illumio

WHITE PAPER

SECURING DATA IN TRANSIT

CONTENTS

OVERVIEW

BUSINESS DRIVERS

Data encryption is a necessity in today's dynamic data centers, where applications are multitiered, distributed, and hosted across environments with varying levels of trust. Encryption is an important part of securing communication between applications as well as communication within tiers of a single application hosted across physical and virtual workloads. Additionally, high-profile security breaches and insiderthreats, as well as regulatory requirements across industries, have driven enterprises to encrypt data within their own networks.

Scenarios where encryption of data in transit is necessary include:

- PCI compliance for credit card processing
- HIPAA compliance when transferring patient data over intermediate networks
- PII data exchanged over untrusted networks
- Sensitive data used by applications hosted by a public cloud provider
- Data exchanged across geographically distributed data centers

CURRENT CHALLENGES WITH SECURING DATA IN TRANSIT

- Manual configurations for IPsec communication are time-consuming and error-prone.
- Distribution and management of security keys becomes non-trivial as networks grow in complexity.
- Migration of workloads to public cloud infrastructure is slowed down by encryption needs.
- Virtual private clouds (VPC) used for traffic segregation in public clouds increase the complexity of IPsec management.

THE ILLUMIO SOLUTION

- **One-click IPsec connectivity.** Eliminates cumbersome manual processes to configure data in transit encryption with IPsec across applications
- **No dependency on infrastructure.** Works across bare-metal or virtual server infrastructure across data centers, public and hybrid cloud infrastructure.
- **Leverages existing infrastructure.** Requires no network changes or additional software and hardware costs.
- **Encryption is policy driven.** Encryption is automatically applied to workload communications based on policy when applications change, are auto scaled, or migrated.
- **Automates security operations.** Associating security policies with workloads right from inception means no manual intervention is required for securing traffic across newly instantiated or migrated workloads.

CURRENT APPROACHES TO SECURING DATA IN TRANSIT

Businesses have used one or more of the following solutions to prevent malicious interception of data when sensitive data is exchanged on networks—spending millions of dollars in the process.

LEASED LINES AND FRAME RELAY CIRCUITS

Businesses use leased lines and frame relay circuits, which create a direct and dedicated connection between distributed networks, when security requirements are stringent and outweigh the expense of setting up and paying for such connections. While these technologies are expensive—and not widely available—they provide data isolation against malicious snooping. Enterprises can achieve secure data transportation without having to set up a choke point to encrypt the traffic.

IPSEC COMMUNICATION

Organizations implement IPsec-based virtual private network (VPN) solutions on dedicated security appliances. IPsec encrypts traffic between end points and can protect against eavesdropping, man-in-the-middle, and denial-of-service (DoS) attacks.

- **Hardware security appliances:** In the early days, IPsec VPNs were set up using dedicated VPN hardware. VPN has since become a component of perimeter firewalls, making it possible for access and egress security policies to be applied to traffic destined for the VPN tunnel before being encrypted. This worked for environments that were static and when hosts were on the same network. But, hardware appliances have finite processing capacity and any upgrades involved capacity-planning efforts for IT teams and potential downtimes that hindered service-level agreement commitments.
- **Software security appliances:** Software firewalls and VPN virtual appliances offer significant cost savings over hardware appliances. With these solutions, adding capacity is easy since virtual appliances can be scaled up by spawning new virtual instances. However, virtualized VPN appliances may share resources with other VMs running on the consistent and predictable VPN throughput, especially during peak loads.

SSL-BASED ENCRYPTION OF DATA IN TRANSIT

The secure sockets layer (SSL) protocol is often used to secure data in transit across untrusted networks. With SSL VPN, encrypted connections are established at the application layer; this differs from IPsec VPNs, which use the network layer of the OSI model. Unlike IPsec VPNs, SSL VPNs have dependencies on the underlying applications and require customizations. In addition, SSL VPNs require separate security key negotiations for every TCP connection. IPsec VPNs avoid this potential performance hit since key negotiation occurs just once for all network layer connections in the tunnel.

Each of these technologies has its benefits, but IPsec connections are considered the most economical since they leverage well-known and time-tested encryption technologies without the need for dedicated carrier-provided resources.

FIVE KEY CHALLENGES WITH EXISTING SOLUTIONS

1. Errors and delays due to complicated IPsec configurations

While IPsec can effectively secure data communications across untrusted public networks, administrators must manually configure all parameters, which is both time consuming and error prone. Every connection requires setting up at least the following parameters—on both ends of the VPN tunnel:

- IP addresses of both security appliance interfaces
- Authentication algorithms
- Encryption protocols
- Security associations and key management
- List of exportable subnets, interface bindings, etc.

IPsec configurations can also complicate security configurations on firewalls. Due to the high processing demands of IPsec connections, organizations tend to limit data encryption to business-critical traffic. This is typically implemented by assigning VPN tunnels to security zones, which increases the complexity of setup and maintenance when an enterprise employs distributed data centers with numerous security zones and related security policies.

2. IT resource drain due to key management

IPsec requires either PKI infrastructures or pre-shared keys for peer authentication. Key and certificate management involve manual processes and the configuration of a large number of end points for secure connections, making it a non-trivial task. IPsec also requires specific IT skills and could potentially strain already stretched IT resources.

3. Scalability limitations of static VPN solutions

Network-based VPN solutions are static and are not built for today's highly scalable and dynamic data centers and clouds. Application migrations (moves, adds, and decommissions) are limited to the boundaries of predefined security zones and VLANs. As soon as application needs go beyond the scope of security zones, manual reconfigurations of IPsec settings are required, which could be time consuming and lead to errors.

4. Lack of IPsec vendor interoperability in public cloud

Although there have been recent improvements, IPsec implementations have had compatibility issues between vendor implementations in public cloud environments. Extending secure connectivity to public cloud infrastructure makes VPN configurations even more challenging due to different VPN solutions offered by cloud providers. These issues could increase the risk of misconfigurations and slow down application rollouts.

5. VPCs increase management complexity in public cloud

In private data centers, traffic streams are managed by a perimeter gateway where security zones and egress policies are applied to segregate VPN flows and achieve application isolation. This segregation of traffic flows is implemented in public cloud environments by using VPC technology with a virtual private gateway at the edge to terminate the IPsec connections. This works well as long as the organization has a limited number of relatively simple applications. However as the number of applications increase, more VPCs are needed, which increases the complexity of application connectivity and management.

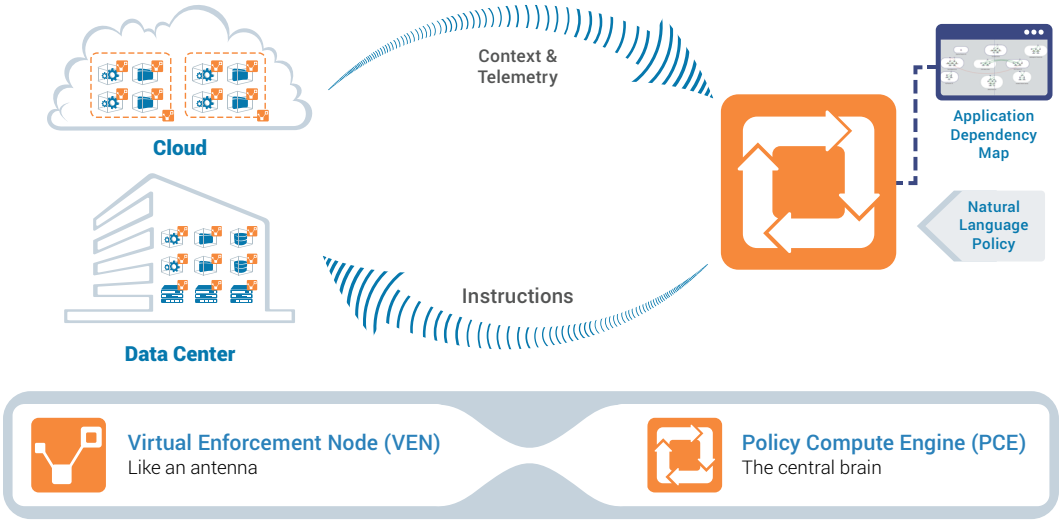
THE ILLUMIO SOLUTION

Illumio Adaptive Security Platform (ASP)™ secures enterprise applications in data centers and private, public, or hybrid cloud environments by decoupling security from the underlying infrastructure. The platform continuously computes security for enterprise applications by using the dynamic context of individual workloads running on virtual machines or physical servers.

The **Illumination** service provides visualization of applications and workload interactions with a graphical view of application topology to help inform security and policy decisions.

The **Policy Compute Engine (PCE)** is a centralized controller than manages all of the state and policies of the computing environment it visualizes and protects. It examines the relationships among workloads, computes the rules required to protect each workload, and distributes those rules out to the **Virtual Enforcement Nodes (VENs)** on the workloads.

Illumio ASP includes support for policy-driven encryption through the **SecureConnect** capability, which provides on-demand IPsec connectivity between workloads regardless of the underlying infrastructure.



The Illumio solution addresses the challenges listed above by providing:

1. One-click IPsec configuration

Illumio completely removes the dependency on physical or virtual network appliances to encrypt traffic. With the simple click of a button, secure IPsec connectivity is initiated between any combination of Linux or Windows workloads across any infrastructure. IPsec configurations also move with workloads as they migrate within or across data centers, public clouds or virtual private clouds. The PCE orchestrates the enforcement of the IPsec configurations and security policies across the workloads. Pre-shared keys that are dynamically generated by the PCE automate key management for the end points that are part of the IPsec connection. Additional security is provided by using the pairing key as the root of trust for setting up the individual IPsec tunnels between workloads.

2. Policy-driven encryption and application agility

The Illumio model provides a simplified, yet adaptive approach to securing traffic using the context of workloads. A flexible, multi-dimensional labeling mechanism is used to define a workload's context based on its processing role, the application thatit serves, its business environment and its location. This approach allows administrators to define security along with secure connectivity in the form of human-readable, explicitly allowed policies. Encrypted communication is automatically setup across all the workloads that match the labels configured as part of the security policies.

The context of the workload (including any environment or IP address changes, etc.) is continuously computed and mapped to its security policies along with its IPsec settings. Newly instantiated workloads automatically inherit pre-configured SecureConnect settings as soon as they are brought under management by pairing them with the PCE. With SecureConnect configured, any traffic initiated to or from new workloads is encrypted without the need for any manual intervention.

3. No dependency on Infrastructure

With Illumio SecureConnect, host-to-host IPsec connectivity can be set up between any number or combination of workloads running on bare-metal servers or VMs. Secure, encrypted communications are established without requiring any changes or upgrades to the existing network infrastructure across private data centers or public cloud providers like Google, Rackspace, AWS, and Azure.

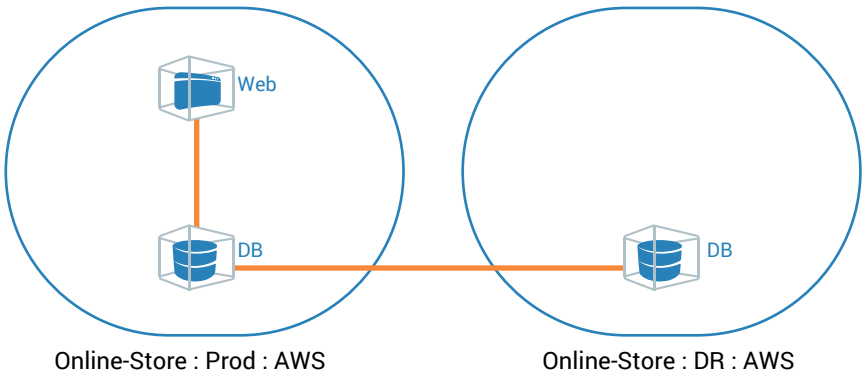
USE CASE: SECURING DATA IN TRANSIT WITH ILLUMIO

To illustrate how Illumio ASP can be used to encrypt traffic flows, consider ABC Corp., an enterprise using Illumio SecureConnect to encrypt traffic flows for its multitier Online-Store application.

IDENTIFY WORKLOADS WITH FLEXIBLE MULTIDIMENSIONAL LABELS

ABC Corp uses Illumio's flexible, multidimensional labeling mechanism to characterize workloads based on their role (database, web server, etc.), application (HR, Ordering, Sales, etc.), environment (testing, staging, production, etc.), and location (US data center, AWS, Azure, etc.). For the workloads that make up the Online-Store application the labels are shown in the table below:

	ROLE	APPLICATION	ENVIRONMENT	LOCATION
Web workloads	Web	Online-Store	Production	AWS
Database workloads	DB	Online-Store	Production	AWS
Database-Backup	DB	Online-Store	DR	AWS



ILLUMIO ASP MAKES IT EASY TO WRITE SECURITY POLICIES BASED ON LABELS

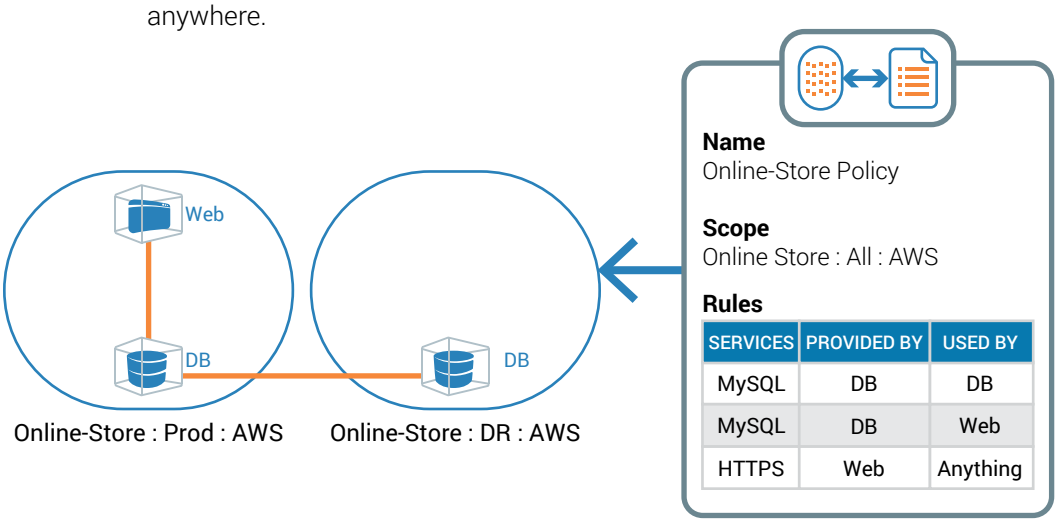
Once ABC Corp. has labeled its workloads, it can write security policies to capture the interactions that are explicitly allowed (whitelisted policies) between the workloads. By definition, all other interactions will be denied.

In the case of the Online-Store application, which uses a web front end and a database back end, ABC Corp. wants to ensure that:

- Port 443 (HTTPS) is open to the internet on web servers.
- Web servers are allowed to access MySQL running on the database server over port 3306.
- SecureConnect will be used to secure traffic between:
  - Web and the database tiers, to ensure data is encrypted over network paths all the way to storage.
  - Master and backup database servers.

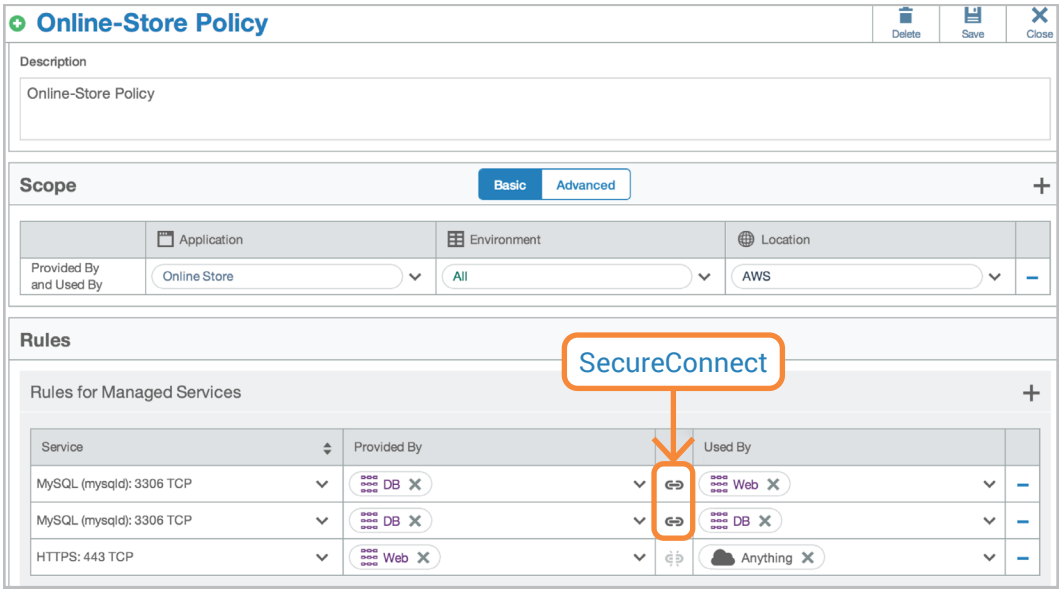
The figure below shows the ruleset that describes the relationships between the workloads of the Online-Store application.

- **RULE 1:** MySQL service running on the database server is accessible from the web server.
- **RULE 2:** MySQL service running on the primary database server is accessible from backup database server.
- **RULE 3:** HTTPS services running on web servers are accessible from anywhere.



ENCRYPTING DATA IN TRANSIT WITH SECURECONNECT

ABC Corp. uses SecureConnect to encrypt data in transit between the workloads. ABC Corp. enables SecureConnect by clicking on the SecureConnect button highlighted in the rulesets below:



As soon as the ruleset is saved and provisioned, traffic flows between the web and database workloads and the master database and backup database workloads are encrypted.

The following IPsec parameters are automatically set up by SecureConnect to encrypt network traffic between the workloads:

IPSEC PARAMETER	VALUE
IKF Version	IKFv2
IKE Auth	Pre-shared key
SA Lifetime	1 hour
Type	Transport Mode
Cipher Suite	Suite-B-GCM-256 (RFC 6379)
ESP Encryption and Integrity	AES-256-GCM
IKEv2 Encryption	AES-256-CBC
IKEv2 PRF	HMAC-SHA-384
IKEv2 Integrity	HMAC-SHA-384-192
IKEv2 DH Group	384-bit random ECP
Dead Peer Detection	On
NAT Traversal	On

Illumio completely eliminates the complexity of configuring IPsec connections. With a simple click of a button, host-to-host IPsec communication is established between workloads across public, private, or hybrid clouds without any dependencies on the underlying infrastructure.

ABOUT ILLUMIO

Illumio, the leader in micro-segmentation, prevents the spread of breaches inside data center and cloud environments. Enterprises such as Morgan Stanley, BNP Paribas, Salesforce, and Oracle NetSuite use Illumio to reduce cyber risk and achieve regulatory compliance. The Illumio Adaptive Security Platform® uniquely protects critical information with real-time application dependency and vulnerability mapping coupled with micro-segmentation that works across any data center, public cloud, or hybrid cloud deployment on bare-metal, virtual machines, and containers. For more information about Illumio, visit www.illumio.com/what-we-do or follow @Illumio.

- Engage with Illumio on Twitter
- Follow Illumio on LinkedIn
- Like Illumio on Facebook
- Subscribe to the Illumio YouTube Channel

CONTACT US

For more information about Illumio ASP and how it can be used to achieve environmental separation, email us at illuminate@illumio.com or call 855-426-3983 to speak to an Illumio representative.

Illumio, Inc. 920 De Guigne Drive, Sunnyvale, CA 94085 Tel (669) 800-5000 www.illumio.com