONTENTS

Introduction 2

The Basics of IPsec 3

Server and Domain Isolation (S&DI) 4

Network Access Protection (NAP) 6

DirectAccess (DA) 9

The Challenges with VPNs 9

Intel® Ethernet Server Adapters with IPsec Offload 10

Conclusion 12

For More Information 12

Network security is an increasingly crucial issue for network administrators. Attacks from outside – and from within the data-center network – must be thwarted to protect service levels, prevent loss of intellectual property, avoid theft of sensitive client data, meet regulatory compliance, and mitigate corporate liability. Internet Protocol Security (IPsec) provides network administrators with a suite of tools to create a robust defense against network attacks from any source.

This white paper provides an introductory overview of IPsec as implemented in Microsoft® Windows Server® 2008. Additionally, the role of new-generation Intel® Ethernet Server Adapters and Ethernet controllers is discussed in terms of how they offload IPsec processing onto silicon to enhance security while maintaining line-rate network throughput.

intel® | Microsoft®

Introduction

Attacks on networks – both from outside and from within the network – continue to be a challenge for network administrators and a potentially costly liability for enterprises. Malicious attacks, such as viruses and Denial of Service (DoS), cause loss of time and business and require use of valuable resources to resolve. Data theft, especially confidential client or customer information, can cause loss of customer trust at minimum and may cost millions of dollars in legal fees and restitution should a class-action suit arise.

Equally troubling are recent estimates that now place the number of attacks from within networks as high as eighty percent of all successful attacks on corporate networks. These attacks can come from employees, on-site contractors, consultants, anyone with access to the corporate network. Considering the potential for loss from data theft – whether it be loss of market advantage or liability for identity theft – the time and expense of providing robust network security is really minimal.

What network administrators need is a flexible, comprehensive set of security tools that can be configured to provide varying types and levels of security to meet the diverse requirements of different organizations. To meet this need, the Internet Engineering Task Force (IETF) developed a set of security standards collectively referred to as Internet Protocol Security or IPsec. IPsec is, essentially, a framework of protocols for providing end-to-end security at the packet processing layer of the network. IPsec provides the ability to implement customizable security for protecting communication among and between workgroups, local area network (LAN) computers, domain clients and servers, branch offices (which might be physically remote), extranets, and roving clients.

IPsec provides the ability to implement customizable security for protecting communication among and between workgroups, local area network (LAN) computers, domain clients and servers, branch offices, extranets, and roving clients.

Microsoft® Windows Server® 2008 contains a robust implementation of IPsec that does not require any hardware or software upgrades to make IPsec work end-to-end. This gives network managers a powerful and cost-effective suite of tools for implementing network security, including capabilities for server and domain isolation (S&DI) and Network Access Protection (NAP).

However, during development of the Windows Server 2008 IPsec implementation, there were concerns about the impact of additional packet processing on system performance. To address this concern, Microsoft and Intel worked together on means to minimize the impact on throughput. Through these efforts, Microsoft included in its software design the ability to offload IPsec encryption, and Intel contributed by providing IPsec encryption and decryption offloading to hardware on its new generation of Ethernet server adapters and controllers. Encryption offloading provides enhanced security while maintaining throughput at near line-rate and minimizing CPU utilization. This white paper provides an overview of the key features and benefits of IPsec as implemented by Microsoft and the performance and security enhancements provided by Intel® Ethernet Server Adapters.

The Basics of IPsec

In the interconnected business world of today, sensitive information is constantly flowing across networks. Whether it is the Internet, intranets, branch offices, or through remote access, there are numerous places and ways that information security can be compromised. The challenge for network administrators and other information technology (IT) professionals is to ensure that sensitive network traffic is kept safe from:

- Data modification while in transit (data integrity)
- Data being read and interpreted while in transit (data confidentiality)
- Spoofing of data by unauthenticated parties (data origin authentication)
- Resubmission (replayed) to gain unauthorized access to protected resources (anti-replay or replay protection)

IPsec, as implemented in Windows Server 2008, safeguards against all of the above attacks end-to-end in IP-based networks. Unlike antivirus, password authentication, and other security methods that protect at firewalls and routers at the edge of the private network, IPsec protects within the network. As a consequence, intrusions that breach the firewall are still blocked or protected against by IPsec. Hence, IPsec has the advantage of protecting against both internal and external attack.

IPsec uses various methods of protection, most notably policy-based packet filtering and encryption. This means that security in terms of which computers can talk to each other or access certain types of data is governed by policies that are set up by the IT organization. IPsec is configurable to meet specific security needs for isolating sensitive systems and data within an organization and ensuring safe data transit throughout the intranet as well as over the Internet to remote sites or branch offices. Additionally, a key feature of Windows Server 2008 is the simplification of IPsec policy management for IT administrators. All the administrator has to do is set policy at one point for all or any set of user machines and servers. Once set, the policies and rules are applied automatically by Windows Server 2008. Windows Firewall with Advanced Security (WFAS) is another key feature for simplification in Windows Server 2008. Windows Firewall and IPsec configuration are integrated into WFAS to provide a single tool that simplifies setup and eliminates potential conflicts between IPsec and firewall security policies.

In general operation, two computers using IPsec to communicate will create two kinds of security associations (SAs). These are referred to as main mode and quick mode. In main mode, the computers mutually authenticate themselves to each other. Authentication is an establishment of a certain level of trust, similar to the various levels of badges issued to employees, visitors, and contractors at a corporate front desk. In quick mode, the two computers negotiate the specifics of the SA based on the trust levels and policies previously set by IT. This negotiation includes how the two computers will digitally sign and encrypt traffic between each other to ensure secure communications. This is analogous to authenticating a vendor or visitor by establishing identity and issuing an entrance badge, then negotiating a nondisclosure agreement before exchanging sensitive information with the vendor.

Each computer is governed by an IPsec policy that is set up once and assigned by the IT administrator. The policy can have any number of rules. Each rule has a filter list and a filter action, and the filter list consists of one or more filters that specify the characteristics of the traffic that the filter should process, for example addresses, port numbers, and protocol types. The filter action specifies the action to be taken for the specified traffic, whether to permit it, block it, or negotiate a pair of IPsec SAs. Security actions can have various policy-driven options, including encryption suites, per-packet authentication methods, how often to generate new authentication keys, whether to allow or block communication with computers not supporting IPsec, and so forth.

In short, IPsec is an extensive framework of tools that allows IT to build customized security based on policies designed by IT. Additionally, because IPsec is integrated into the operating system (OS) at the Network layer (layer 3 of the OSI model), it provides security for all IP-based traffic. As a result, there is no need to include support for and configure security for each application using IP traffic, and IPsec is transparent to users.

In Windows Server 2008 and Windows Vista® security negotiation is handled by the Authenticated Internet Protocol (AuthIP) module. AuthIP is an enhanced version of the standards-based Internet Key Exchange (IKE) protocol used in previous Windows Server versions. AuthIP provides simplified IPsec policy configuration and maintenance. Additionally, AuthIP extends IKE to provide user-based authentication, authentication with multiple credentials, improved authentication method negotiation, and asymmetric authentication.

It is also equally important to note that AuthIP is designed to coexist with IKE, which is used in Windows XP and Windows Server 2003. This coexistence feature is important for carrying out IPsec authentication in networks containing a mix of Windows Vista, Windows XP, Windows Server 2003, and Windows Server 2008 operating systems. In essence, this coexistence consists of a preliminary negotiation between peers to determine whether authentication should be IKE-based or AuthIP-based.

As mentioned previously, IT administrators can configure IPsec policies and security to meet a wide range of specific needs. This includes the security requirements of an application, computer, group of computers, domain, site, or global organization. Additionally, IPsec can be customized for use in numerous scenarios, including packet filtering, securing host-to-host traffic on specific paths, securing traffic to servers, Layer Two Tunneling Protocol (L2TP)/IPsec for virtual private network (VPN) connections, and site-to-site (also known as gateway-to-gateway) tunneling.

At this point, several possible questions may come to mind. For example: How much processing burden does IPsec place on the hosts? By far, the largest burden is packet encryption and decryption. However, Windows Server 2008 provides an efficient method for server adapters to perform IPsec cryptographic operations in hardware. Intel and Microsoft are working together to introduce IPsec offloads in new-generation Intel Ethernet Server Adapters and Controllers. This offloading allows IPsec-protected systems to run at near line speed with virtually no throughput or CPU utilization penalties for IPsec implementation.

Other common questions include:

How do you provide different levels of protection for various organizational groups without physically altering the network topology? The answer is to implement a Server and Domain Isolation (S&DI) solution based on Microsoft® Windows® IPsec and Active Directory®.

How do you protect against viruses and worms that might be introduced to your intranet? An answer to this question is provided by Network Access Protection (NAP) for Windows Server 2008. NAP allows administrators to enforce compliance to computer health requirements using IPsec policies.

IPsec offloading to Intel Ethernet Server Adapters, S&DI, and NAP are the topics covered in the rest of this paper, beginning with S&DI.

Server and Domain Isolation (S&DI)

An S&DI solution based on Microsoft Windows Server 2008 IPsec and the directory services of the Active Directory feature allows network administrators to dynamically segment networks into more secure and isolated logical networks. This isolation is based on group policies and machine and user authentication rather than costly physical changes to the network infrastructure or applications.

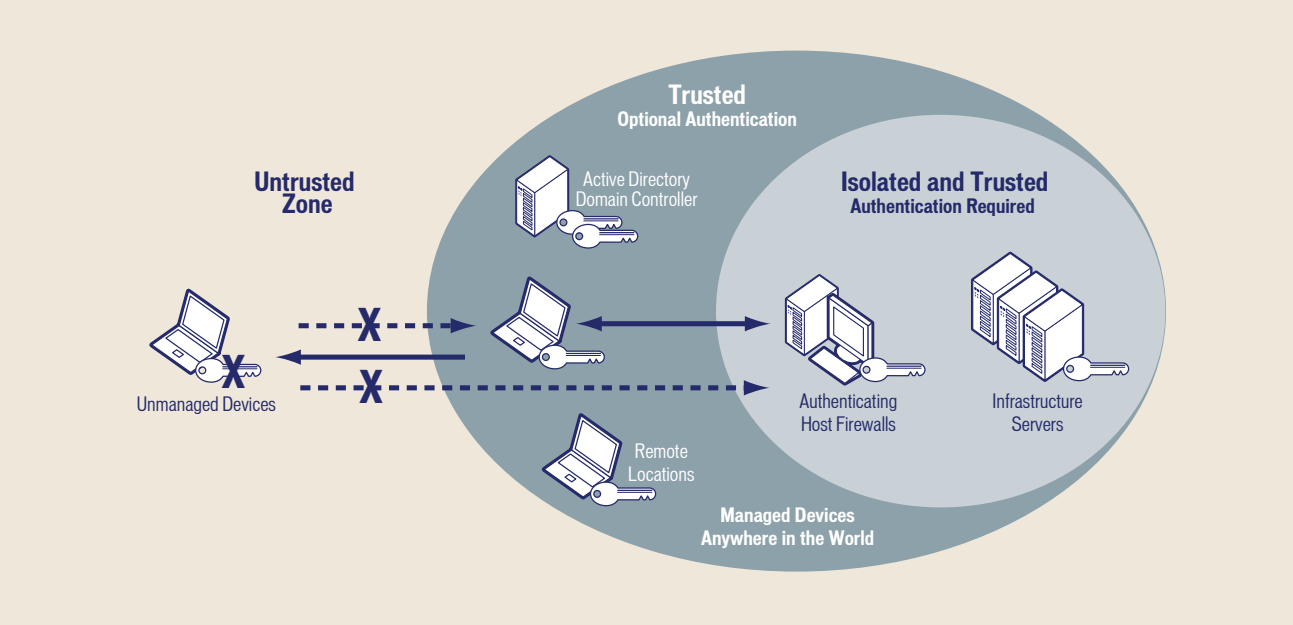

Figure 1. Server and Domain Isolation provides a layered, policy-driven means of enhancing security for specific domains or groups within a network without restricting or limiting the physical location of trusted devices.

The result is an additional layer of policy-driven protection for enhanced protection against network attacks and prevention of unauthorized access to trusted networked resources. Additionally, S&DI makes it easier to achieve regulatory compliance and reduce operational costs.

Figure 1 illustrates the basic concept of S&DI, where the environment is logically defined or separated into an untrusted zone, a trusted zone or domain, and an isolated and trusted zone. In this example an entire managed network has been isolated (domain isolation) and specific application servers, data, and clients have been isolated (server isolation) within the domain. Server and domain isolation can be implemented independently or in combination, as shown in Figure 1.

For example, you can use domain isolation to better protect a managed Windows environment from threats originating from unmanaged or rogue computers. Then you can further restrict network access to specific resources, such as a human resources database or banking information database, to a limited set of machines and/or users by implementing server isolation within the domain using the AuthIP protocol available in Windows Server 2008.

S&DI enforces the logical boundaries you define through end-point authentication policies created, distributed, and managed through Active Directory Group Policy. Policy is seamlessly deployed when a computer joins the domain.

As described earlier, end-point authentication as configured using AuthIP is based on the machine credentials of the computer and/or the user credentials of the interactively logged in user. The machine credentials can be either an Active Directory-issued Kerberos ticket, NTLMv2 credential, an X.509 certificate automatically enrolled for the computer through Group Policy, or a Network Access Protection (NAP) Health Certificate. Additionally, user credentials can be either an Active Directory-issued Kerberos ticket or NTLMv2 credential. By using Active Directory for credential issuance and management, S&DI provides a flexible, integrated experience for both IT administrators and users.

Policy enforcement is handled by the built-in IPsec functionality of Windows Server 2008. Instead of the conventional use of IPsec as a tunneling and network encryption protocol (for example remote access VPN), S&DI uses IPsec transport mode for end-to-end security between computers, even across Network Address Translation (NAT). With the policies in place, trusted computers are protected and can easily communicate with each other without any additional steps or login procedures. Just as importantly, unmanaged or rogue computers are unable to establish network communications with computers protected within the logically isolated network. However, domain members can be allowed to establish network communications with computers outside of their domain. For example, as indicated in Figure 1, computers in the trusted zone can initiate and carry on communication with computers in the untrusted zone if needed, but the opposite case of an untrusted computer accessing a trusted or isolated domain is not allowed.

The many benefits of S&DI under IPsec for Windows Server 2008 include the following:

- **Reduced surface area exposed to attacks.** Establishing network communication is limited to trusted, managed computers to help mitigate the risk of an unmanaged or rogue computer exploiting vulnerabilities, spreading malware, or launching denial-of-service (DoS) attacks.
- **Adds another layer to your defense-in-depth security strategy.** The policy-driven safeguards are added at the network layer and enhance the network control benefits of host firewalls while complementing other host- and network-based security technologies.
- **Increases manageability and helps ensure compliance**. Since S&DI requires domain membership (authentication) to access trusted resources, IT administrators can use Group Policy and tools such as Microsoft System Management Server (SMS) to help increase system reliability and compliance.
- **Safeguards sensitive data and intellectual property.** Enhanced protection of confidentiality and integrity of sensitive corporate data with authenticated network communications, virtually tamper-proof data integrity, and optional encryption for sensitive data.
- **Requires no additional investments in hardware or software.** S&DI eliminates the need for potentially disruptive changes to network topology, applications, or costly infrastructure upgrades.
- **Extends the value of Active Directory.** Group Policy is used to create, distribute, and manage end-point authentication policies from a centralized location. There is no need to install any new software, and end users will not require any additional training.
- **Integrates with other Microsoft policy-driven network access solutions.** Network Access Protection (NAP), discussed in the next section, builds upon an existing S&DI deployment, using it as an enforcement method to restrict network access based on computer health. S&DI also works seamlessly with 802.1x-based secure wireless LAN solutions.

Network Access Protection (NAP)

The Network Access Protection (NAP) feature of Windows Server 2008 extends the S&DI and AuthIP solutions to include computer health. This saves time for IT by addressing one of the more challenging IT tasks – ensuring that computers connecting to the network are up to date and meet health policy requirements. Enforcing computer health requirements and protecting the private network become even more difficult when some computers, such as home computers or mobile laptops, are not under IT control. Yet failing to keep computers that connect to network up to date is one of the most common ways to jeopardize network integrity with exposure to viruses and malware attacks.

NAP provides various components and an Application Programming Interface (API) that help IT administrators define and enforce compliance with health requirement policies for network access or communication. Administrators can create solutions for validating computers connecting to the network, providing needed updates or access to health update resources, and limiting the access or communication on noncompliant computers.

NAP has the following three important and distinct aspects:

- **Health state validation.** When a computer connects to a network and periodically thereafter, its health state is validated against the health-requirement policies as defined by the administrator. Administrators can also define what to do if a computer is not compliant. For example, an administrator may restrict the computer's access to the network or the administrator may choose to report the computer's health compliance state with no access restriction.
- **Health remediation.** Administrators can help ensure compliance with health policies by choosing to automatically remediate noncompliant computers. In a reporting-mode environment, computers can have access to the network while they are updated. In a limited access environment, noncompliant computers have restricted network access until the updates and configuration changes are completed. In both "reporting-mode" and "enforcement-mode" environments, NAP-capable computers are driven to become compliant with the administrator's defined NAP compliance policy. For those computers that are non-NAP-capable, administrators may define appropriate access exceptions.
- **Restricted network access.** Administrators can optionally protect their networks and computers by limiting the network access of non-compliant computers, as defined by the administrator. "Non-compliant" computers that have their network access restricted can access resources on the network that enable them to become compliant. For example, non-compliant computers whose network access is restricted may be able to access a server containing patches, anti-virus signatures, etc.

Note that network access restriction is an optional mode of NAP and it is not required to obtain many of NAP's benefits.

While NAP can support various types of network protection and policy enforcement – IPsec-protected traffic, 802.1x authenticated connections, remote access VPN, and so forth – IPsec enforcement is one of the strongest and most flexible forms of policy enforcement available.

With IPsec enforcement, a computer must be compliant to initiate communications with other compliant computers. Because NAP enforcement is leveraging IPsec, you can define requirements for protected communications with compliant computers on a per-IP address or per-TCP/UDP port number basis. And finally, IPSec allows for logical grouping and policy assignment without necessarily requiring modifications to network architecture or topology.

In operation, NAP validates computer compliance against an administratively defined health compliance policy. If the computer is compliant, NAP issues a health certificate to the computer that is then used by IPSec to enable communication between different computers. Computers without a health certificate cannot communicate with other IPSec-protected computers that require possession of a health certificate. Computers periodically renew their health certificate every few hours. Client computers that are not in compliance with the health policy can be provided with restricted network access until their configuration is updated and brought into compliance with policy. Depending on how NAP is deployed, noncompliant clients can be quarantined or automatically updated so that users can quickly regain full network access without manually updating or reconfiguring their computers.

NAP supports IPsec policies as a means of enforcing computer compliance with network health requirements. IPsec policies can be created to require that incoming network connections are accepted only from computers with a valid health certificate. These health certificates are managed by the IPsec EC.

The IPsec EC requests a health certificate for the client computer if the client meets network health requirements. The health certificate remains in force until it is removed. Removal occurs upon the expiration of the health-certificate validity period or if the client becomes noncompliant with network health requirements.

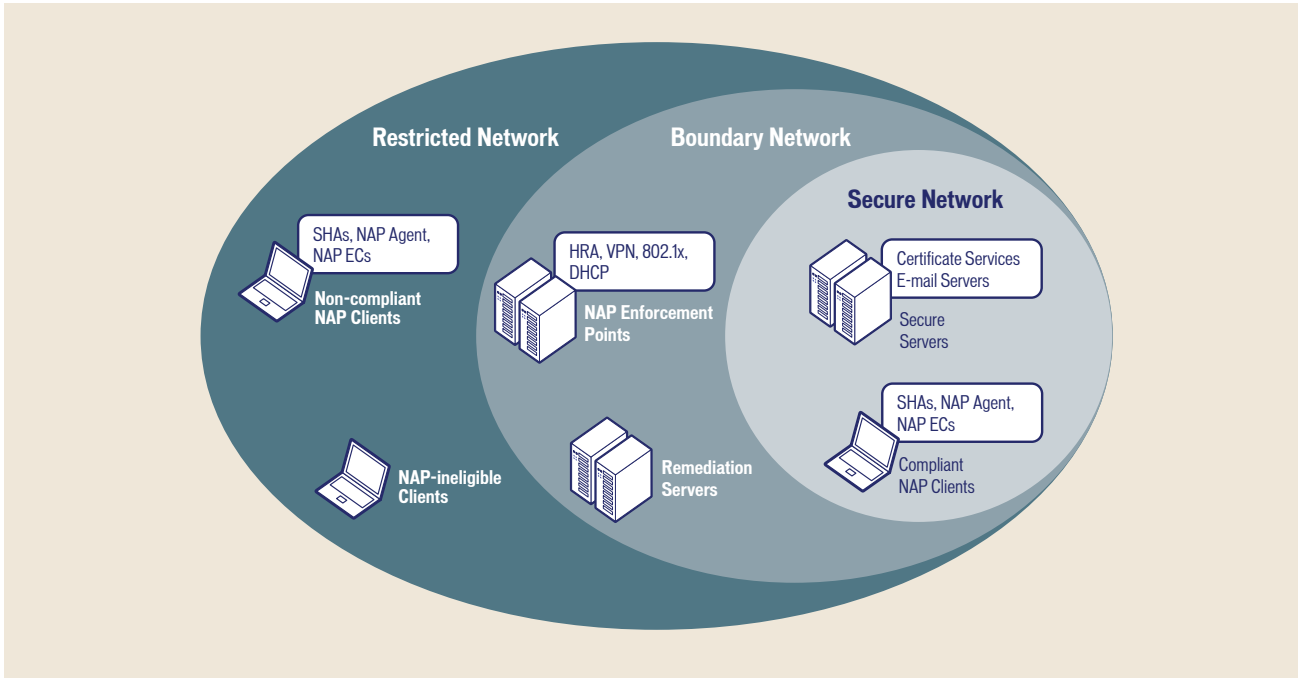

Figure 2. IPsec divides a physical network into three logical networks for NAP enforcement.

To provide NAP enforcement, IPsec policies divide a physical network into three logical networks as shown in Figure 2. A computer is a member of only one logical network at a time, and logical networks are defined in terms of whether computers require IPsec authentication with health certificates for incoming communication attempts. The logical networks limit the access of noncompliant computers and provide compliant computers with an environment that is protected from threats introduced by noncompliant computers. Noncompliant computer access is limited to resources required to correct their health state in order to gain full network access.

The IPsec logical networks for NAP consist of the three following types:

Secure network (or "full-access network"). An NAP secure network corresponds to the S&DI trusted and isolated zone. Computers that have health certificates and that require these certificates for authentication of incoming communication attempts are on a secure network. These computers have a common set of IPsec policy settings that provide IPsec protection. For example, most server computers that are members of an Active Directory infrastructure would be in a secure network. Microsoft Network Policy Server (NPS), servers running Active Directory Certificate Services (AD CS), and e-mail servers are examples of network components that normally reside in the secure network. Clients that are compliant to NAP health policy and possess a valid NAP health certificate exist in this network.

Boundary network. An NAP boundary network corresponds to the S&DI trusted zone. Computers that have health certificates but do not require that incoming communication attempts authenticate with these certificates are on the boundary network. Computers in the boundary network must be accessible to computers on the entire network. These types of computers are the servers required to assess and remediate NAP client health or otherwise provide network services for computers in the restricted network, such HRA servers and remediation servers. Because computers in the boundary network do not require authentication and protected communication, they must be closely managed to prevent them from being used to attack computers in the secure network.

Restricted access network. An NAP restricted access network corresponds to the S&DI untrusted zone. Computers that do not have health certificates are placed in the restricted network. These are computers that have not completed health checks, or have been determined to be noncompliant with network health policy. They might be guest computers, or non-NAP-capable computers.

DirectAccess (DA)

The Windows® 7 and Windows Server® 2008 R2 operating systems will introduce DirectAccess, a new solution that provides users with the same experience working remotely as they would have when working in the office. With DirectAccess, remote users can access corporate file shares, web sites, and applications without connecting to a virtual private network (VPN).

DirectAccess establishes bi-directional connectivity with the user's enterprise network every time the user's DirectAccess-enabled portable computer is connected to the Internet, even before the user logs on. With DirectAccess, users never have to think about whether they are connected to the corporate network. DirectAccess also benefits IT by allowing network administrators to manage remote computers outside of the office, even when the computers are not connected to a VPN. DirectAccess with NAP enables organizations with regulatory or other compliance concerns to provide continuous compliance and compliance reporting for roaming Windows 7 computer assets.

The Challenges with VPNs

Traditionally, users connect to intranet resources with a VPN. However, using a VPN can be cumbersome because:

- Connecting to a VPN takes several steps, and the user needs to wait for authentication.
- Any time users lose their Internet connection, they need to re-establish the VPN connection.
- VPN connections can be problematic in some environments that filter out VPN traffic.
- Internet performance is slowed if both intranet and Internet traffic goes through the VPN connection.

Because of these inconveniences, many users avoid connecting to a VPN. Instead, they use application gateways, such as Microsoft® Outlook® Web Access (OWA), to connect to intranet resources. With OWA, users can retrieve internal e-mail without establishing a VPN connection. However, users still need to connect to a VPN to open documents that are located on intranet file shares, such as those that are linked to in an e-mail message.

DirectAccess gives users the experience of being seamlessly connected to their corporate network any time they have Internet access. With DirectAccess enabled, requests for corporate resources (such as e-mail servers, shared folders, or intranet Web sites) are securely directed to the corporate network, without requiring users to connect to a VPN. DirectAccess provides increased productivity for a mobile workforce by offering the same connectivity experience both in and outside of the office.

IT professionals also benefit from DirectAccess in many ways:

Improved Manageability of Remote Users. Without DirectAccess, IT professionals can only manage mobile computers when users connect to a VPN or physically enter the office. With DirectAccess, IT professionals can manage mobile computers by updating Group Policy settings and distributing software updates any time the mobile computer has Internet connectivity, even if the user is not logged on. This flexibility allows IT progressions to manage remote computers on a regular basis. By incorporating NAP with DirectAccess, mobile Windows 7 computers can maintain compliance to security and configuration policies at all times.

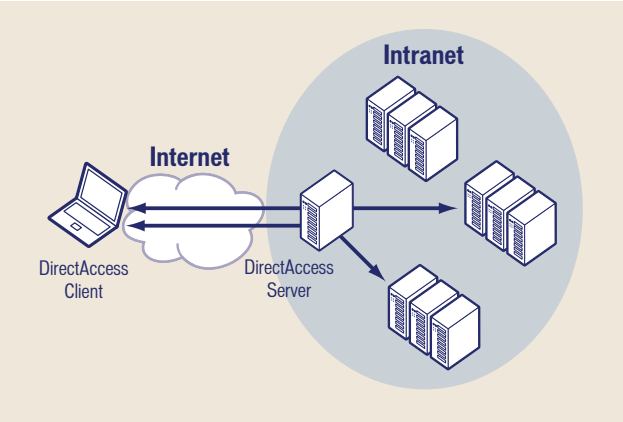

Figure 3. End-to-End Protection - IPsec is used between client and application servers (requires that application servers run Windows Server 2008 or Windows Server 2008 R2 and use both IPv6 and IPsec).

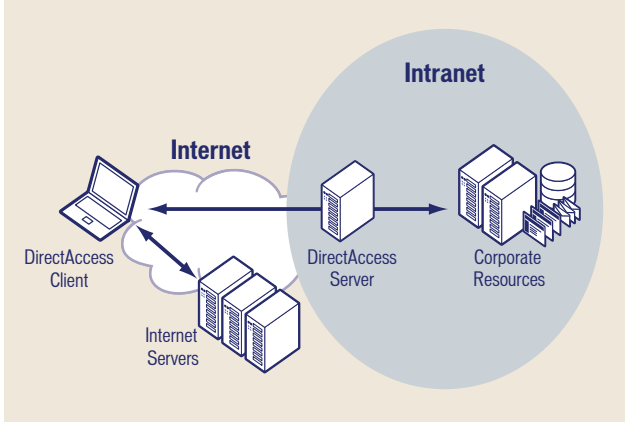

Figure 4. Separating Internet and Intranet Traffic - DirectAccess separates intranet traffic from Internet traffic to reduce unnecessary activity on the corporate network.

Secure and Flexible Network Infrastructure. Taking advantage of technologies such as Internet Protocol version 6 (IPv6) and Internet Protocol security (IPsec), DirectAccess provides secure and flexible network infrastructure for enterprises by using S&DI. Below is a list of DirectAccess security and performance capabilities:

- **Authentication.** DirectAccess authenticates the computer, enabling the computer to connect to the intranet before the user logs on. DirectAccess can also authenticate the user and supports two-factor authentication using smart cards.
- **Encryption.** DirectAccess uses IPsec to provide encryption for communications across the Internet.
- **Access Control.** IT professionals can configure which intranet resources different users can access using DirectAccess, granting DirectAccess users unlimited access to the intranet or only allowing them to use specific applications and access specific servers or subnets.

IT Simplification and Cost Reduction. DirectAccess separates intranet from Internet traffic, which reduces unnecessary traffic on the corporate network by sending only traffic destined for the corporate network through the DirectAccess server. Optionally, IT can configure DirectAccess clients to send all traffic through the DirectAccess server.

DirectAccess improves the productivity of mobile users by keeping them connected to corporate resources. Combined with other Windows 7 improvements, such as Federated Search, which searches intranet resources, and Folder Redirection, which synchronizes files across the network, users will be able to find and access corporate resources seamlessly, wherever they are.

Intel® Ethernet Server Adapters with IPsec Offload

In a joint effort, Intel and Microsoft developed a method of IPsec acceleration to process IPsec-protected packets in a faster, less burdensome manner. This jointly developed method provides packet throughput that is near line rate. Additionally, the process has very little impact on CPU utilization and essentially unburdens the CPU from IPsec processing. In short, it avoids the processing burdens and throughput penalties paid in a purely software implementation of IPsec.

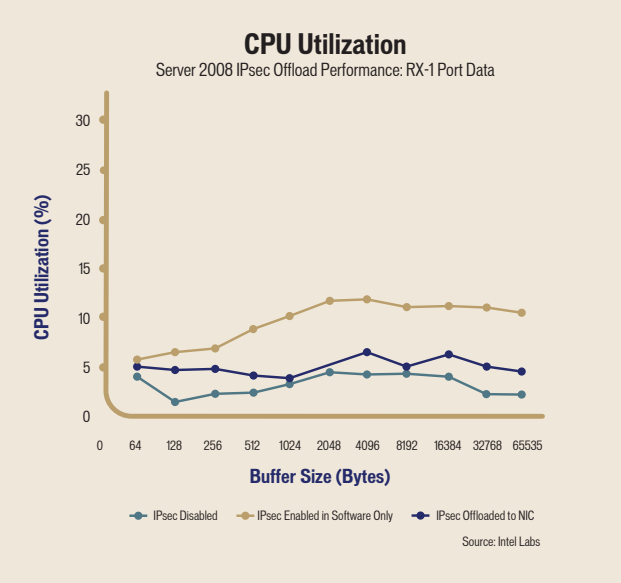

Figure 5. IPsec performance results in terms of CPU utilization percentage for Microsoft® Windows Server® 2008 and an Intel® Ethernet Gigabit Server Adapter. CPU utilization is for received data on a single port with IPsec disabled, IPsec enabled in software only, and IPsec offloaded to the network interface card (NIC)[1]

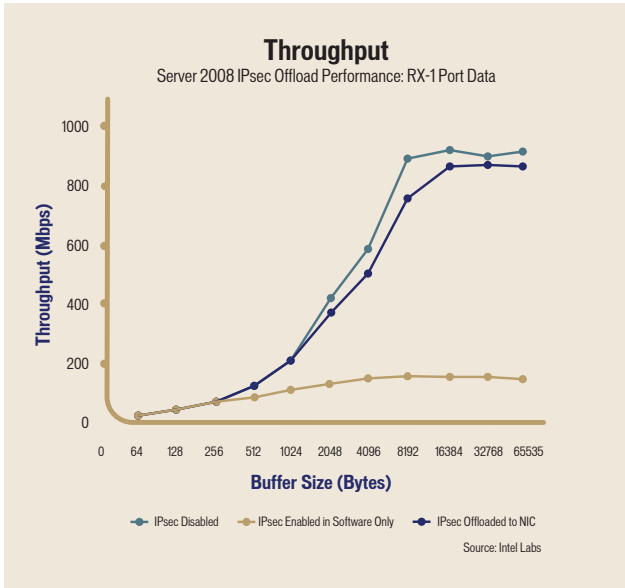

Figure 6. IPsec throughput performance for Microsoft® Windows Server® 2008 and an Intel® Ethernet Gigabit Server Adapter. Throughput is for received data on a single port with IPsec disabled, IPsec enabled in software only, and IPsec offloaded to the network interface card (NIC)[1]

On the Microsoft side, Windows Server 2008 provides a method for offloading IPsec operations to hardware in the server network adapter. On the Intel side, new-generation Intel Ethernet Server Adapters and Controllers take advantage of the offloading capability and perform IPsec tasks and other IPsec operations with greater efficiency in the adapter hardware.

IPsec capabilities and operations offloaded to the Intel Server Adapter include the following:

- Provisioning of 256 or more security associations (SAs) for IPsec
- Support for IP Authentication Header (AH) protocol
- Support for IP Encapsulation Security Payload (ESP) for IPsec authentication and encryption
- Support for AES-128-GMAC Engine
- IPv4 and IPv6 support

These offloads provide significant throughput improvement and reduction of CPU utilization as compared to a purely software IPsec implementation and result in virtually no throughput penalty for using IPsec. This has been supported by extensive performance testing, the results of which are summarized in Figure 5 and Figure 6.

Figure 5 shows CPU utilization percentage results for various test scenarios. The baseline performance can be considered to be the line graph indicated in the legend as IPsec Disabled. This is the performance without IPsec, and it is generally just a few percent in CPU utilization.

With IPsec enabled in software only, CPU utilization is approximately doubled. This should be expected since more CPU resources are required for performing IPsec authentication and encryption tasks solely in software. However, with IPsec offloaded to the NIC, the CPU burden is reduced by nearly one half or more at the higher buffer sizes. This CPU Utilization performance with IPsec offloading is quite close to the baseline performance achieved by a system not using IPsec (IPsec disabled).

Figure 6 shows throughput performance for the same scenarios discussed for Figure 5. The throughput performance differences are most noticeable and dramatic at the higher buffer sizes. Notice that performance with IPsec enabled in software only is less than 150 megabits per second (Mbps), even at higher buffer sizes. By contrast, throughput with IPsec offloaded to the NIC is much higher, approaching 900 megabits per second at higher buffer sizes and nearly equaling the throughput achieved with IPsec disabled.

Clearly, IPsec task offloading to the server adapter essentially eliminates any performance penalty for using IPsec. This makes IPsec quite attractive for providing end-to-end network security, especially with the additional advantage that IPsec does not require any hardware or software upgrades to make it work end-to-end.

Conclusion

IPsec, as provided in Microsoft Windows Server 2008, is the long-term direction for secure networking. It provides aggressive protection against private network and Internet attacks through policy-driven, end-to-end security. The only computers that must know about IPsec protection are the sender and receiver in the communication. IPsec provides the ability to protect communication between workgroups, local area network computers, domain clients and servers, branch offices (which might be physically remote), extranets, and roving clients. IP sec also provides data encryption for DirectAccess, which will be introduced with Windows 7 and Windows Server 2008 and will provide simplified remote connectivity.

By offloading encryption/decryption tasks to the new-generation Intel Ethernet Server Adapters and Controllers, networks can be fully protected with virtually no capacity penalty to the network or processors. Network throughput is maintained at near line rate, providing throughput comparable or equal to those achieved without IPsec implementation.

IPsec provides a secure foundation for Server and Domain Isolation (S&DI), Network Access Protection (NAP), and DirectAccess (DA). These solutions provide a highly configurable, very robust end-to-end security solution that does not require any software or hardware upgrades for implementation to support IPsec processing. When combined in a network using new-generation Intel Ethernet Server Adapters based on the Intel® 82576 Gigabit Ethernet Controller or Intel® 82599 10 Gigabit Ethernet Controller, the solution is both performance enhanced by IPsec offloading and security enhanced by the flexibility and configurability of IPsec features.

For More Information

To find out more about IPsec and NAP in Windows Server 2008, visit **www.microsoft.com/nap**

To find out more about Intel Ethernet Server Adapters with IPsec offloading, visit **www.intel.com/network**

[1] Performance tests and ratings are measured using specific computer systems and/or components and reflect the approximate performance of Intel products as measured by those tests. Any difference in system hardware or software design or configuration may affect actual performance. Buyers should consult other sources of information to evaluate the performance of systems or components they are considering purchasing. For more information on performance tests and on the performance of Intel products, visit www.intel.com/performance/resources/limits.htm or call (U.S.) 1-800-628-8686 or 1-916-356-3104.

Printed in USA 0509/TAR/OCG/XX/PDF ♻ Please Recycle 320172-002US