IT@Intel White Paper

Intel IT
IT Best Practices
Cloud Security and Secure Virtualization
November 2011

Overcoming Security Challenges to Virtualize Internet-facing Applications

To enable virtualization of Internet-facing applications, we developed a virtualization hosting environment that includes a broad set of security capabilities.

Bill Sunderland
Cloud Foundation Engineering Lead, Intel IT

Ajay Chandramouly
Industry Engagement Manager, Intel IT

Executive Overview

To realize benefits such as increased agility and efficiency, Intel IT is undertaking a major transition to an enterprise private cloud for our Office and Enterprise applications. To create the infrastructure for this cloud, we set a goal of virtualizing 75 percent of our Office and Enterprise computing environment.

However, technical obstacles and concerns about security have been a key challenge to achieving this goal. These concerns initially prevented virtualization of several categories of applications, including Internet-facing applications used to communicate with customers and consumers.

Virtualizing applications can increase risk because we consolidate multiple applications onto one host, removing physical barriers between them. If one virtual machine (VM) or physical host is compromised, the other VMs sharing the same hypervisor or residing on the hypervisor are also at risk.

To enable virtualization of Internet-facing applications, we developed a virtualization hosting environment that includes a broad set of security capabilities.

Our solution includes a secure virtualization host architecture that uses private virtual LANs (PVLANs) to isolate VMs, helping to prevent compromise of one application directly spreading to others. This architecture also maintains existing secure administration policy by separating network and server administrative duties. In addition, we segregate virtualization host servers into landing zones analogous to those in the physical environment, and we harden and isolate virtualization management systems. Over time, we plan to further enhance our secure virtualization capabilities by taking advantage of hardware-assisted security with Intel® Trusted Execution Technology and Intel® Advanced Encryption Standard–New Instructions.

We have already deployed our secure virtualization infrastructure at multiple data centers and are successfully migrating applications to it. Using this approach, we plan to virtualize all suitable Internet-facing applications in 2011 and 2012. This is a significant step toward our goal of virtualizing 75 percent of the Office and Enterprise environment.

Contents

IT@INTEL

The IT@Intel program connects IT professionals around the world with their peers inside our organization – sharing lessons learned, methods and strategies. Our goal is simple: Share Intel IT best practices that create business value and make IT a competitive advantage. Visit us today at www.intel.com/IT or contact your local Intel representative if you'd like to learn more.

BUSINESS CHALLENGE

To realize benefits such as increased agility and efficiency, Intel IT is undertaking a major transition to a private cloud for our Office and Enterprise computing applications.

We are building this private cloud on virtualized infrastructure. One of our first steps in migrating applications to the cloud is to virtualize and then consolidate them onto host servers based on the latest Intel® Xeon® processors. This process delivers considerable efficiency benefits: We are achieving average consolidation ratios of up to 22:1.

Like many organizations, we began our virtualization efforts by focusing on the applications that are easiest to virtualize and present the least risk. These included smaller Office and Enterprise applications that are not mission-critical, have relatively low security requirements, and are not exposed to the Internet. To achieve our goal of virtualizing 75 percent of the Office and Enterprise environment, we need to overcome significant technical obstacles that have previously prevented virtualization of several categories of applications (see sidebar).

A key obstacle is security. Due to these concerns, we initially did not virtualize applications with significant security requirements. These include Internet-facing applications such as those used to communicate with customers and consumers.

SECURITY IN THE TRADITIONAL COMPUTING ENVIRONMENT

Prior to virtualizing our Office and Enterprise computing environment, we applied several approaches to provide increased security for these applications.

Each application tier typically ran on a dedicated physical server, which was connected to the enterprise network through a dedicated virtual LAN (VLAN). This physical separation reduced the risk of compromises spreading from one application to others within the environment.

We further mitigated risk in our traditional computing environment by segregating servers into multiple landing zones within our demilitarized zone (DMZ), separated from the rest of the enterprise environment by firewalls.

VIRTUALIZATION SECURITY RISKS

Virtualizing these enterprise servers introduces significant security concerns due to aggregation of risk. When virtualizing, we consolidate multiple servers onto one host. This removes the physical separation between servers, increasing the risk that a compromise may spread from one application to others on the same host. In addition, compromise of the hypervisor can lead to compromise of all the hosted virtual machines (VMs) as well as shared physical resources, such as hard drives storing application data and code.

Attackers can target several components of a virtualization host: the guest OSs and applications within individual VMs, the hypervisor, and the hardware. They can also target the virtualization management system. To mitigate the security risk associated with virtualization, each of these components must be isolated and protected.

Guest OSs and applications. Attacks to the guest OSs and applications remain a significant threat. If one VM is compromised, there is a threat that the compromise could spread to other VMs on the same host or other hosts within the shared virtualized environment. A key concern is that this compromise could occur by way of the host's network connections, which are shared by all applications on the host.

Hypervisor. Fundamental hypervisor-level protection can be provided by Intel® Trusted Execution Technology (Intel® TXT), which is included in current Intel Xeon processors. This hardware-assisted security feature enables trusted hypervisor boot, providing assurance that the hypervisor has not been compromised.

Hardware. Server hardware is protected by physically securing servers within the data center, both in our traditional computing and virtualized environments. Intel IT implements a variety of measures to achieve this.

Virtualization management systems. To protect these critical systems, we isolate and harden them, monitor them extensively, and require additional authentication in order to gain access.

MITIGATING THE RISKS

Since server hardware is already physically protected within the data center using appropriate access restrictions, we focused our security initiative primarily on providing isolation at the level of the VM supporting each application, as well as isolation and protection of the virtualization layer—the hypervisor and the virtualization management system.

To help mitigate the threat related to application compromise, we need to be able to provide separation between applications that is analogous to the protection provided in the physical environment. This includes private virtual LAN (PVLAN) connections and resource pool landing zones (virtualization server clusters) designed to prevent the spread of a compromise—between the zones within the DMZ or out to the Office and Enterprise environment.

Intel IT Virtualization Goals and Limiting Factors

Intel IT has implemented virtualization in several phases, as shown in Figure 1. We first focused on the applications that were easiest to virtualize. Initially progress was relatively slow, as we needed to build supporting infrastructure and processes, and convince our internal business partners of the merits of virtualization. Once we achieved these objectives, we were able to triple the rate of virtualization (Phase 2); as a result, we virtualized about 42 percent of our environment by the end of 2010.[1]

In the final phase of our strategy, our goal is to virtualize about 75 percent of the environment. To reach this goal, we need to virtualize applications that were initially out of scope due to a variety of limiting factors. While we have already solved several of these challenges, others still remain.

Challenges Solved

Security. We have implemented capabilities that are enabling us to virtualize most applications that require increased security, including Internet-facing applications (using the approach described in this paper) and important internal business applications. Exceptions are a small percentage of applications that we do not plan to virtualize because the residual risk would remain unacceptably high. These include systems where we cannot risk memory exposure or virtual machine (VM) theft.

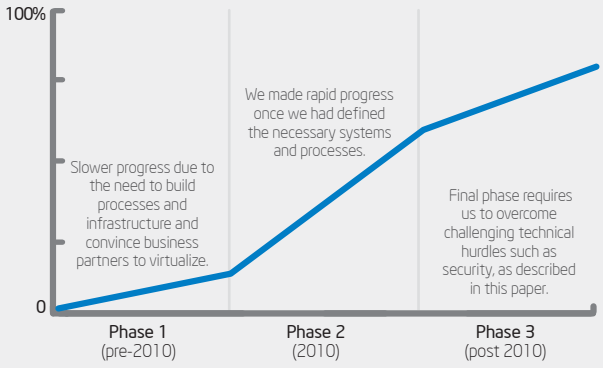

Figure 1. Intel IT virtualization progress

Mission-critical applications. To support these, we implemented features such as clustering, database mirroring, and Web server load balancing.

Very large VMs. We support VMs up to 48 GB in size today and anticipate supporting 96-GB systems in early 2012.

Lengthy backup and recovery. Some applications require very large backups; if we combine multiple applications onto a single virtualization host, the time required for backup could exceed the available backup time window. We have deployed new backup software that allows direct backup from storage area network (SAN) to tape; this is much faster because it removes the need for traffic to pass through the host.

Sarbanes-Oxley Act (SOX) compliance. We assessed whether there were SOX requirements that prevented us from virtualizing specific applications. We conducted a formal risk assessment to document the potential risks of virtualization to financial data, processes, and systems, and defined the necessary controls needed to mitigate those risks.

Challenges Remaining

Supplier support. Some software suppliers have not supported virtualization of their applications to date, due to performance, latency, licensing challenges, or other concerns. We have worked directly with each supplier to validate or overcome each challenge and anticipate that virtualization of some of these applications will be possible in the future.

Physical server connections. Some applications require direct access to peripherals or other external equipment rather than access through a hypervisor. This ties the application to the physical host, reducing flexibility and agility.

[1] "Applying Factory Principles to Accelerate Enterprise Virtualization." Intel Corporation, February 2011.

We set out to develop technical capabilities to achieve this separation, enabling us to virtualize applications with significant security requirements and move closer to our goal of virtualizing 75 percent of the environment.

IMPLEMENTING SECURE VIRTUALIZATION

Our goal was to enable secure virtualization of externally facing applications.

To achieve this, we increased security by enforcing separation between applications in the virtualized environment, analogous to the separation provided in the physical environment.

We implemented this separation at multiple levels.

- **Secure virtualization host architecture.** Within each virtualization host, we isolate applications by providing a dedicated PVLAN for each VM. For additional security, we also maintain separation of network and server administration duties.
- **Landing zones.** We segregate the virtualization hosts into secure landing zones within the virtualized environment. These are comparable to the security zones that exist in our traditional (physical) Office and Enterprise environment.
- **Secured management infrastructure.** We deploy a dedicated hardened virtualization management infrastructure separate from other virtual environments. This environment is hardened with additional controls over privileged and non-privileged access to the virtual environment, including controls that enforce separation of duties and robust logging of administrative activity.

Secure Virtualization Host Architecture

We designed a virtualization host and virtual networking architecture that enhances security by providing two significant security capabilities: a separate PVLAN for each VM and separation of administrative duties with role-based access.

We created this architecture by implementing capabilities based on new hypervisor and distributed switch features. Figure 2 shows our new secure virtualization architecture, together with our previous virtualization architecture for comparison.

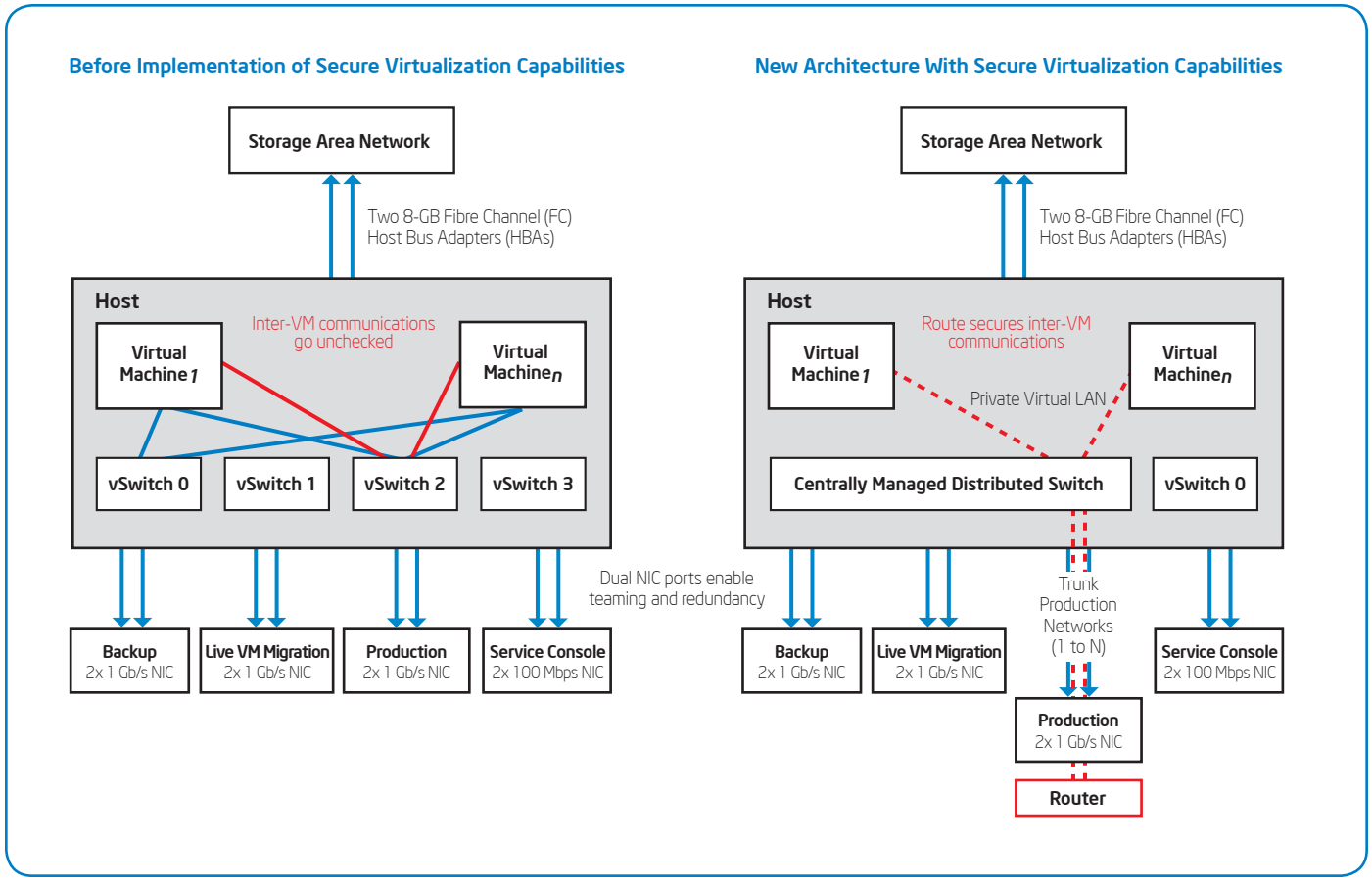

Figure 2. Intel IT virtualization host architecture for Internet-facing applications. Left: Before implementation of secure virtualization capabilities. Right: New architecture with secure virtualization capabilities.

In both architectures, each virtualization host uses eight physical network interface ports:

- Two 1 Gb NIC ports for production application traffic, shared among the VMs on the host.
- Two 1 Gb NIC ports for backup and recovery
- Two 1 Gb NIC ports for live VM migration
- Two 1 Gb NIC ports for connection to the hypervisor management software
- One 100 Mb NIC for server management

Virtualization hosts include virtual networking capabilities that are used by VMs residing on the server to communicate with each other and with resources outside the server. In our previous architecture, four virtual switches were used to connect the VMs to physical NICs. In the new architecture, this function is provided by a centrally managed distributed switch. The new architecture also takes advantage of recently introduced PVLAN capabilities in the hypervisor, which provide isolation between VMs by preventing unauthorized communications between them.

Features of the new architecture include:

Separate PVLAN for each VM by default. This provides application network isolation similar to the protection provided within our traditional computing environment. Network segmentation using PVLANs helps avoid a compromise affecting one application spreading to other applications.

In our traditional secure hosting environment, each physical server is connected to the enterprise network through a dedicated vLAN. All communication between vLANs passes through a gateway, which is typically a router that controls access based on security policy. The gateway thus filters all traffic between applications, helping to prevent compromises from spreading from application to application.

Our new secure virtualization architecture implements similar protection. As shown in Figure 2, each application has its own dedicated PVLAN, and all communications between applications pass through a firewall or other gateway. This applies even to communications between applications sharing the same host server. This approach thus helps prevent compromises from spreading from one VM to other VMs on the same or different hosts.

Separation of duties and role-based administration. Our secure virtualization architecture enables separation of duties, which is a key security concept. This reduces risk by allowing only network administrators to manage the network and only server administrators to manage the host. We are able to implement this because the distributed switch is centrally managed by network administrators rather than by server administrators. Management of the switch is secured using an authentication, authorization, and accounting (AAA) protocol.

Our architecture thus separates server and network administration. It provides role-based authentication and audit trails of all server and network management activities.

Secure Landing Zones

To further mitigate risk, we implement multiple landing zones, using an approach analogous to our physical environment. Virtualization hosts are clustered into separate landing zones, in order to maintain logical and physical isolation, within the DMZ. Each DMZ landing zone consists of a subnet protected from the Internet by a firewall and separated from the intranet by a different set of firewalls. We also implement secure internal zones (SIZs) that host applications that must integrate with the DMZ.

These zones help to prevent a successful attack from spreading through the virtualized environment and to detect when attacks occur. With this model, multiple VMs and landing zones would have to be breached to result in widespread compromise of the environment.

What Intel IT Does Not Plan to Virtualize

While many public clouds run entirely on virtualized infrastructure, achieving 100 percent virtualization in most enterprise environments may not be realistic or desirable, for a number of business and technical reasons. Examples of scenarios in which we do not expect to implement virtualization are:

Very large VMs (greater than128 GB today, such as in-memory databases). Some applications are too large for us to be able to consolidate multiple applications onto a single server. Therefore, there may be limited financial incentive to virtualize.

Small and medium remote sites. At small sites, it may not be cost-effective to install the virtualization infrastructure, such as a SAN, necessary to virtualize applications. Issues of latency also compel a need for local servers.

Applications where performance is critical. This includes some mission-critical software such as database applications.

Real-time applications. Some applications, such as real-time collaboration software, video, and Voice over Internet Protocol (VoIP), require very fast, predictable response times. These may require dedicated hardware rather than a shared host.

The organization of secure landing zones is shown in Figure 3 and described below.

DMZ

Externally facing applications typically consist of three software tiers:

- **Presentation layer.** This is the Internet-facing system that is directly accessed by users. It is typically a web server.
- **Application layer.** This contains the business logic.
- **Database layer.** This is the application data store.

Our traditional computing environment contains separate landing zones for presentation, application, and database tiers. Each tier of an application is typically implemented on a separate server that is deployed into the appropriate landing zone. A single landing zone may be shared by multiple applications, as long as they have similar risk profiles and do not require the highest levels of security.

Our secure virtualization environment implements a similar approach. The presentation, application, and database tiers of externally facing applications are separated into different landing zones within the DMZ. They may share virtualization hosts within each zone.

The DMZ also includes Services landing zones. These host services support the applications in the other DMZ zones: server and application monitoring, patch management, and authentication services for hosts and applications within the DMZ.

We implemented dedicated storage for each landing zone to provide additional protection. This helps prevent a compromised VM or hypervisor within a landing zone from spreading an infection to other landing zones by writing to a shared hard drive.

SIZ

The SIZ provides a secured hosting environment used for applications that must integrate with the DMZ and for deploying VMs to the DMZ. These include software that is used for logging, managing distributed virtual switches, and other administrative functions.

We also protect our hardened virtualization management systems by isolating them within a dedicated central management landing zone.

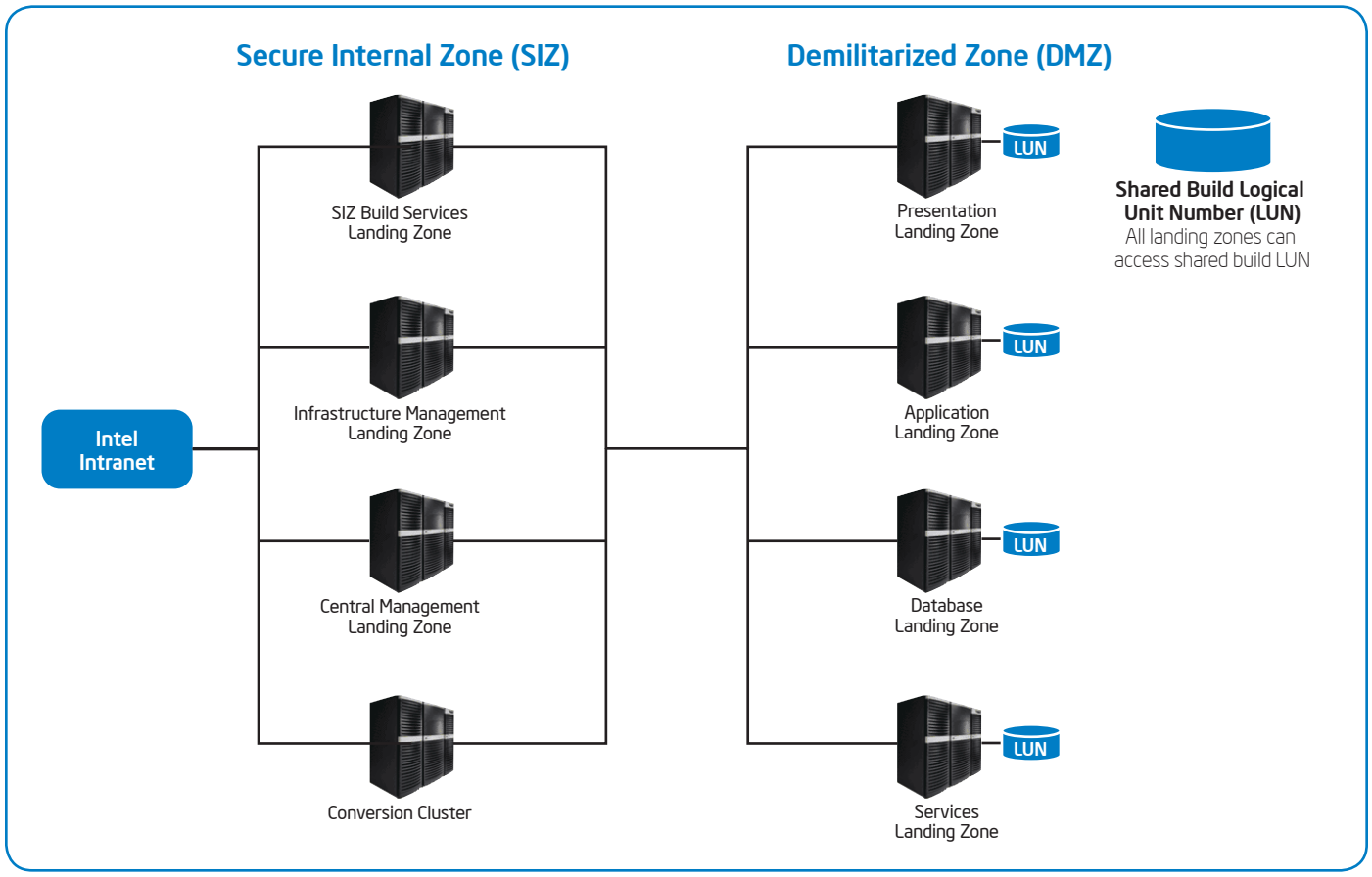

Figure 3. Secure virtualization environment landing zones.

VM Deployment and Provisioning

To deploy applications into our secure landing zones, we need secure provisioning processes and infrastructure so that we do not expose the internal production environment during the build process.

Deploying New Applications

To deploy new applications, we created a SIZ Build Services landing zone, as shown in Figure 3. Servers in this zone can gain access to the internal provisioning infrastructure in order to build a new VM. A shared build logical unit number (LUN) is used to temporarily store VM configuration data and other related files. Once the new VM has been created, we cold migrate the VM, as well as the related data, to the target zone. Only one-way migration is allowed from the Build zone. This helps prevent compromise of production systems in the DMZ from spreading to other zones.

Deploying Existing Applications

To migrate existing applications from our physical to virtualized environment, we created a zone that contains a cluster of hosts used for physical-to-virtual conversions. We first move applications to this zone; after conversion, the applications are then migrated to the target zone.

CONCLUSION AND NEXT STEPS

We designed and have begun implementing an environment that meets our security requirements for virtualizing Internet-facing applications within our private cloud.

We have already deployed our DMZ and SIZ virtualization infrastructure in multiple data centers and begun successfully migrating applications to it. We plan to rapidly expand and take advantage of this infrastructure throughout the Intel environment. By deploying applications into this environment, we plan to virtualize all suitable Internet-facing applications by 2012. This is a significant step toward our goal of virtualizing 75 percent of the Office and Enterprise environment.

Over time, we plan to take advantage of additional security features included in servers with Intel Xeon processors, including Intel TXT and enhanced encryption with Intel® Advanced Encryption Standard–New Instructions, to further increase the security assurance within our virtualized environment.

CONTRIBUTORS

Sridhar Mahankali
Ed Tafoya
Esteban Gutierrez
Sanjay Rungta

ACRONYMS

AAA	authentication, authorization, and accounting
DMZ	demilitarized zone
Intel® TXT	Intel® Trusted Execution Technology
LUN	logical unit number
PVLAN	private virtual LAN
SAN	storage area network
SIZ	secure internal zone
SOX	Sarbanes-Oxley Act
VLAN	virtual LAN
VM	virtual machine
VoIP	Voice over Internet Protocol

For more information on Intel IT best practices, visit www.intel.com/it.

Printed in USA
1111/ABC/KC/PDF

Please Recycle
326183-001US