CERTES NETWORKS

White Paper

TrustNet Group Encryption

Executive Summary

Protecting data in motion has become a high priority for a growing number of companies. As more companies face the real and growing threat of data theft, along with increased regulatory pressure to protect their data, encryption of data in motion has gone from a “nice to have” technology to a budgeted project. However, companies that have deployed IPsec VPNs across their network have discovered that while encryption is a great mode of data protection, the deployment and management of network encryption is difficult, time consuming and largely incompatible with other network requirements, such as flexibility, performance and intelligent traffic routing.

Encryption often gets the blame for poor network performance (in terms of bandwidth and latency) and time-consuming management, but upon closer examination, one finds that the issue is not the encryption, but the set-up and management of the encryption and the artificial constraints that historical network encryption solutions have imposed upon the network.

The heart of the problem is that organizations are trying to use a method for key generation and distribution that was designed to secure point-to-point links, not the any-to-any networks in use today. Originally defined in 1998, Internet Key Exchange (IKE) is a remarkably efficient and creative method for distributing shared encryption keys between two routers. However, it is fundamentally limited to exchanging keys between only two endpoints. IKE was not and is not a solution designed for distributing a shared key to a group of endpoints.

This white paper introduces TrustNet Group Encryption for policy and key management. TrustNet makes network encryption quick to set up, easy to manage, and transparent to network and application performance and behavior. TrustNet decouples security policy, key management and policy enforcement in order to provide an optimal solution to each of these separate problems. TrustNet securely distributes shared group keys among authorized group members so that any group member can encrypt and decrypt traffic to and from any other group member.

While TrustNet is not the only solution available for group encryption, TrustNet provides a number of unique and important benefits that no other group encryption solution can claim.

The Challenges of Securing Any-to-Any Networks with a Point-to-Point Solution

Protecting data in motion has been a best practice since the introduction of networking. As networking technologies have advanced, so has the technology used to secure data in motion. With today's IP-based networks, the data in motion standard is IPsec for data packet protection and Internet Key Exchange (IKE) for point-to-point key management.

IPsec was designed to provide encryption and authentication of IP packets and IKE was designed to exchange keys between two points across an untrusted connection. To use IKE for key management, a connection is initiated, each endpoint authenticates the other, and the peers negotiate symmetric keys for the connection. The result is a point-to-point secure tunnel through the network. While IKE is an effective means of exchanging keys between two endpoints, it only works between two endpoints and thus it is only a point-to-point solution.

IPsec packet protection requires the configuration of traffic policies at each endpoint or gateway for all other potential peer destinations. For each connection, the algorithms for protection, authentication, key exchange, gateway addresses, and numerous other parameters must be defined. Each end of the tunnel must have the same configurations or the IKE negotiation will fail. In configuring an IPsec deployment, most systems require each unit to receive a painstakingly generated set of policies carefully crafted and manually installed on each system.

The point-to-point nature of an IKE-created IPsec tunnel precludes the effective use of IPsec for multicast traffic, latency sensitive applications, and multi-path data flows because IKE views all connections as point-to-point. The point-to-point nature of IKE often causes unnecessary traffic "hairpins" where traffic is aggregated to a central hub and then redistributed. This may be done to avoid tunnels between each pair of endpoints in the network, but the result is increased network latency as traffic is encrypted and decrypted at the aggregation point, and extra latency as the traffic is backhauled to the aggregation site and then redistributed to the destination. The point-to-point orientation of IKE-created IPsec tunnels also makes provisioning, status monitoring and error detection problematic, as there is typically no centralized management for the secured network. This also makes auditing the secure network a challenge.

Point-to-point tunnels have an inherent scalability problem. The number of point-to-point tunnels required to achieve full-mesh connectivity for n nodes is approximately n^2. In other words, for a network with 100 nodes, approximately 10,000 point-to-point tunnels are required. Each tunnel requires CPU and memory resources to set up and maintain. These resource requirements quickly become significant and limit the overall router performance and scalability. In addition to the tunnel setup and maintenance requirements, the router must consider each policy rule for each incoming and outgoing packet (policy rules specify which tunnel and which encryption keys to use). So in addition to the CPU load due to tunnel setup and maintenance and performing the encryption, the policy lookup puts a heavy burden on the CPU. In addition to the likelihood of configuration errors for such a large task, the loading, reviewing, and monitoring of the thousands of policies on each machine can quickly become overwhelming to the security administrator.

IKE is most often deployed on routers, which does not allow the security team to have any control over security policies or encryption keys. Only by taking security out of the router and deploying it on a separate device, and by providing role-based access to security administrators, can the security team have effective control and responsibility for network security.

The combination of these factors diminish the investment made in the router and make IKE-based IPSec hard to maintain, which costs you money.

A Smarter Approach to Network Encryption

Given that the management costs and performance issues associated with network encryption are a direct result of using IKE, it stands to reason that a policy and key management solution designed specifically for network encryption deployments would eliminate the issues noted above. A purpose-built solution would greatly reduce the complexity of configuration, remove the current challenge of scale, and eliminate the limitations for multicast or multiple path encryption.

In order to accomplish this goal, the solution should:

- Distribute keys efficiently using group keying to allow any-to-any encrypted and authenticated communication among group members
- Expand IPsec protection to multicast and multiple nodes through group keying with centralized management of keys and policies.
- Simplify management through centralized, straightforward policy definition, distribution and management.
- Provide maximum security and network uptime with reliable and scalable key and policy distribution and regular key rotation
- Separate security from the router and provide role-based access control to allow the security team to control keys and policies while allowing cost-effective outsourcing of network management functions.
- Use IPsec standards-based packet formats and FIPS 140-2 validated AES-256 encryption to provide Layer 2 Ethernet encryption, Layer 3 IP encryption or Layer 4 payload-only encryption.
- Duplicate the inner IP address to the outer IPsec header to preserve routing information.

TrustNet Group Encryption

In order to meet these requirements, Certes Networks developed TrustNet, an evolutionary group encryption solution. With TrustNet, encryption and authentication keys are generated centrally and then securely distributed to all of the authorized group members. This is the fundamental difference between TrustNet and IKE key distribution. TrustNet Group Encryption avoids point-to-point tunnels and the associated configuration and maintenance headaches associated with point-to-point-tunnels by distributing the encryption keys to all group members so that any group member can communicate securely with any other group member (see Figure 1 below). Encryption keys are distributed to Certes Enforcement Points (CEPs) which enforce the encryption and authentication policies.

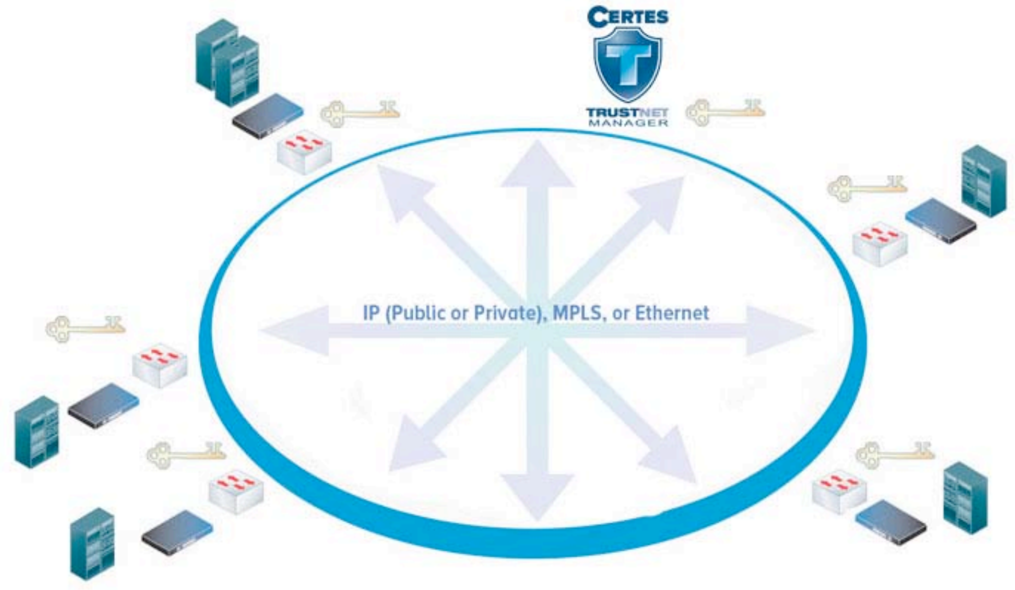


Figure 1: TrustNet Group Encryption

In some cases, all of the CEPs in the network are defined to be in a single group so that any site can send and receive encrypted data to and from any other site. Each site in the group possesses the shared group key, so all of the sites in the group can communicate. In other cases, administrators may want to segment the network into trust zones to isolate areas of the network that are particularly sensitive from the rest of the network. With TrustNet Group Encryption, groups of CEPs can be placed into multiple sets so that sites in different groups do not have the same encryption and authentication keys. This provides cryptographic isolation based on strong encryption (AES-256) and authentication (SHA-1); decrypting the traffic requires access to a key that is constantly rotated. Sometimes firewalls are used for this purpose, but group encryption provides stronger isolation that is much harder to bypass.

TrustNet Group Encryption does not interfere with network optimization and high availability features such as load balancing, traffic engineering, and fast failover because any group member can receive and decrypt the traffic.

TrustNet is a major technological advancement over tunnel-based IPsec solutions, over Layer 2 encryption-only solutions and over other Layer 3 group encryption solutions. TrustNet is the only solution that supports group encryption across multiple network layers (Layer 2 Ethernet, Layer 3 IP, or Layer 4 payload-only encryption). It is the only solution that supports group encryption across the Internet or in a private network with multiple carriers. It is also the only solution for group encryption that separates encryption from the router in order to provide network encryption that can be controlled by the security team without affecting the applications and services of the network. TrustNet provides authentication on a packet-by-packet or frame-by-frame basis. Security experts have proven that encryption without authentication is not secure. It is critical that authentication always be used with encryption to provide data confidentiality and integrity.

TrustNet Architecture

The TrustNet Manager user interface securely connects to the central TrustNet Manager server cluster in order to define group policies. Group policies specify what traffic to secure, how to secure it and which enforcement points should use the rule. Group policies also specify which encryption and authentication algorithms to use and how often to rotate the keys. The TrustNet Manager server cluster generates keys and securely distributes the keys and group policies to Certes Enforcement Points (CEPs). The TrustNet Architecture is shown below in Figure 2.

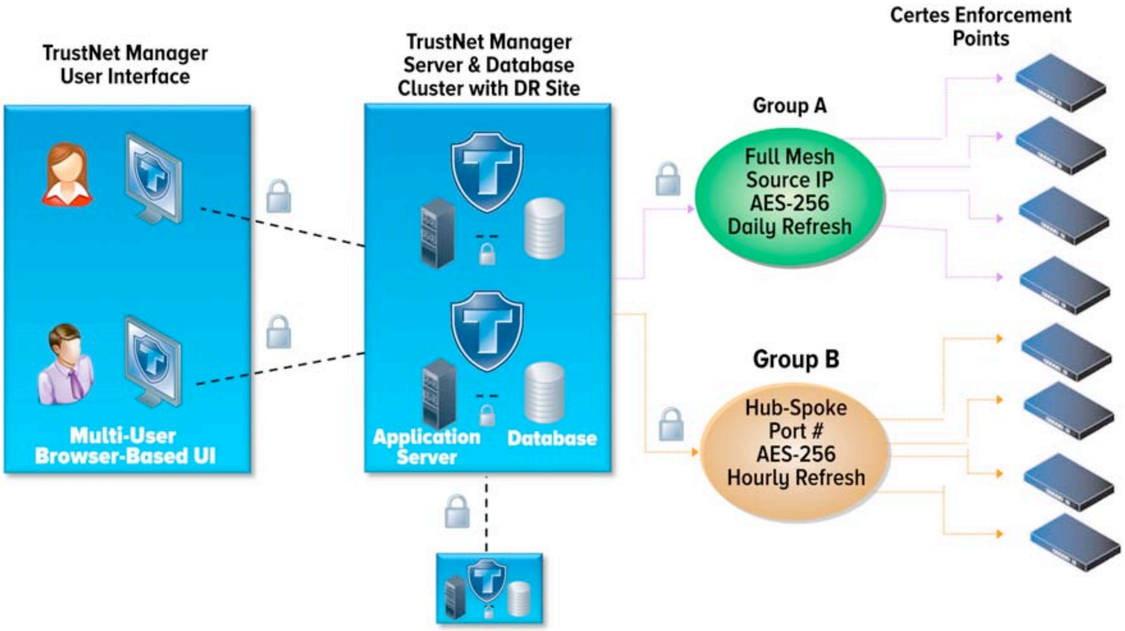

TrustNet Manager User Interface
TrustNet Manager Server & Database Cluster with DR Site
Certes Enforcement Points
Group A
Full Mesh
Source IP
AES-256
Daily Refresh
Group B
Hub-Spoke
Port #
AES-256
Hourly Refresh
Multi-User Browser-Based UI
Application Server
Database

Figure 2: TrustNet Architecture with group policies

Communication between the TrustNet Manager browser-based interface and the server is protected using a secure SSL (TLS) encrypted connection. Certificate exchange is used to authenticate the server and prevent man-in-the-middle attacks. A username and a password are required to log in to the server.

The TrustNet Manager server securely distributes keys and policies to the CEPs using SSL (TLS) encrypted and authenticated sessions, with optional bilateral authentication (where both sides check the certificate of the other side) to prevent man-in-the-middle attacks. The system supports RSA key sizes up to 4096 bits for protecting the key distribution channel.

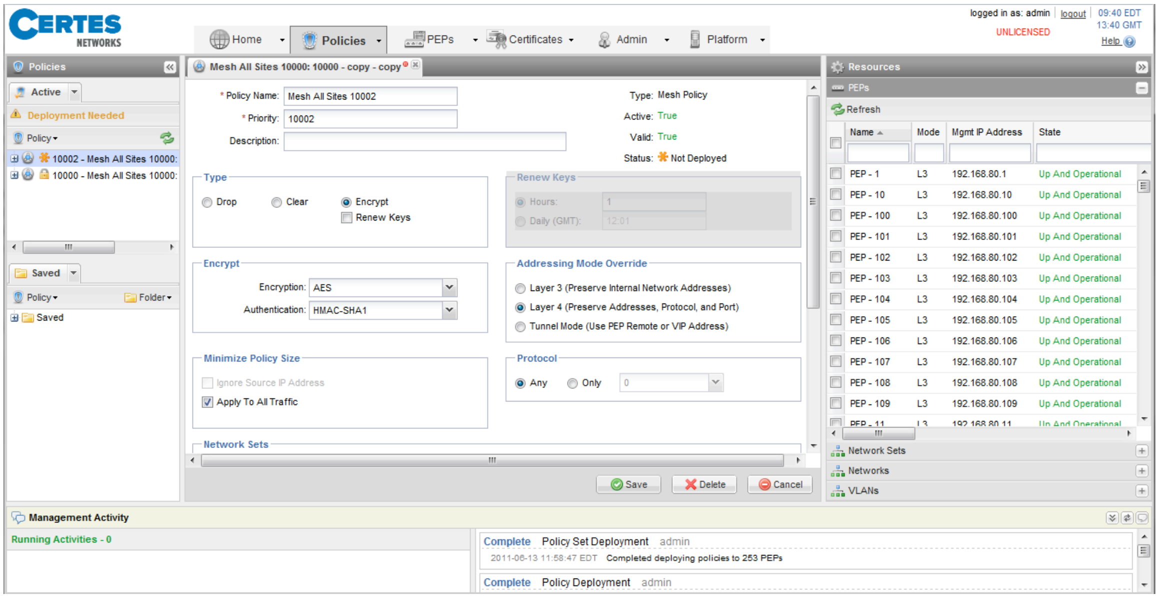
TrustNet Group Policies

TrustNet allows group policies to be defined flexibly according to any organization’s security needs. The whole network can be encrypted using one shared key, or unique keys can be allocated per group to cryptographically segment the network. Each group policy specifies:

- the group of CEPs to which the policy applies
- the packet selection criteria (for example “encrypt everything”, or “encrypt according to VLAN id, IP addresses, protocols, ports, etc.”, or “leave all protocol control traffic in the clear”)
- the policy action: encrypt, pass in the clear, or drop

- the re-key period
- the encryption and hash algorithms to be used
- whether the key generation technique being used is per group or global

The ability to define group encryption policies from a central location greatly simplifies the installation and management process of network encryption. Changes to the network can be accomplished in seconds using the drag and drop policy builder, even for large networks with multiple, overlapping encryption groups. The result is that it is easy to define and deploy group encryption policies from anywhere using a central server for key generation and distribution. Figure 3 below shows the TrustNet user interface.



logged in as: admin | logout | 09:40 EDT 13:40 GMT
UNLICENSED
Help

10002 - Mesh All Sites 10000:
10000 - Mesh All Sites 10000:

Mesh All Sites 10000: 10000 - copy - copy

* Policy Name: Mesh All Sites 10002
* Priority: 10002
Description:

Type: Mesh Policy
Active: True
Valid: True
Status: Not Deployed

Type
○ Drop ○ Clear ● Encrypt
□ Renew Keys

Renew Keys
● Hours: 1
○ Daily (GMT): 12:01

Encrypt
Encryption: AES
Authentication: HMAC-SHA1

Addressing Mode Override
○ Layer 3 (Preserve Internal Network Addresses)
● Layer 4 (Preserve Addresses, Protocol, and Port)
○ Tunnel Mode (Use PEP Remote or VIP Address)

Minimize Policy Size
□ Ignore Source IP Address
☑ Apply To All Traffic

Protocol
● Any ○ Only 0

Network Sets

□	Name	Mode	Mgmt IP Address	State
□	PEP - 1	L3	192.168.80.1	Up And Operational
□	PEP - 10	L3	192.168.80.10	Up And Operational
□	PEP - 100	L3	192.168.80.100	Up And Operational
□	PEP - 101	L3	192.168.80.101	Up And Operational
□	PEP - 102	L3	192.168.80.102	Up And Operational
□	PEP - 103	L3	192.168.80.103	Up And Operational
□	PEP - 104	L3	192.168.80.104	Up And Operational
□	PEP - 105	L3	192.168.80.105	Up And Operational
□	PEP - 106	L3	192.168.80.106	Up And Operational
□	PEP - 107	L3	192.168.80.107	Up And Operational
□	PEP - 108	L3	192.168.80.108	Up And Operational
□	PEP - 109	L3	192.168.80.109	Up And Operational
□	PEP - 11	L3	192.168.80.11	Up And Operational

Running Activities - 0

Complete Policy Set Deployment admin
2011-06-13 11:58:47 EDT Completed deploying policies to 253 PEPs

Complete Policy Deployment admin

Figure 3: TrustNet Manager policy creation GUI

TrustNet Manager makes it easy to deploy policies without breaking the network by automatically checking the policies for mistakes and by showing the user which network elements will be affected by a policy change, before the change is made. TrustNet Manager users can also save and retrieve policies so a policy can always be recovered. These features make it easy to avoid mistakes and to recover the previous state.

TrustNet Role-based Access Control

TrustNet Manager offers role-based access controls that provide separate roles for security control and network management. The following are a few of the roles provided by TrustNet Manager:

- Administrator
- Policy Creator
- Policy Deployer
- Appliance Administrator
- Appliance Operator

Each user can be assigned one or more of these roles. By using roles and separating duties among personnel, organizations can follow security best practices and even outsource some network management tasks while retaining control of security-critical responsibilities.

TrustNet with Multicast

TrustNet Group Encryption is well suited to encrypting multicast traffic because traffic encrypted with a group key can be decrypted by all of the group members without re-encapsulating it or rekeying it for each individual destination with a unique key (as is necessary with IKE tunnels). Encryption groups can easily be created for multicast video or Voice over IP without adding measurable latency or jitter, and without the need to modify native traffic flows. The benefit of this approach is that multicast traffic can be encrypted without changing the application or the network.

TrustNet Key Rotation

TrustNet Manager automatically performs key rotation for all CEPs in the network by generating new keys and distributing the keys to the CEP appliances to replace the old keys. This key update feature can be set to occur at specified intervals or at specific times, all being set by the security administrator.

Frequent key rotation makes it much more difficult for an attacker to decrypt the data and a brute-force attack on the AES-256 encrypted data can only expose the data sent during a single rekey period. After keys are rotated, the attacker needs to start over, so the payoff and hence the incentive to carry out an attack are minimized.

TrustNet High Availability

TrustNet Manager operates continuously; generating new keys and resending any failed rekey messages. In deployments where TrustNet Manager is running on a cluster of servers, any cluster node can fail without affecting the rekey schedule, since both cluster elements are tightly synchronized with the same rekey information. In the event of a failure of the main site, the disaster recovery site with TrustNet Manager will perform a network rekey and take over scheduled rekey operations automatically until the main TrustNet Manager site returns to active status.

Group Encryption Payload

TrustNet's ability to deploy transparent group encryption over any infrastructure or topology is made possible by the solution's ability to encrypt only the payload portion of a frame or packet and leave the header information in the clear. TrustNet can encrypt the payload at Layer 2 (Ethernet), Layer 3 (IP) or Layer 4 (IP). TrustNet also works transparently with MPLS-based services such as IP VPN and Metro Ethernet services such as E-LAN and E-Line.

TrustNet uses standards-based IPsec packet formats for Layer 3 (IP) encryption and authentication. TrustNet preserves the original IP header, rather than appending a tunnel IP address when encrypting the entire IP packet; this allows the encapsulated packet to be sent through the network with no changes. TrustNet uses header and packet formats that are similar to the IPsec standard formats for Layer 2 and Layer 4 encryption and authentication. TrustNet uses standard algorithms for encryption and authentication: FIPS 140-2 validated AES-256 for encryption and FIPS 140-2 validated HMAC-SHA-1-96 for authentication. TrustNet also supports other algorithms.

Figure 4 below shows the various packet formats utilized by the CEP appliances.

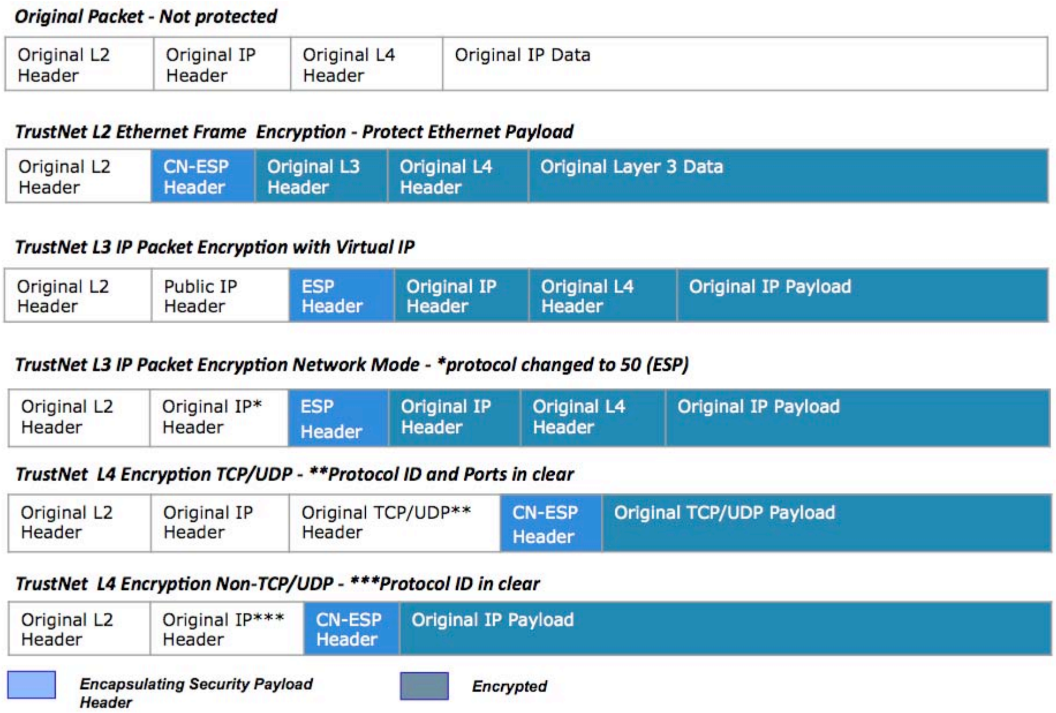


Figure 3: TrustNet Packet and Frame Formats

TrustNet Group Encryption at Layer 2 not only leaves VLAN information in the clear, but it also allows group encryption policies to be based on VLAN IDs. TrustNet allows users to create IP or MPLS encrypted groups for multiple topologies at Layer 3. Only TrustNet has the ability to encrypt the data payload while leaving the Layer 4 header in the clear. This unique capability preserves network services that rely on information contained in the Layer 4 header, such as traffic shaping, CoS-based routing, and Netflow or J-Flow. Furthermore, payload-only encryption at Layer 4 simplifies network troubleshooting by passing all of the headers in the clear. This allows the networking team to troubleshoot an encrypted network, without having to turn off the encryption. This is very difficult to do with other network encryption solutions.

While authentication headers and preserving packet headers adds a small amount of overhead to each packet, the CEP appliances compensate by supporting line rate fragmentation and reassembly. When a large packet exceeds the link MTU, the CEP appliances transparently fragment it and later reassemble it after authenticating and decrypting the fragments at wire speed. Fragmentation avoids changing the network MTU (which may be impossible if the network is owned by a service provider) and it avoids sending ICMP messages to the host (which are often blocked by firewalls).

TrustNet Group Encryption Applications

Layer 3 WAN (IP/MPLS) Encryption
While MPLS and other forms of IP transport remain popular due to their improved performance and cost benefits over private lines, there is now broad consensus that the logical separation offered by MPLS is not secure and is not an adequate form of data protection. With TrustNet, organizations can now secure their data across the WAN using group encryption policies that mirror their WAN transport topologies and application flows. TrustNet offers transparent data privacy and regulatory compliance without any changes required to the existing infrastructure.

Layer 2 WAN (Metro Ethernet/VPLS) Encryption
Customers using Layer 2 technologies for their WAN are often forced to deploy point-to-point encryption solutions, or worse, introduce latency-inducing Layer 3 VPNs to secure their data in motion. TrustNet allows companies to secure their data with an encryption solution that can secure any Layer 2 topology, including multipoint-to-multipoint or mesh. Only TrustNet Group Encryption allows policies based on VLAN IDs, allowing companies to cryptographically segment their VLANs. Unlike many other Layer 2 encryption solutions, TrustNet provides authentication for each encrypted packet and frame. Authentication is a critical component of security. Encryption without authentication is not secure and it can result in network attacks that provide enough information to tamper with or even decrypt and read encrypted data.

VoIP/Multicast Video Encryption
VoIP and multicast video are two of the fastest growing network applications. Organizations recognize the need to secure these applications, but concerns about the latency and jitter of IPsec VPNs often lead to these applications operating in the clear. With TrustNet, encrypting VoIP or Video can be accomplished without impacting quality or adding jitter. TrustNet offers group encryption policies for multicast, full mesh, and hub and spoke topologies. This allows applications to flow in their native environment without redirects and without the need to re-encrypt each packet for each destination.

Data Center and Private Cloud Security
TrustNet makes it easy to encrypt data coming in and out of data centers and private clouds. By creating encrypted groups and setting a “deny all, permit by encryption group association” policy, enterprises can not only protect their data in motion, but can also ensure that the data was not modified in transit because TrustNet authenticates on a packet by packet basis. In addition, the wire speed capabilities of the CEP encryptors make it possible to discard unauthorized packets at wire speed, helping to prevent DDoS attacks.

Encryption as a Service
TrustNet is an ideal solution for service providers looking to offer Encryption as a Service (EaaS). TrustNet allows service providers to add an encryption service without altering the existing network infrastructure or modifying the customer-premise router/switch. The unique ability to leave the Layer 4 header in the clear ensures that this value-added security does not impact SLA’s that use Layer 4 information to shape or monitor traffic. With its distributed web-based architecture, TrustNet Manager provides an ideal platform for customers to have a web-based portal to monitor the status of the managed encryption service from anywhere in the world.

Public Internet and Multi-Carrier
TrustNet’s ability to create flexible policies that meet the requirements of any network is unique among network encryption solutions. TrustNet is the only group encryption solution that supports

multiple network layers (using Layer 2 Ethernet, Layer 3 IP, or Layer 4 payload-only encryption), group encryption over the public Internet (or with a mix of public and private addresses) and group encryption in a multi-carrier environment.

About Certes Networks

Certes Networks is the leader in developing scalable security solutions for high performance networks. We provide advanced encryption and policy and key management solutions for securing wide area networks, and enable secure connectivity to private and public clouds. Certes Networks helps organizations improve security, decrease risk, and reduce the cost of compliance with data privacy regulations while enabling high performance and secure connectivity to critical infrastructures in the branch office, data center or in the cloud.