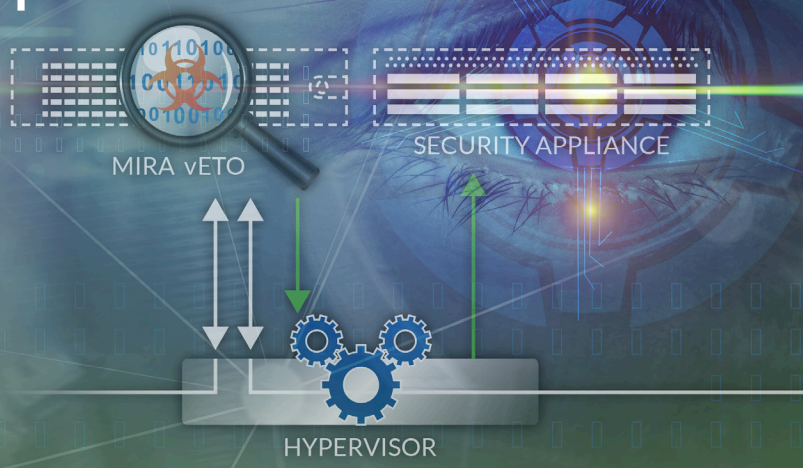
Detect. Decrypt. Deter.

Virtual Encrypted Traffic Orchestration

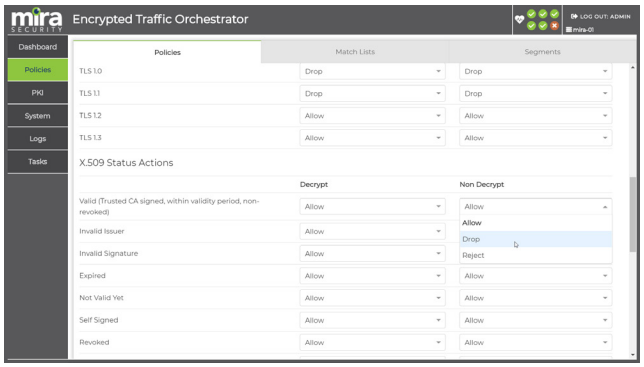


Encrypted traffic has become ubiquitous in networks today, delivering privacy and protecting users' data. However, encrypting data also creates a new set of security issues for enterprises, as existing security mechanisms are "blind" to any threats carried by encrypted connections. The Mira ETO software enables an enterprise to remove this "blind spot" by providing visibility into the unencrypted connection for the full range of security and analytic tools being used. Mira ETO software runs on physical appliances (ETO) and as a virtual appliance (vETO) on KVM or ESXi.

Encryption Orchestration without Compromise

Mira Virtual Encrypted Traffic Orchestration (vETO) software provides safe and secure visibility into encrypted traffic allowing the tools used by enterprise security teams to function effectively, even when all the important traffic is encrypted. Enabling the enterprise security stack to detect and mitigate threats while providing features to enable privacy and ensure compliance requirements can be met is central to Mira vETO software.

- Automatically detect all SSL/TLS and SSH traffic in the network, no matter what ports are being used
- Capable of decrypting SSL v3, TLS 1.0, 1.1, 1.2 and 1.3, as well as SSHv2
- Transparent to the higher-level protocols being carried on top of the encrypted layer providing decrypted flows to security tools for any existing or future protocols
- Seamless integration with existing security tools protects existing security investments
- Policy control over which encrypted traffic is made visible allows compliance with industry requirements and enterprise policies on data privacy
- Policy control over which encryption mechanisms are allowed in the enterprise network to prevent weak or obsolete methods from being used
- Comprehensive logging enables the enterprise to analyze encrypted traffic within the network and derive actionable changes to operational policy
- Scaling from 500Mbps for branch offices and micro edge locations to 5Gbps of decrypt allows for growth and supports the increasing use of virtual tools within the Enterprise and in private cloud environments.



Configure whether to allow or deny traffic based on the SSL/TLS version or certificate status.

MiraSecurity.com

mira SECURITY

info@mirasecurity.com

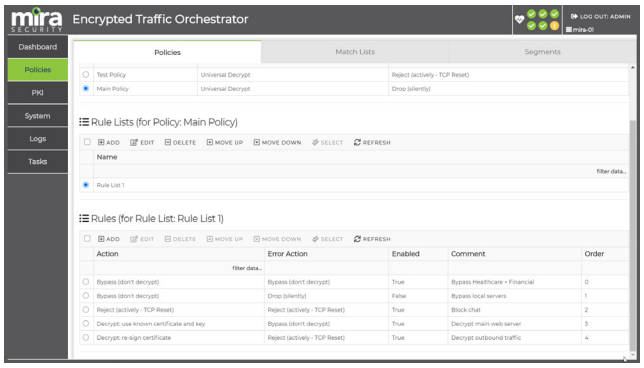
Encrypted traffic has become ubiquitous in networks today, delivering privacy and protecting users' data. However, encrypting data also creates a new set of security issues for enterprises, as existing security mechanisms are "blind" to any threats carried by encrypted connections. The Mira vETO software enables an enterprise to remove this "blind spot" by providing visibility into the unencrypted connection for the full range of security and analytic tools being used.

Mira vETO automatically detects SSL, TLS and SSH traffic and can decrypt this traffic in order to send the unencrypted data to one or more security tools. Port numbers are not used during detection of encrypted traffic, so all traffic will be discovered irrespective of the port number being used. Decrypted data is sent to security tools with the same packet header details as the original encrypted flow. Optionally, the decrypted flow can be marked allowing the tool to determine that the flow was originally encrypted.

Flexible policy control features of Mira vETO allow enterprises to enforce policy on what encryption mechanisms are allowed in order to ensure a secure environment. For example, policy can be used to prevent any traffic from using obsolete encryption versions such as SSLv3 or TLS 1.0 and TLS 1.1. For encrypted traffic that is allowed, there are fine-grained policies that allow control over which encrypted flows are decrypted and made visible to security tools. Policy controls can optionally make use of the Mira category database and/or a locally created category database to determine which types of traffic are decrypted. Enterprises need to balance security risks of not decrypting traffic with the privacy implications of doing so, and Mira ETO provides the flexible policy controls to ensure that balance is achieved.

Enterprises are increasingly adopting virtual tools both within the datacenter and in private cloud environments. This means that scalable virtual solutions to provide visibility into traffic are required. Mira vETO software is designed for high-performance decryption and can work in either KVM or ESXi environments, providing decryption for anywhere from 500Mbps up to 5 Gbps of encrypted traffic. Mira vETO software provides the same features, functionality and management interface in the virtual appliance as are provided by the Mira physical appliances.

Mira vETO software decrypts traffic and feeds it to one or more physical or virtual security tools that actually detect and mitigate any threats that may be present. No special interfaces or software changes are required



Configure whether and how to decrypt traffic using match/action rules.

to the security tools; they simply receive traffic from Mira vETO as if it was traffic directly from the network. This means the existing security stacks can regain their effectiveness, diminished by the increase in encrypted traffic, simply by deploying Mira vETO to feed them.

Multiple decryption mechanisms are supported by Mira vETO software and the system allows for the appropriate mechanism to be used on a per-flow basis. The three primary mechanisms are:

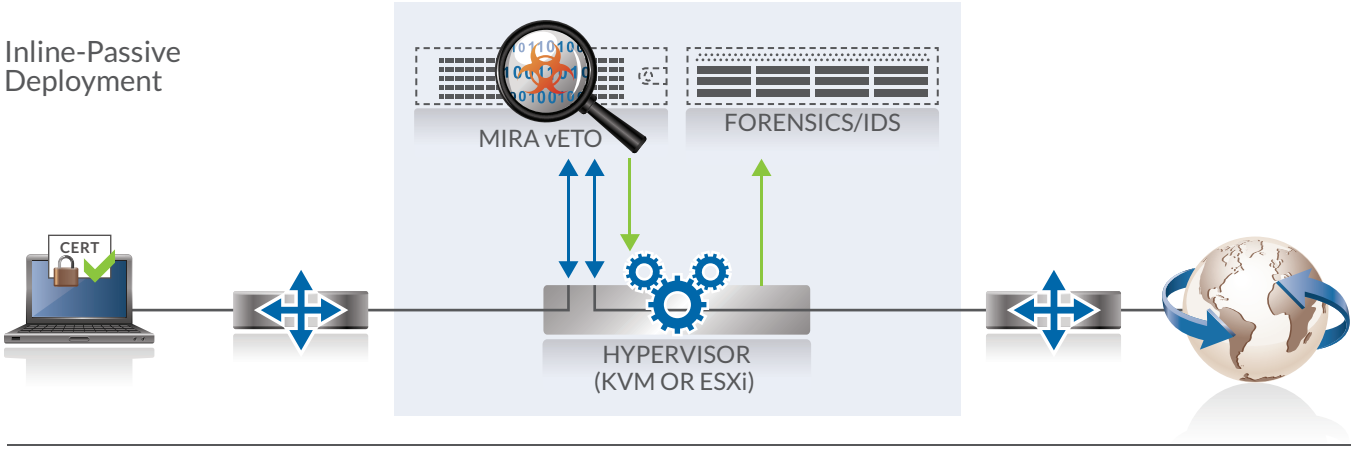
- Known server key mode. This can be used for TLS and SSH traffic and requires that the server private key is available to the Mira vETO software. This is used by enterprises to inspect encrypted traffic to servers under their control.
- Certificate re-sign mode. This can be used for TLS traffic and relies on the Mira vETO software acting as a Certificate Authority that enterprise clients trust.
- Self-signed mode. This can be used for TLS traffic to servers that have a self-signed certificate.

Depending on the decryption mechanisms being used, the Mira vETO software needs to be located either in-line as a "bump in the wire" or attached to a network tap, so that it receives copies of packets. Deployments where Mira vETO is attached to a network tap can only be used to provide visibility into traffic when known server key mode is being used and when the TLS handshake is using RSA key exchange. TLS 1.3 does not support the use of RSA key exchange, so this mode cannot be used for TLS 1.3 traffic. This passive-passive deployment is used by a limited number of enterprises. The majority of deployments rely on in-line deployment modes that allow for all decryption mechanisms to be used and TLS 1.3 traffic to be handled.

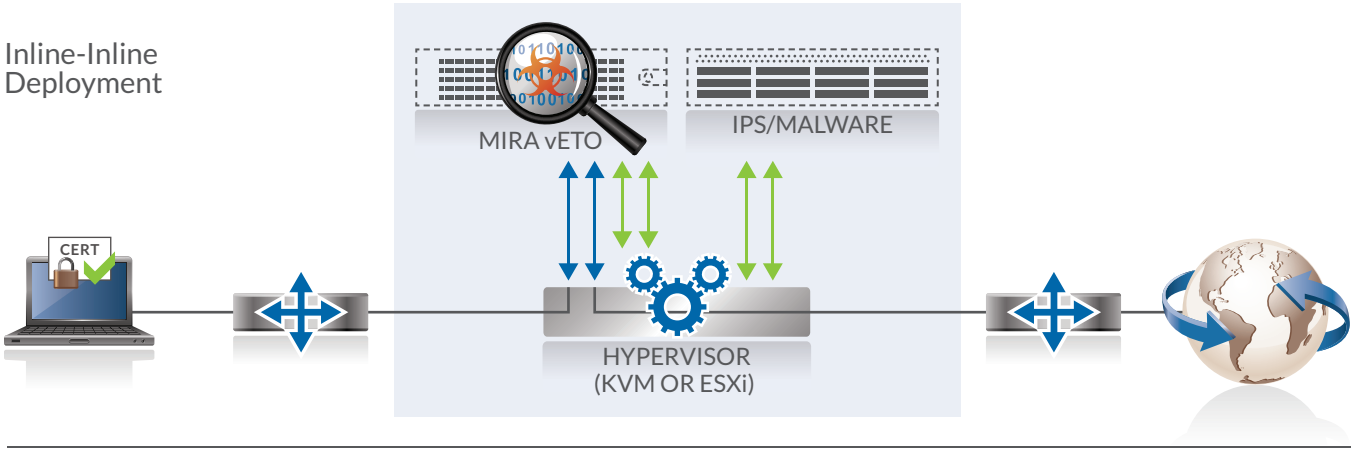
The Mira vETO software operates transparently at Layer 2, so there is no requirement to assign IP addresses to interfaces and no need to re-engineer the

Typical Deployment Topologies

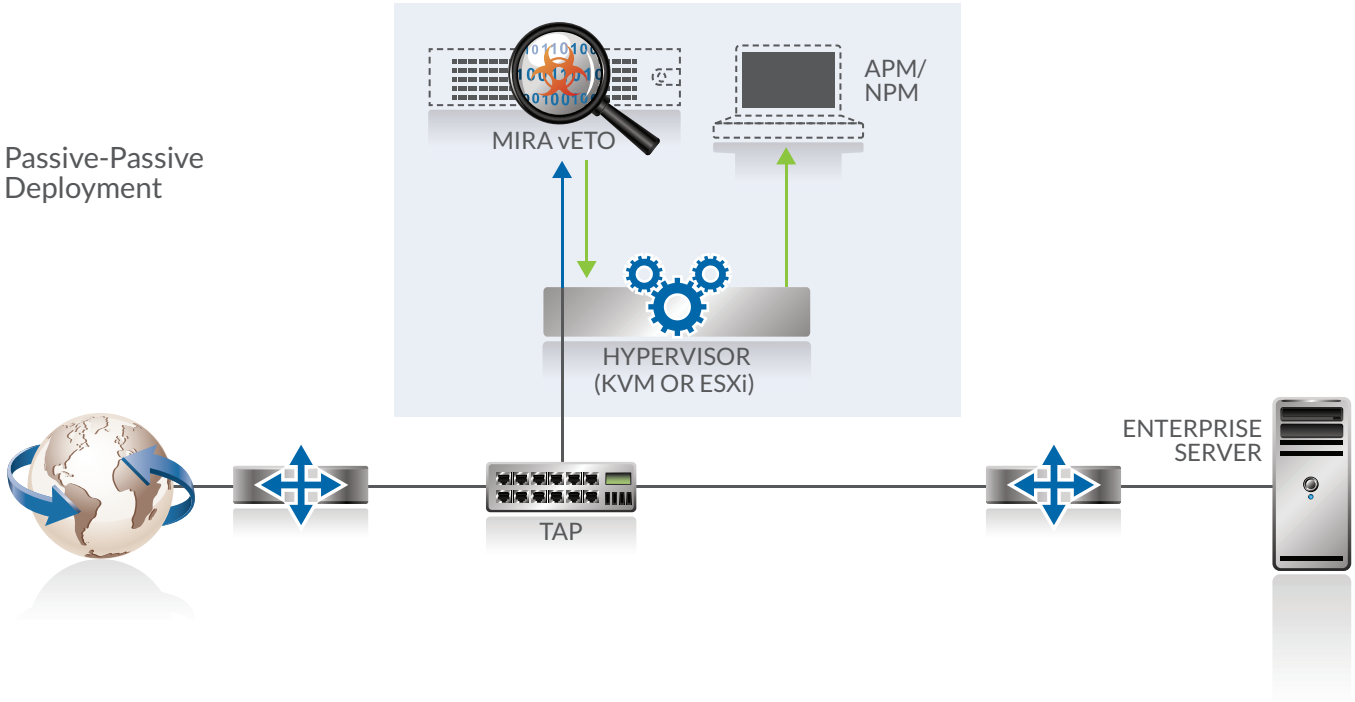
Inline-Passive Deployment



Inline-Inline Deployment



Passive-Passive Deployment



enterprise network addressing. Decrypted traffic sent to attached security tools retains the original packet header information, allowing these to be used as part of the threat detection and mitigation mechanisms used by the tool. Encrypted traffic within tunnels, such as GRE or VXLAN, can be detected and decrypted without requiring the tunnel to be terminated and re-originated.

Mira vETO software is managed by a web user interface and implements role-based access controls (RBAC), allowing enterprises to ensure that network and security team staff have appropriate access. A REST API is supported, allowing programmatic access to all of the features that are accessible via the web UI. Details of encrypted sessions are captured in a session log capable of holding 5M entries. Session log details can be sent to remote syslog servers, allowing analysis and monitoring using existing enterprise tools, such as Splunk. Mira vETO can be used to prevent the use of QUIC, thus forcing the use of TLS.

Software Subscription License

Mira vETO software is licensed as a subscription model for either KVM or ESXi. Subscriptions can be for 12 months or 36 months and can be upgraded during the subscription period. The license purchased determines the amount of encrypted traffic that can be decrypted to provide visibility for security tools.

The Mira vETO software will run on KVM or ESXi systems using Intel Haswell or equivalent CPU(s).

Performance numbers shown here are measured on a system using Intel® Xeon® Gold 6248 CPUs. Performance is likely to be lower on systems with older CPUs.

CPU core numbers are for real cores – no hyperthreading being used.

Minimum CPU cores shows the requirement to be able to decrypt sufficient traffic to meet the licensed capacity and the new TLS sessions per second this number of cores can support. Numbers are measured in a reference system with Intel® Xeon® Gold 6248 CPUs.

vETO Software Subscription Options

vETO	ETO-DL-0.5	ETO-DL-1	ETO-DL-2.5	ETO-DL-5
Licensed Decrypt Gb/s	0.5	1.0	2.5	5.0
Min CPU Cores/Memory	8/16GB	8/16GB	10/24GB	12/32GB
TLS Sessions/s RSA 2048	750	750	2,200	3,000
TLS Sessions/s EC256	1,400	1,400	3,800	5,800
Max TLS sessions	100,000	100,000	300,000	400,000
Boosted CPU Cores/ Memory	10/24GB	10/24GB	12/32GB	14/40GB
TLS Sessions/s RSA 2048	2,000	2,000	3,000	4,500
TLS Sessions/s EC256	2,000	2,000	5,000	8,800
Max TLS sessions	300,000	300,000	400,000	650,000

Max session log entries for all vETO models is 5 million entries.

Boosted CPU cores shows the increase in new TLS sessions per second provided by use of additional cores in the reference system. Note that adding cores will not increase the decrypt capacity or the sessions per second capacity beyond what is determined by the license.

MiraSecurity.com

info@mirasecurity.com

Mira Security
3159 Unionville Road, Suite 100
Cranberry Township, PA 16066
Phone: +1 (412) 533-7830

Email: info@mirasecurity.com
mirasecurity.com

MIRA-vETO-V1-2/22