xerobank

ONYX NETWORK

XeroBank develops and operates covert communication solutions that provide protection of client information across multiple levels. Onyx is a decentralized and distributed anonymity network operated by multiple legal entities, using state of the art traffic obfuscation techniques. All critical operations have been segmented, so no single entity can be coerced to compromise security by global adversaries such as foreign governments and intelligence agencies. Our enterprise offerings are designed to address threats related to content, context, and trust.

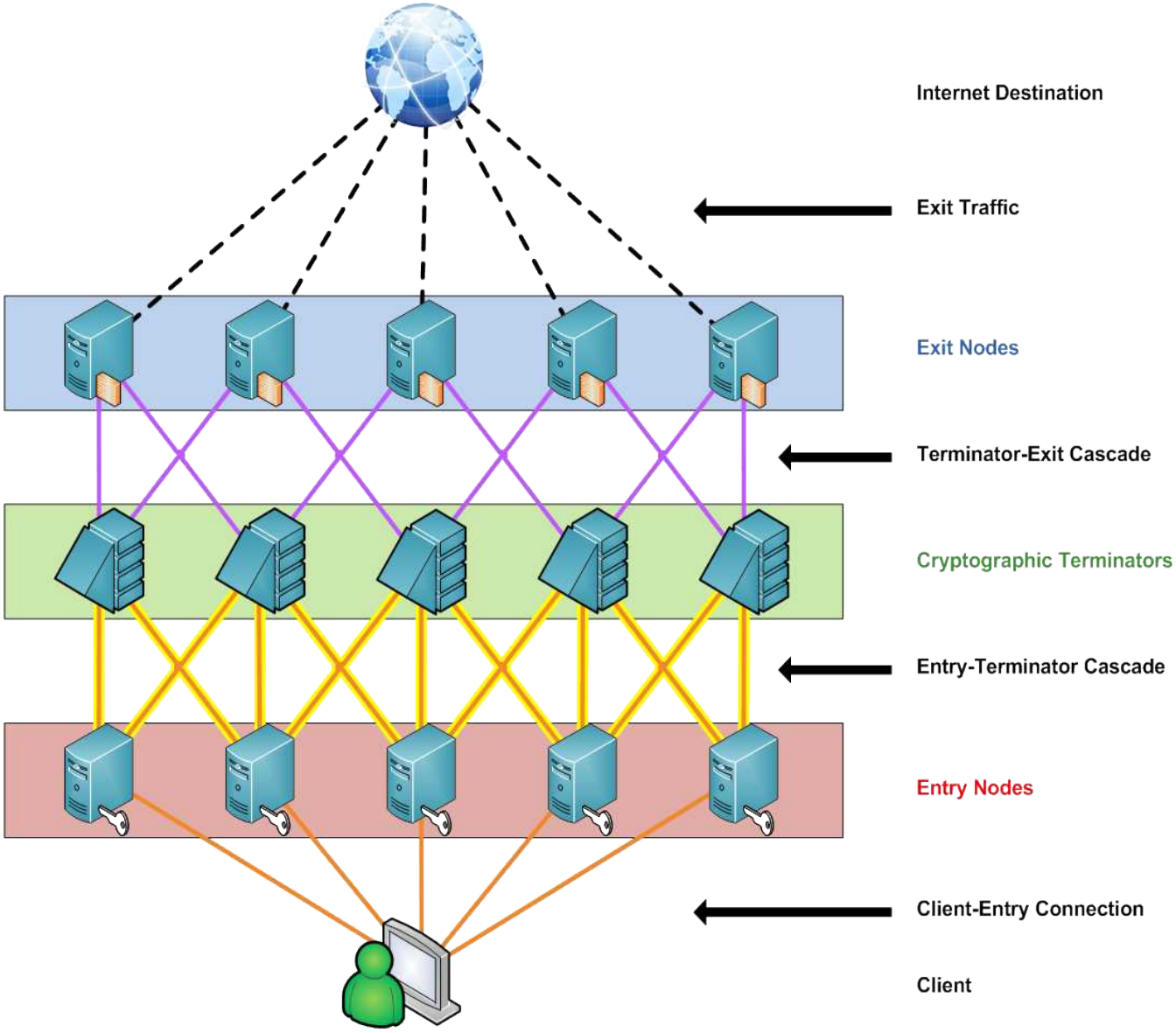
> **Content** is the "what" of a transmission and is the primary concern regarding communication privacy. To maintain privacy, the content must be kept from being intercepted and read by unintended parties.
>
> **Context** is the "who, where, why, when, and how," which are relevant to anonymity. To maintain anonymity, the context must be obscured from attackers. This information, while not immediately as valuable as content, can be of almost equal value in many circumstances because it is the silhouette of the content. If adversaries know who you are communicating with, the frequency, message size, and other incidental pieces of information, they can develop an idea of the content and anticipate future behavior.
>
> **Trust** involves the intent of your privacy service as well as their capability. Although there is a history of services operated by untrustworthy parties, the majority simply store their information poorly or expose client data via leakage, theft, or misuse. This is because the tactical, technical, and legal expertise required is beyond their capability. When trust is commensurate with the intent but not the capability of a privacy service, it is only a question of time before client data or communications are compromised.

ONYX NETWORK STRUCTURE

Onyx is designed to protect clients from breaches of both content and context. The operational, corporate, and network structures are designed so that clients do not have to depend upon XeroBank itself. No third party can gain any knowledge about the content or context of your communications, not even XeroBank. The various parts of our network are isolated from each other and are operated by multiple companies in different jurisdictions; none of the operators can collect the required data to learn about your communication's content and context.

XeroBank technology provides multi-jurisdictional routing of communication to make sure that traffic does not enter and exit our network through the same country. This technology makes it exceedingly difficult for adversaries to trace client connections.

Additionally, our technology allows for the creation of closed groups to communicate with each other in a very secure, end-to-end encrypted, globally-distributed network without interference from, or leakage to, any third parties, including XeroBank itself.



SIMPLIFIED ONYX ROUTING EXPLANATION

Nodes are individual computers or devices connected to a network. Cascades are relays that chain nodes together in a fixed sequence. Relays are specialized routers that not only transfer data but also change the protocol data like IP addresses of the communication. The above diagram depicts a client to internet connection, as opposed to closed-group routing, which is a client to client connection. Onyx first creates an encrypted connection, through the entry node, to the cryptographic terminator node. An encrypted cascade from the entry node to the terminator node is created to obscure the client IP address from the Terminator and third-party observers. The cryptographic terminator then decrypts the

Entry-Terminator Cascade encryption, and the Client to Terminator encryption. It then recrypts the communication stream to an Onyx exit node, eliminating cryptographic fingerprinting and data watermarking evidence. Exit nodes then decrypt the data, and send it on to the destination address and pass the returning data, such as a website, back to the client in reverse of this process. This explanation is extremely oversimplified, and does not take Onyx anonymization and IP correlation-resistance techniques into account. These techniques are detailed below.

ONYX KEY TECHNOLOGIES

XeroBank Onyx supports both OpenVPN and IPSec access with the following operational security properties:

Content

- Standards-based military cryptography using AES-256, RSA-2048, DH-2048, SHA1 / SHA256 protocols.

Context

- Multi-Jurisdictional routing
- Mixing of incoming packets at entry node
- Traffic Padding / Chaff
- Connections are relayed and re-encrypted against watermark attacks
- Temporary internal IP space
- Authenticator is IP address agnostic
- Authenticator does not know login / logout times
- Random assignment of outgoing IP, only fixed per destination and session
- Full integrity protection of network traffic between routers and nodes to combat watermarking attacks
- Traffic between entry, termination and exit nodes is encrypted to elevate the difficulty of fingerprinting attacks
- Exit and termination node selection is automated to optimizing crowding

Trust

- Different parties for 1) token issuing, 2) entry node operation, 3) termination node operation
- Temporary authentication and per-session only authentication
- Entry node does not know internal IP
- Entry node selects termination node
- Termination node does not know original IP or new outgoing IP
- Exit node does not know internal IP

CryptoRouters on Onyx

- CryptoRouters can perform closed-group end-to-end encryption with each other
- All traffic between Onyx and the CryptoRouter is encrypted
- Internal firewall does not allow rogue traffic back to CryptoRouter
- Policy routing used to perform all-or-nothing traffic protection

ANONYMIZATION METHODS

Mixing
Mixing is a technique that makes it difficult for a third party to correlate incoming and outgoing connections at a relay, by encrypting and reordering of communication. Mixing is employed on both the Entry to Termination cascades as well as inter-cascade connections. Onyx uses adaptive mix pools with a size of 100 - 200,000 packets depending on network use, with a positive correlation between data exchange and pool size. Mixing delays are kept between 10 to 1000 milliseconds.

Crowding
Crowding is used to increase the total number of user nodes that are connected to a relay. When crowding is combined with encryption, it harder for a third party to attribute an outgoing connection to an incoming connection. The result is that each connection becomes "hidden in the crowd". Onyx uses a load-based mechanism to direct an optimal number of client connections to a cascade which focuses clients on as few other cascades as possible to increase crowding factors. The minimum number of client connections to one cascade is 120 for entry nodes, and 30 connections for termination nodes. No additional methods are employed for exit node crowding optimization.

Splitting
Cascade splitting is allows CryptoRouter devices to distribute connections over two or more cascades. Cascade selection is available per protocol, port and destination address as well as by source type

Lag Obfuscation
Data takes time to travel from one node to another. Often times, this seems instantaneous, but can be measured in milliseconds. The amount of time required for the path can give away information about where the nodes are located and how they are connected to each other. Attacks used to determine contextual data based on lag time are called Timing Attacks.
To increase resistance against timing attacks, IPSec based connections have access to adaptive client-cascade artificial network delays. Delay duration is automatically calculated by constantly measuring the lag and normalizing it over all clients connected to the cascade. Onyx supports both entry and exit delays for client and cascade entries. Minimum and maximum delays are automatically adjusted per client, resulting in 0 to 800 millisecond delays.

Traffic Padding
IPSec based access methods use fractional padding to normalize packet lengths to a modulus of 256 bytes. MixPPP based access methods have all packets padded to 950 bytes per packet.

Chaff Traffic
Chaff is non-client traffic that is generated to obfuscate true client netflows. This is to mix “wheat with the chaff,” creating a requirement to try to separate traffic for analysis. Onyx supports both random and adaptive chaff traffic generation both for Client to Cascade and Cascade to Client connections. For Inter-Cascade traffic, random chaff

traffic generation is used. Chaff traffic timing precision is 50 to 500 milliseconds. All chaff is Client to Termination only. Client-Entry and Client-Exit chaff is not supported.

Compression
Client-Cascade and Termination-Exit connections use adaptive compression to optimize throughput and increase the resistance to traffic-based stream fingerprinting methods.

Channel Multiplexing
Multiplexing combines multiple connections into one new connection. Multiplexing, when used with encryption, prevents third-parties from knowing what or how many connections are established since only one is visible to them. All Onyx traffic within our network uses a single multiplexed connection, regardless of how many connections are tunneled. This multiplexing method resists connection-timing correlation techniques that are used to unmask anonymous traffic.

Integrity Protection
All Onyx traffic has integrity protection as well as access policies so that watermarked traffic will be discarded as soon as possible.

IP CORRELATION-RESISTANCE TECHNIQUES

IP Pool
All connections to Onyx are assigned in Last-In / Last-Out order from an IP Pool. IPSec based connections can change IP assignment during a session. It is a common misconception that large pools of IP addresses create anonymity. This is not the case, as this lowers per-IP crowding and makes IP addresses unique and therefore attributable.

Non-Unique IP Addressing
Entry to Termination connections do not use unique IP addresses, however all IP addresses are shared between all cascades, which resists non-live traffic analysis.

Per-Connection IP Assignment
Public IP addresses are assigned based on decaying table lookups, keyed with source and destination addresses. IP address pools for public addresses are optimized by load so that at least 10% of the port range is used by outgoing connections.

Late IP Assignment
Public IP addresses are assigned only at exit nodes, and are independent from internally assigned IP addresses.

Multi-Jurisdictional Routing
Exit node selection takes the jurisdiction of the connection destination into account. This ensures that connections do not exit the Onyx network through an exit node in the same jurisdiction unless specified per contract.

SEPARATION OF CONCERNS

An Internet Service Provider has access to all of the content and context of client communication as well as knowledge of the identity and physical location of the client. This gives a third party (the ISP) the full knowledge of who is communicating what from where to whom, including e-mail, voice over IP, web-surfing and file transfers. To limit the information a single third party can know about a communication, "Separation of Concerns" is used. By employing technological and organizational means XeroBank ensures that no one, including XeroBank, has access to all the information that constitutes Onyx communications.

Multi-Hop Connections

All client to internet connections travel at least two hops. Entry and termination nodes are not operated by the same legal entities and are not usually located in the same jurisdiction. Entry nodes only know the original IP address of the connection but do not have access to the contents or the destination information of the connection. When multi-jurisdictional routing is applied, termination nodes do not know the newly assigned public IP address.

Offshore Authentication

To authenticate and authorize connections to our network we use a token based authentication method. Tokens are issued by a party that is not operating any other parts of the network, and does not control any information directly linkable to the client identity. Each session uses a new set of tokens so that the network cannot correlate sessions. Authentication happens exclusively at the termination nodes so that no information about the original source address is known. Authenticators are operated in countries that do not host cascade nodes. Multiple mutually independent authenticators are used, and each is operated by a different legal entity.

Traceback Protection

Entry Nodes employ traceback protection methods that prevent termination nodes from measuring the distance or path to a client. Onyx uses packet sanitation, TTL fixing and exit delays for traceback protection.

OPERATIONAL LOGGING

Traffic Logging

Termination nodes generate per-session usage statistics that are sent to the authenticators after connection shutdown to enable billing. During sessions, no traffic information is sent or associated with a session.

Connection Logging

Depending on termination, exit node selection, and protocol, we may create logfiles containing internal source and external destination addresses. Clients can select cascades without any logging, except for outgoing SMTP traffic which is always logged.

SMTP Logging
In the case of SMTP connection logging, data is stored for 48 hours and destructively erased afterwards. This is done to be able to keep abuse of our networks for SPAM as low as possible.

Exit Traffic
XeroBank's default policy is to not create any temporary or permanent logs of any activity except traffic usage. Termination and exit node logging may legally required depending on the jurisdiction in which the nodes are located. In these cases, we log the internal source address, external source address, external destination address, ports, protocol and time of connect and disconnect. This logging data is encrypted on-the-fly and stored in a translucent database. Closed-group network communication is never logged.

All lookups to the database require previous knowledge about the ports, protocols and times used as well as external source address and external destination address in order to access results in the database. This ensures that a legal agency must have a specific communication requested in their warrant, and that no “fishing expeditions” are possible. Additionally, requests cannot be performed without the consent of both the node operator and the network management center, because our log database requires cryptographic authorization.

Access to logged data requires a court order to both the node operator and the network management center. The data revealed only covers a single outgoing connection and only points to the internal IP address, not to the client identity or entry node used. Entry nodes are not permitted to do any logging. No logging is permitted in locations where terminator and exit nodes are not legally forced to do logging.

Logged data is stored for 7 days to 6 months, depending on node jurisdiction. Access keys to this data automatically expire, and data is automatically and destructively erased after expiry. Clients are notified when their communications are traveling through nodes that log connection data, and are given the opportunity to switch to cascades that are not forced to log.

Session logging
XeroBank's default policy is to not create any temporary or permanent logs of any activity except traffic usage. The authenticator gains knowledge about the times a session starts and ends depending on access method used. Closed-group network communication is never logged.

Session information is inaccessible to the authenticator when token-based authentication is employed. All CryptoRouters use token-based authentication by default. The authenticator only receives a daily report on total traffic used by each token so that billing can take place.

Termination nodes temporarily store both internal IP addresses and tokens of a session if the node is located in a jurisdiction where logging is required by law. This data is kept encrypted and can only be accessed with previous knowledge of the internal IP address and cryptographic authorization by both node operator and network management. Clients

are notified when their communications are traveling through nodes that log connection data, and are given the opportunity to switch to cascades that are not forced to log.

OPERATIONAL SECURITY

Client Database

Client databases are only operated by authenticator operators and not by network operators. They are required by contract to be located outside of any jurisdiction involved in network operations and need to operate on encrypted media.

Jurisdictional Leverage

Entities that could correlate content and at least one direction of the context are not allowed to be located or operated from the same jurisdiction. All jurisdictions are selected based on the data secrecy and privacy laws applicable. Cascades are configured so that insufficient data is collected for correlation.

No Cross-Ownership

Cross-ownership is denied between legal entities involved in network operations, client relations and authenticator services. Only mutual service contracts exist between the entities. Critical positions in administration and management may not be shared by the same person. This decentralization and distribution of information ensures data integrity against collusion and coercion of involved parties.

Anonymous Audit

Critical operations that could affect the security or privacy of clients require cryptographic authorization by a randomly selected, anonymous auditor.

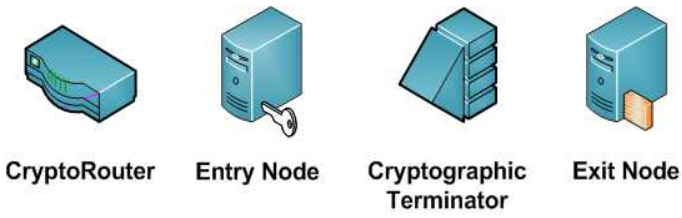
Node Security

All network nodes use up-to-date software, storage and swap encryption, exploit protection systems and integrity verification methods. Onyx nodes only allow encrypted access, requiring multi-level authentication. There are no shared account passwords or keys, and they employ single-task ephemeral keys to encrypt storage of key material and usage data.

CRYPTOROUTERS

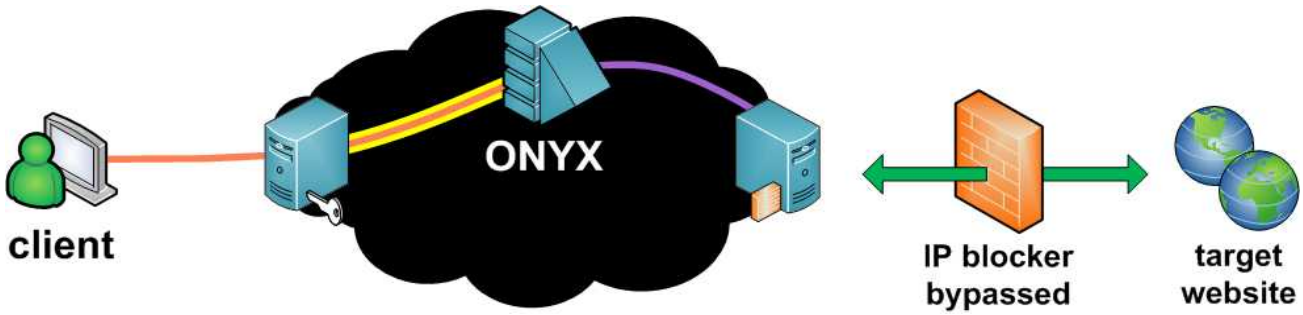
XeroBank's primary hardware access device to Onyx is the CryptoRouter, which can replace or stand alongside other routers. CryptoRouters effectively extend the closed Onyx network onto the client's premises, and all computers connected to the router are directly protected. Several levels of service are available (high-bandwidth, high-volume, etc.), but all share essentially the same suite of protection technologies. Closed-group routing is restricted to government clients, and vetted corporate clients.

NETWORK LEGEND

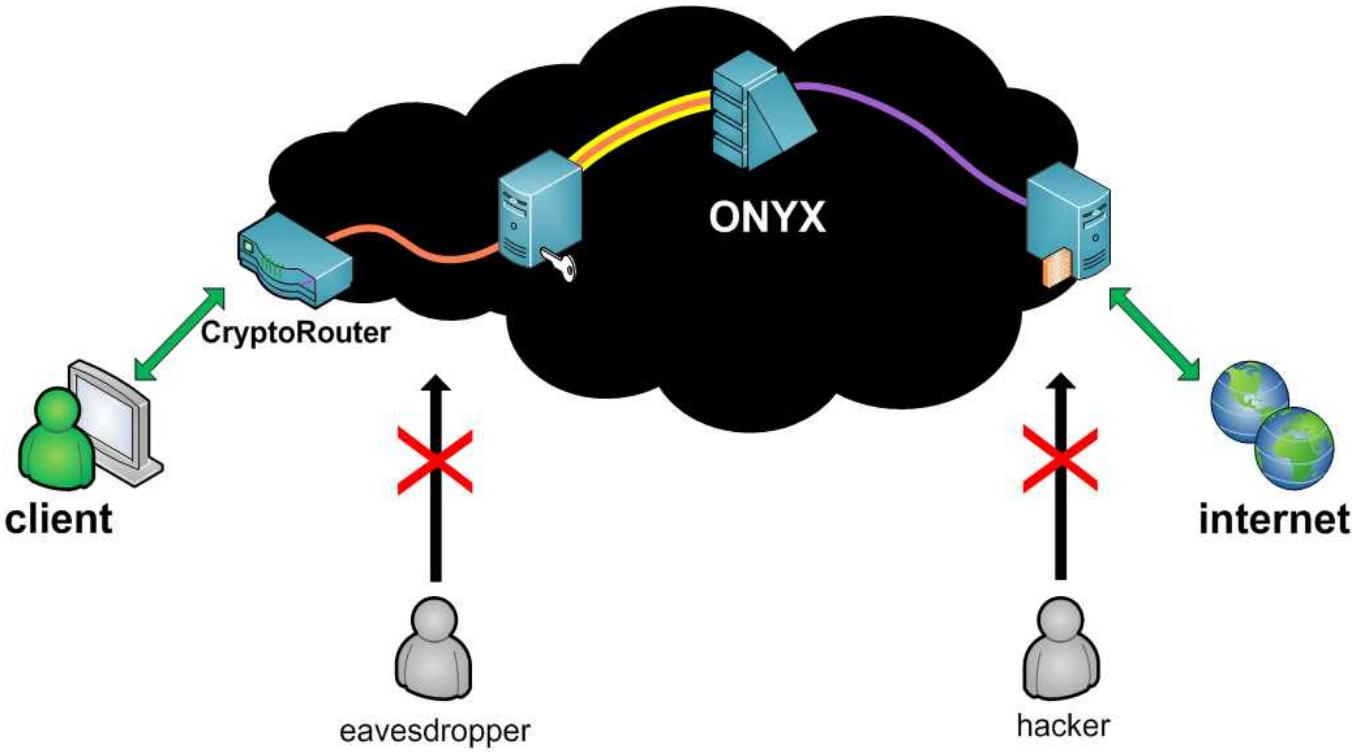


NOTE: Connection colors in Onyx represent encrypted communication tunnels

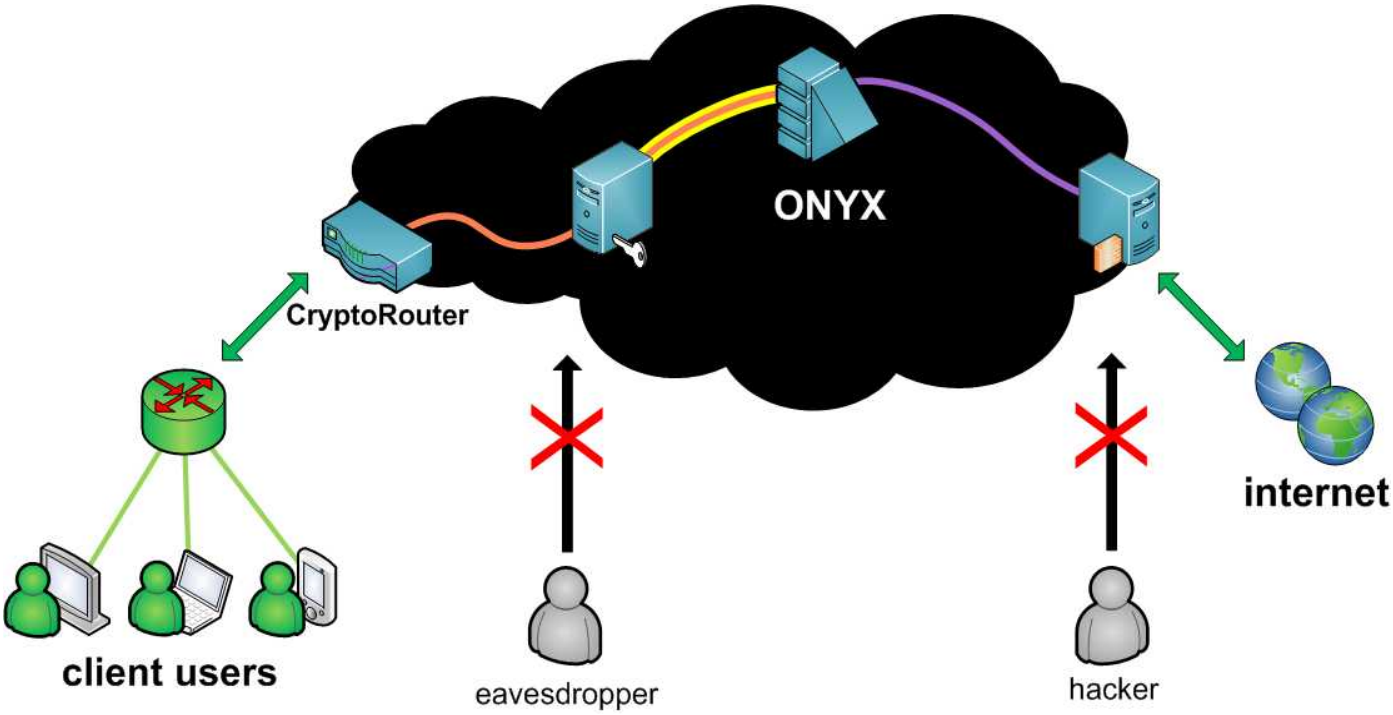
COMPETITIVE INTELLIGENCE IMPLEMENTATION



SMALL OFFICE IMPLEMENTATION



ENTERPRISE IMPLEMENTATION



CLOSED-GROUP IMPLEMENTATION