Technolution
Prime

Cross-domain solutions

Secure communication between classified domains

Redefining **solutions**

“Protection of classified information is of vital importance - but so is sharing it! **Our Information Exchange Gateways provide secure interoperability and fit seamlessly into your existing IT infrastructure**.”

Jonathan Hofman
Business Unit Director High Assurance

Technolution
Prime

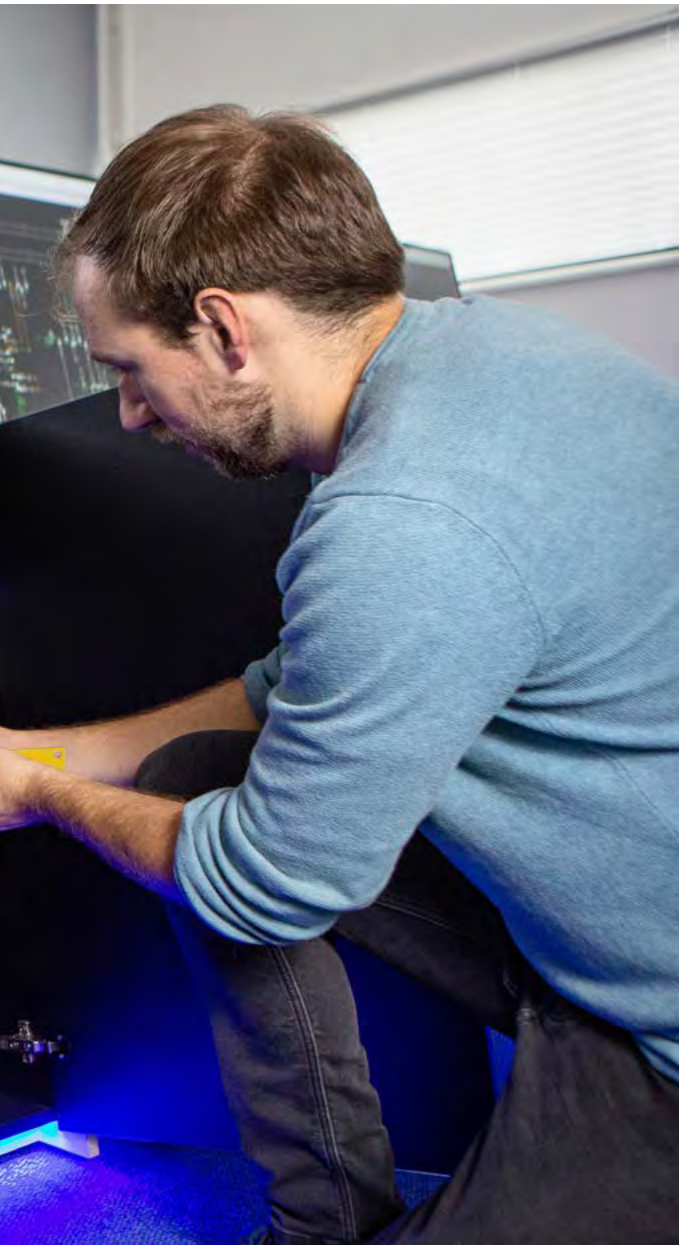
Contents

Cross-domain security

Whenever connections are established between classified network domains, the information and systems in those domains must be properly secured. Installing an Information Exchange Gateway between the network domains creates an effective, secure cross-domain connection.

An Information Exchange Gateway for communication and security

An Information Exchange Gateway (IEG) facilitates the data exchange that you need between the two network domains, while respecting the condition that the IEG should offer the required security for the classified data or systems within those domains. Data exchange and security must be seamlessly fine-tuned to each other.



Building blocks for IEGs

An IEG consists of several building blocks. At its core stands a device that guards the domain crossing. This can be a data diode, which permits data traffic in one direction but blocks it in the other direction, or a data filter, which filters data before it passes through the connection. The central device is supported by proxies on both sides of the domain crossing.

Preparation and implementation

The implementation of an IEG requires careful preparation. This is to prevent the data exchange between the domains from compromising the security of the classified information and systems. At the same time, the continuity of the applications must not be jeopardized.

Insight into IEGs

This brochure offers you an overview of the way cross-domain IEGs function and of how they are built. It provides insight into the various building blocks that together make up an IEG. In addition, it gives practical examples of IEGs and specific solutions for data exchange and security. Finally, it sets out the most important focus areas when preparing and implementing IEGs.

Building blocks for **Cross-domain IEGs**

A cross-domain Information Exchange Gateway (IEG) consists of various building blocks. The core of each IEG is a cross-domain device: a certified device with a hard security function, such as a data diode or a data filter. The IEG is supported by proxies.

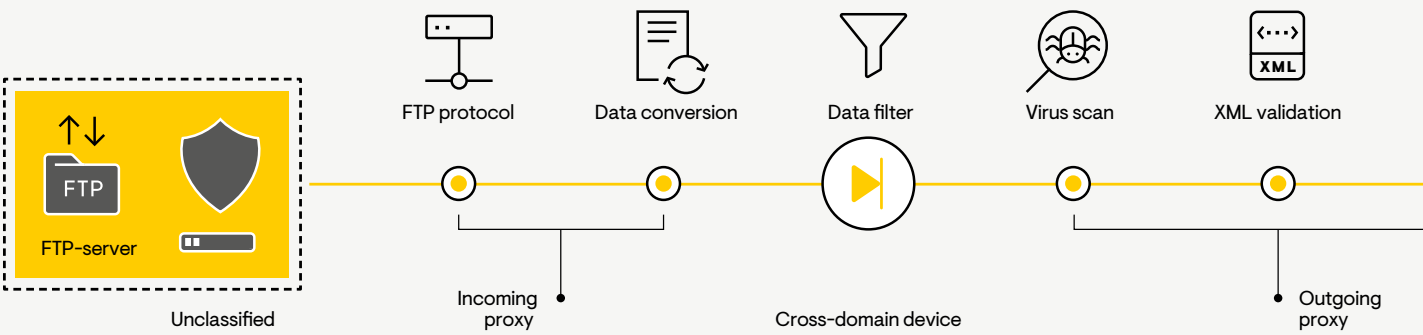
Cross-domain devices
A *data diode* is used whenever confidential data must not leave a domain, or if the integrity of a system must be protected against possible attacks from outside. A data diode only permits the passage of data across the IEG in one direction; the other direction is physically blocked.

A *data filter* filters and processes data before it passes the IEG. For example, it can remove classified information from the data. Filtering happens on the basis of specific (customized) filter proxies.

Supporting proxies
Cross-domain devices restrict data traffic between network domains, or even block it completely in one direction. Many communication protocols and applications cannot function with an IEG if no further measures are taken. For this reason, the cross-domain devices on either side of the IEG are supported by proxies in the form of *protocol handlers*. Protocol handlers facilitate the proper functioning of communication protocols. Data handlers provide additional functionality, such as virus scan and data conversion. These handlers are implemented in software on a proxy server.

An Information Exchange Gateway consists of a chain of a cross-domain device and handlers.

Cross-domain chain



Technolution
Prime

Technolution Prime's **Cross-domain devices**

Technolution's cross-domain devices are developed, tested, and assembled in the Netherlands by Technolution, and are certified by the National Communications Security Agency NBV, also know as "Unit Weerbaarheid" (Resilience Unit).

PRIMEDIODE 5001/5010

Data diode for classifications up to TOP SECRET (Stg. ZEER GEHEIM)

- Bandwidth of 1 Gbit/sec (PrimeDiode 5001) or 10 Gbit/sec (PrimeDiode 5010)
- Space-saving, compact housing – up to 12 diodes in one 2U rack
- Space-saving thanks to the PrimeProxy Micro for specific, simple protocols (e.g. TCP, NTP or HTTP)

PRIMEDIODE 3010

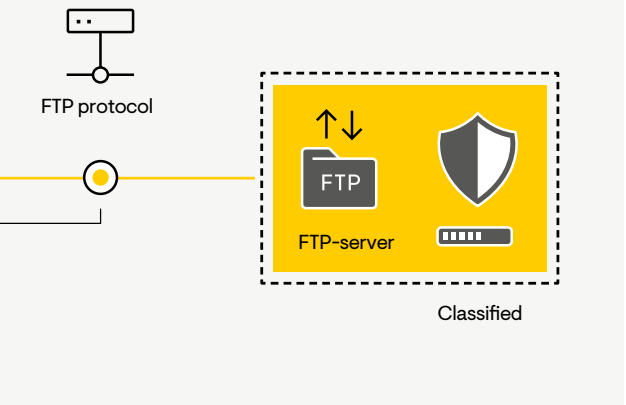
Data diode for classifications up to SECRET (Stg. GEHEIM)

- Bandwidth of 1 or 10 Gbit/sec
- Automatic bandwidth selection
- Built-in redundant power supply

PRIMECROSS

Hardware data filter with configurable filter polices

- Blocks transmission of specific data, or changes data before transmission in accordance with customized filter policies
- Filter policies work with automatic message validation, pattern matching, XML validation, conversion, etc.
- Develop and load filter policies for multiple message types



The PrimeDocks platform

Use the PrimeDocks platform to develop and configure proxy software for complete and functional IEGs between your network domains.

Multifunctional chains
Use PrimeDocks to configure multi-functional chains of protocol handlers and data handlers. You can even configure multiple parallel chains for the same IEG. This makes complex connections possible, for example an IEG that imports data from multiple domains using one configuration consisting of multiple diodes.

Standardized and customized
A number of standard handlers is immediately available, including email, FTP, SNTP, and virus scanners. Simply develop handlers yourself using the Software Development Kit which is included. This allows you to keep a grip on the data in your domain. Do you need specific or more complex handlers? We are happy to develop customized handlers for your cross-domain IEGs.

PrimeManage
Use PrimeManage to manage and maintain the configurations of your cross-domain IEGs. Its user-friendly graphical interface allows you to configure multiple cross-domain devices and their accompanying proxies. In addition, PrimeManage offers functionalities for the configuration and management of handlers in a chain.

PRIMEDOCKS

Platform for the configuration of multifunctional chains of protocol handlers and datahandlers.

- For PrimeProxy 19'', PrimeProxy VM, PrimeProxy Flex and PrimeProxy Integrated
- Handlers: standard, customized or developed with SDK
- GUI for drag-and-drop configuration
- Minimal Linux platform, no OS maintenance required

Technolution
Prime

PrimeDocks Overview

HANDLERS FROM THE LIBRARY

Protocol handlers

Support for communication protocols such as HTTP, FTP, or email

Data handlers

Additional functionality for data transport, such as virus scan, conversion, or validation

SDK

Development of customized protocol handlers, data handlers

TYPES OF PROXIES

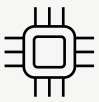
PrimeProxy 19"

Server for the installation and execution of (chains of) proxies

PrimeProxy Flex

Compact version of the PrimeDocks server, for the PrimeFlex rack of the PrimeDiode 5001

PrimeProxy Integrated



PrimeProxy integrated into e.g.
the PrimeCross FS60 and PrimeCross FV40

PrimeProxy VM

Proxies implemented in a virtualized environment – no special hardware required

DEPLOY VIA PRIMEMANAGE

Chain configuration

Configure chains of handlers and filter policies

Parameters

Configure the handlers

Filter definitions

Filter policies (library and customized) for PrimeCross

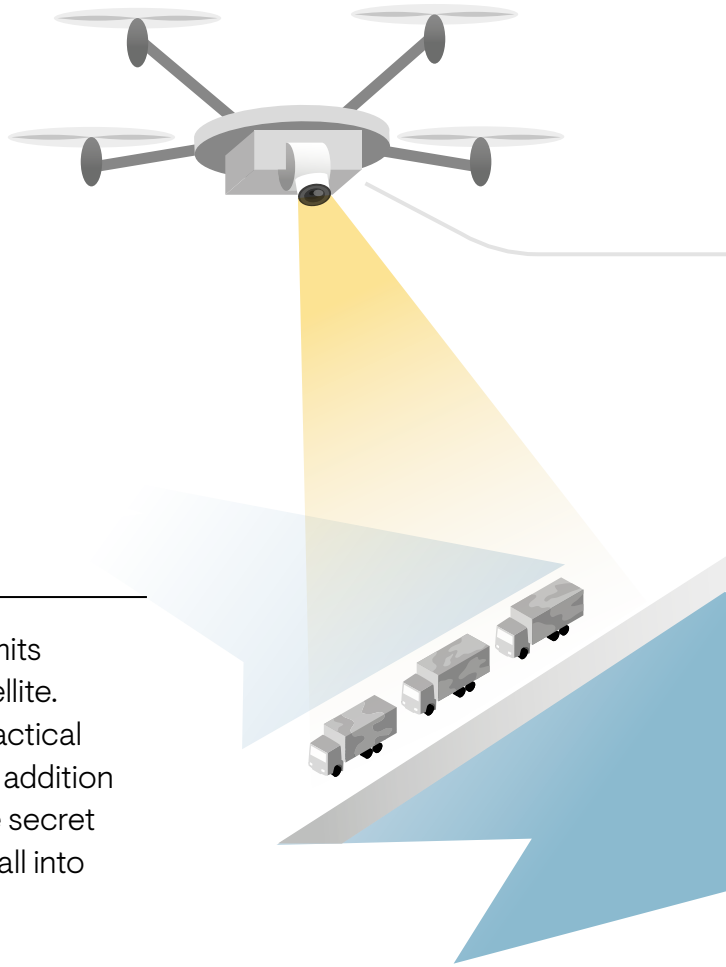
Technolution
Prime

Cross-domain IEGs in practice

The following pages showcase examples of Information Exchange Gateways (IEGs). The examples and the solutions selected are all very different, but they have one thing in common: they require access to an interest, asset, or classified information that needs to be protected, to be limited or blocked. The configuration and implementation of IEGs requires a thorough approach. We are here to help you plan and design an effective Cross-domain solution.

CASE 1

Drone **observation**



SITUATION

A military drone observes an enemy location and transmits the images to a command post on the ground via a satellite. The images are analyzed in the command post. These tactical analyses are stored on the command post's network, in addition to other sensitive information. This information is a state secret (NLD SECRET) and must not under any circumstances fall into unauthorized hands.

SECURITY RISK

The video images of the enemy location are streamed to the command center by the drone using a satellite connection. The connection between the satellite and the command post is bidirectional and has a high bandwidth. There is a risk that the connection will be used to gain access to the command center. The classified information can then be disclosed.

There is also a risk that the drone will be hacked or that a hostile party takes control of the device. This is an acceptable risk because the images are not classified and the observed situation is already known to the enemy.

PHYSICAL CONTEXT

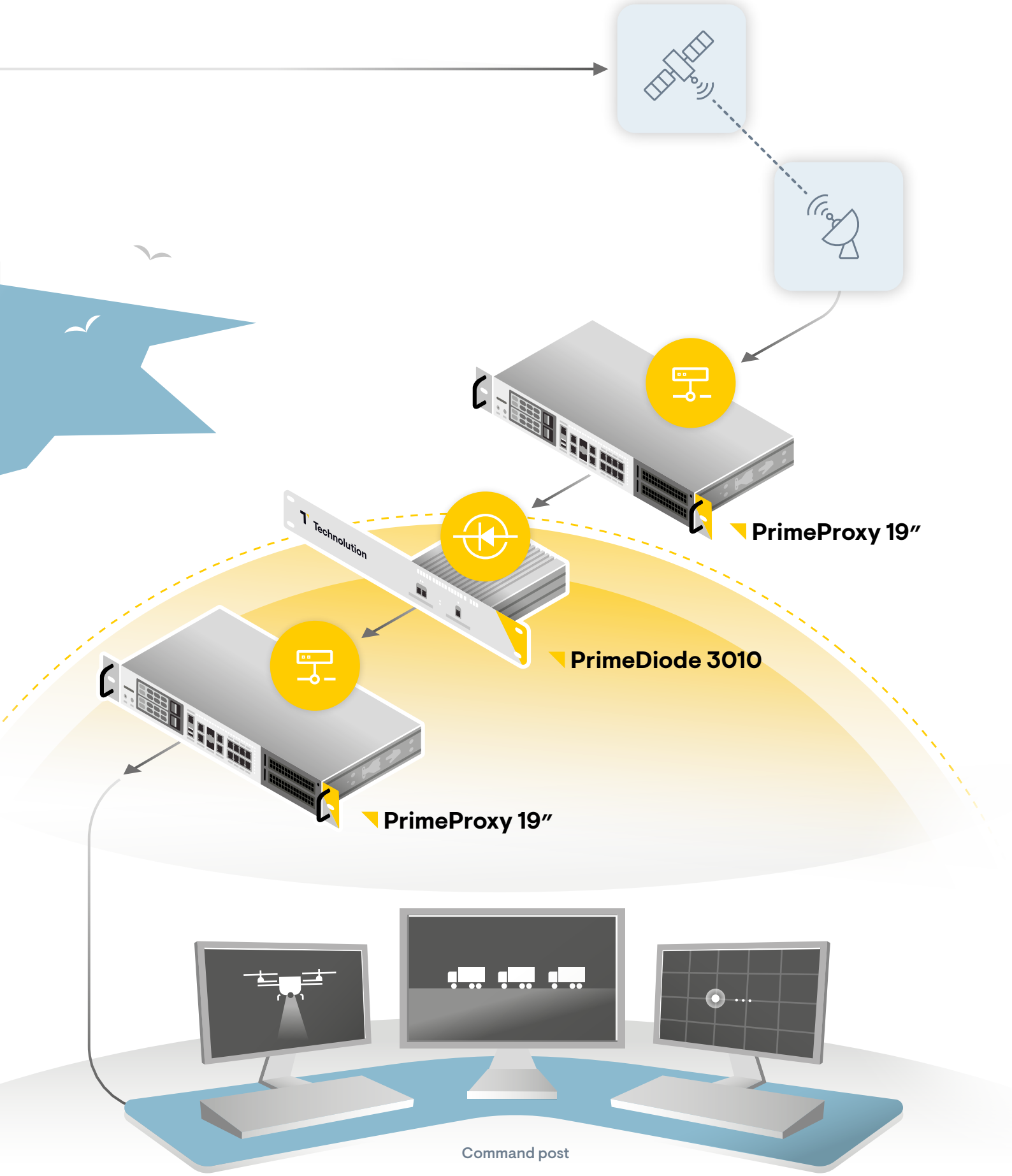
The command post is heavily guarded. Only authorized persons have access. There is enough physical space to install security equipment.

INFORMATION EXCHANGE GATEWAY

A PrimeDiode 3010 is placed in the command post. It will still be possible to receive the video signal from the satellite across the IEG, but transmission of data from the command post to outside the command post across this connection will be entirely blocked.

A PrimeProxy 19'' will be installed on each side of the data diode. The servers will be equipped with PrimeDocks software that enables the reception of the video stream.

All physical devices (3U rack space in total) will be located in the command post.


PrimeProxy 19″
PrimeDiode 3010
PrimeProxy 19″
Command post

CASE 2

Critical infrastructure Flood barrier

SITUATION

A flood barrier is operated from an on-site control room. Log files of the flood barrier, including operating data and other statistics, are being shared with a commercial service provider for maintenance purposes. To facilitate this, a permanent connection has been created between the control room and the service provider. Opening or closing the flood barrier at the wrong moment can have catastrophic consequences.

SECURITY RISK

The integrity of the flood barrier control room is literally a matter of life and death. If malicious parties succeeded in taking over control, this can result in life-threatening situation, such as inundations.

The flood barrier's log files are sent to the commercial service provider by an FTP application. The FTP protocol needs a two-way data connection. There is a risk that malicious parties could use the FTP connection to gain access to the controls of the flood barrier. If they succeed in doing this, they could be in a position to open or close the flood barriers.

The government body that is responsible for the installation requires that the integrity of the flood barrier controls be guaranteed. This applies both to physical and to online access to the controls.

PHYSICAL CONTEXT

Physical access to the control room of the flood barrier is secure: only staff with electronic access cards can enter. The control room has enough space for the installation of security equipment.

INFORMATION EXCHANGE GATEWAY

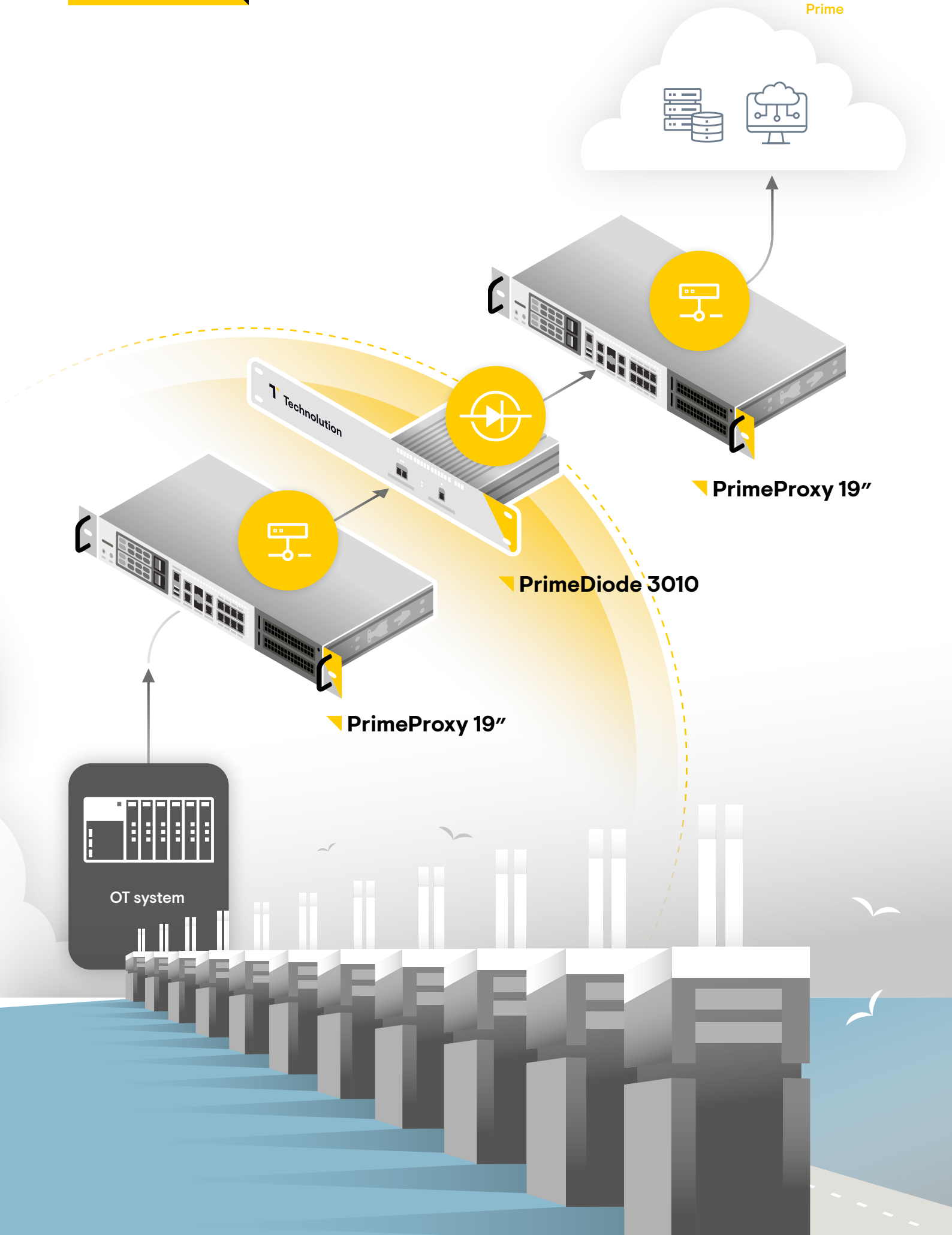
A PrimeDiode 3010 is placed on the IEG between the flood barrier and the control room. It will still be possible to send the log files to the commercial service provider, but reception of external data in the control room will be fully blocked.

A PrimeProxy 19'' will be installed either end of the data diode. This server will be equipped with the PrimeDocks software that supports the transmission of log files through FTP.

All physical devices (3U rack space) will be installed in the control room.

THE SOLUTION

Technolution
Prime



CASE 3

Connected military simulations

SITUATION

The Netherlands and Germany are organizing a joint simulated military. A Dutch fighter jet simulation will be connected to a German tank simulation. The exercises will be held in a connected simulation environment. The Dutch simulation domain contains secret information that must not be shared with the German allies. The other information within the domain may be shared.

SECURITY RISK

Military simulations use information that is directly derived from reality. Part of this information is secret and may not be shared, not even with allied countries, for example information about certain capacities such as the top speed of a rocket.

The Dutch and German simulation environments are connected through DIS (Distributed Interactive Simulation). The DIS standard permits simulation systems in different locations to work together and exchange data to create joint training environments. Because simulation data will be exchanged via DIS in both directions, there is a risk that secret Dutch information will end up in the German simulation.

PHYSICAL CONTEXT

The German and Dutch simulation domains each run in a strongly guarded military environment. There is little to no risk of external trespass.

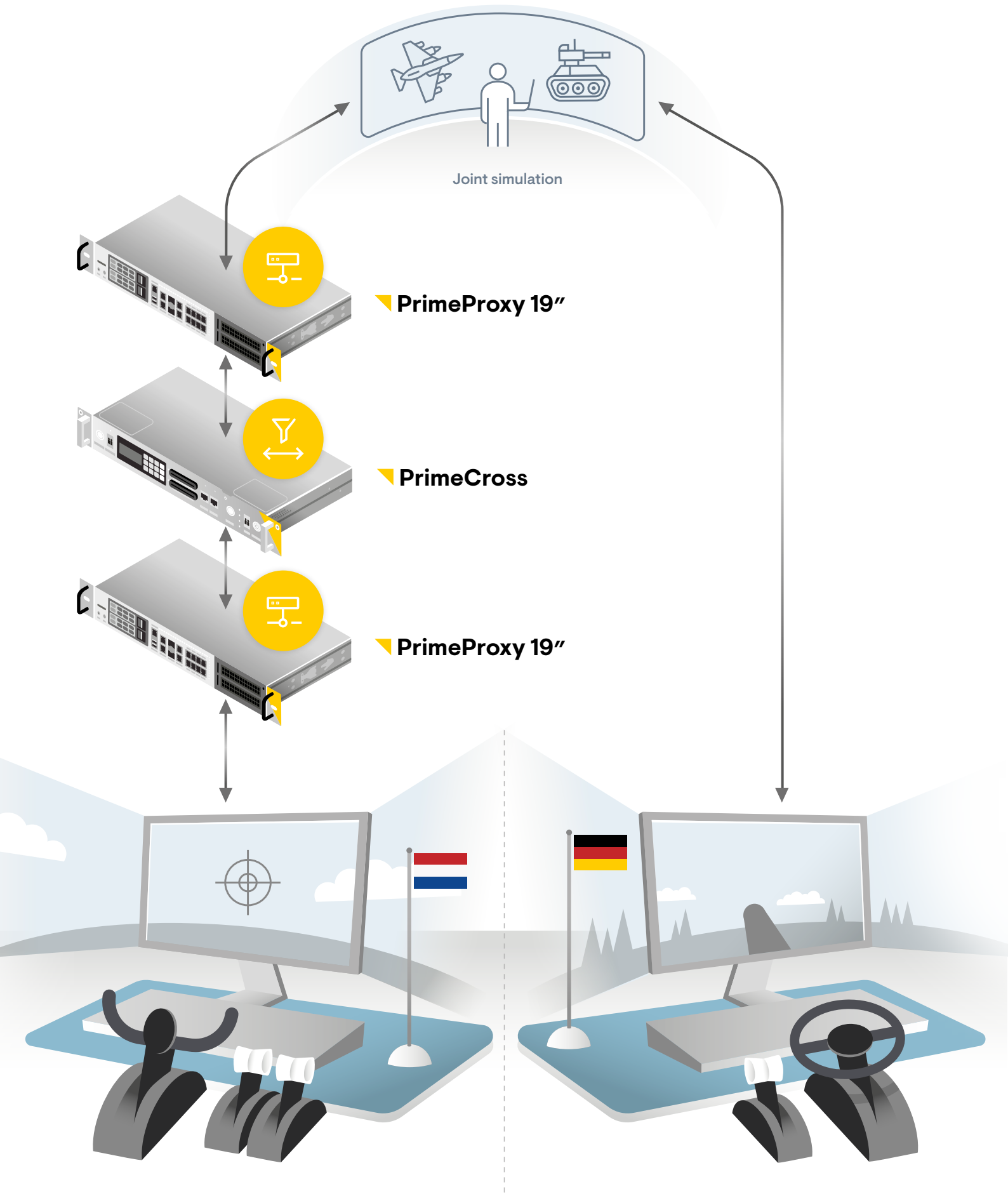
INFORMATION EXCHANGE GATEWAY

A bidirectional PrimeCross data filter will be installed between the two simulation domains. All data from the German simulation will be received in the Dutch domain, but data from the Dutch domain will be filtered using customized filter policies. Only data that meets the conditions set in the policy will be transmitted to the German domain.

A PrimeDocks proxy server is installed on either side of the PrimeCross. The servers run PrimeDocks, which will support the functionality of the simulation environments by handling the DIS protocol and preparing the data for filtering.

All physical devices (3U rack space) will be installed in the same environment as the Dutch simulation.

Technolution
Prime



CASE 4

Time synchronization on a naval frigate

SITUATION

A naval frigate has a complex ICT infrastructure with many systems. Mission-critical internal systems, such as the bridge, radar, propulsion, and weapons systems, depend for the coordination of actions on time synchronization. The high-frequency NTP signal of the time synchronization is received from an external system, for example a satellite or another naval vessel. The integrity of the internal frigate systems is crucial.

SECURITY RISK

In a military environment, the integrity of the bridge and weapon systems is a matter of life or death. A data leak of classified data from the database and the bridge constitutes the greatest risk for the frigate. But the integrity of the internal systems is similarly of crucial importance. Control over these systems onboard the frigate must never be compromised.

The connection of the external time synchronization with the internal systems of the frigate therefore constitutes a risk. Theoretically, this connection could be used to gain access to the internal systems and the operations center.

PHYSICAL CONTEXT

All internal systems and the operations center are located on the frigate. Both the physical environment and the ICT environment are heavily protected against external access, but space for installing new equipment is limited.

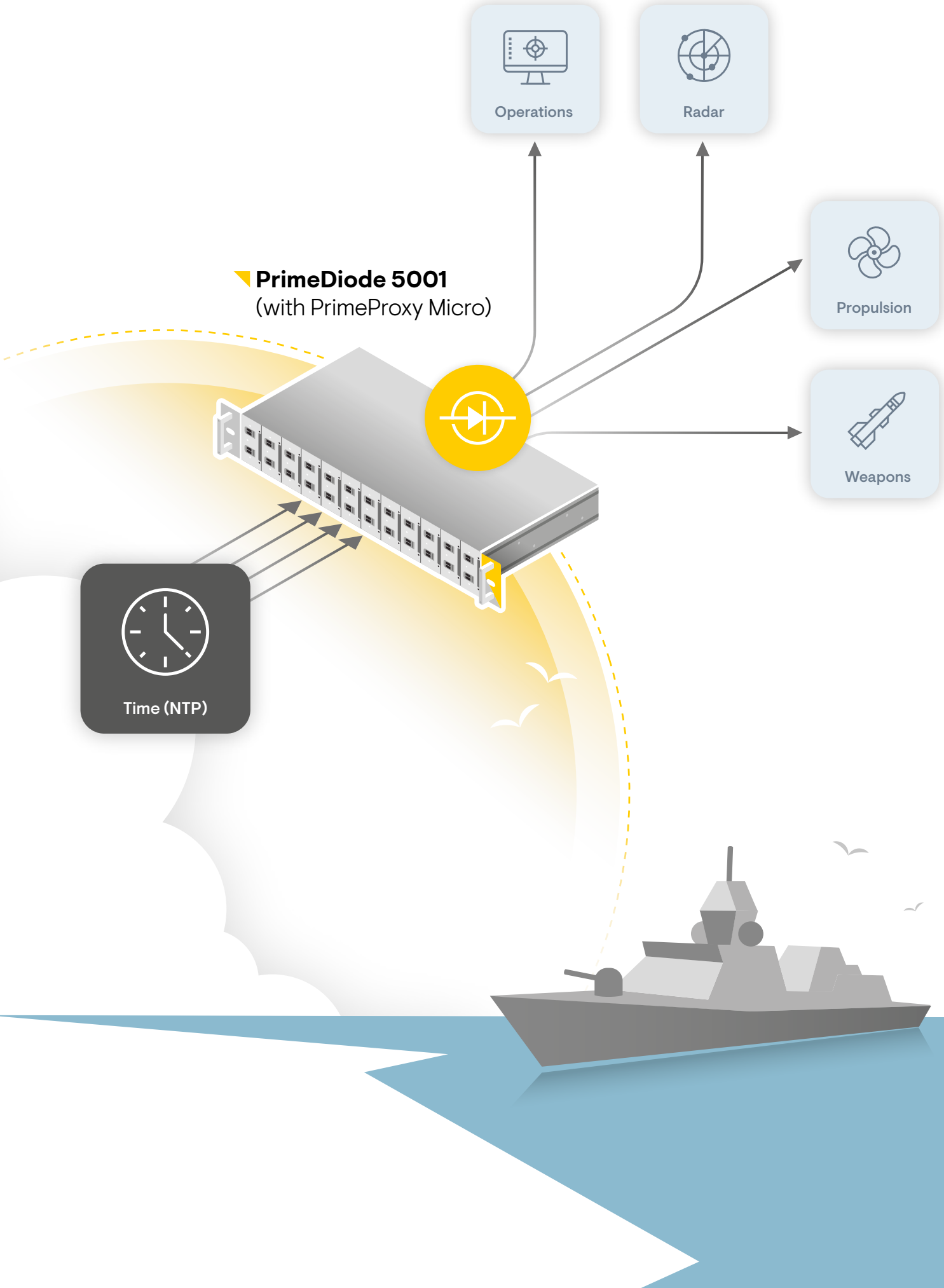
INFORMATION EXCHANGE GATEWAY

Multiple PrimeDiode 5001s will be used to create IEGs between the external time synchronization and the internal systems. This will ensure that the highly confidential information on operations and operational systems, such as the radar, propulsion, and weapons, is securely protected from the outside world.

The PrimeDiodes will be equipped with a PrimeProxy Mico on either side, which handles the NTP protocol. No additional equipment is required for the PrimeProxy Micro. Thanks to the PrimeDiode 5001's compact housing, up to 12 diodes can be installed in 2U rack space.

THE SOLUTION

Technolution
Prime



CASE 5

Classified cloud environments

SITUATION

A private cloud provider offers services for working with classified information. Users and administrators work remotely in various virtualized cloud applications that have been cleared for various classifications. Files with the correct classification are exchanged between the cloud applications. Updates are collected from the internet and installed on the cloud applications by the administrators.

SECURITY RISK

The various cloud environments have different classifications; file exchange between these environments must happen only in a controlled manner. Users work from their own physical work stations in unknown locations via secure connections.

The administrators also work remotely from various locations. Updates of applications in the cloud environment are validated and verified by the administrators before they are applied. The infrastructure is dynamic and subject to frequent change – for example by the addition of new cloud environments and applications.

In this context, there is a risk that highly classified information will end up in a domain cleared for a lower classification. In addition, the online connection with the management environment carries the risk of data leaks of classified data.

INFRASTRUCTURE

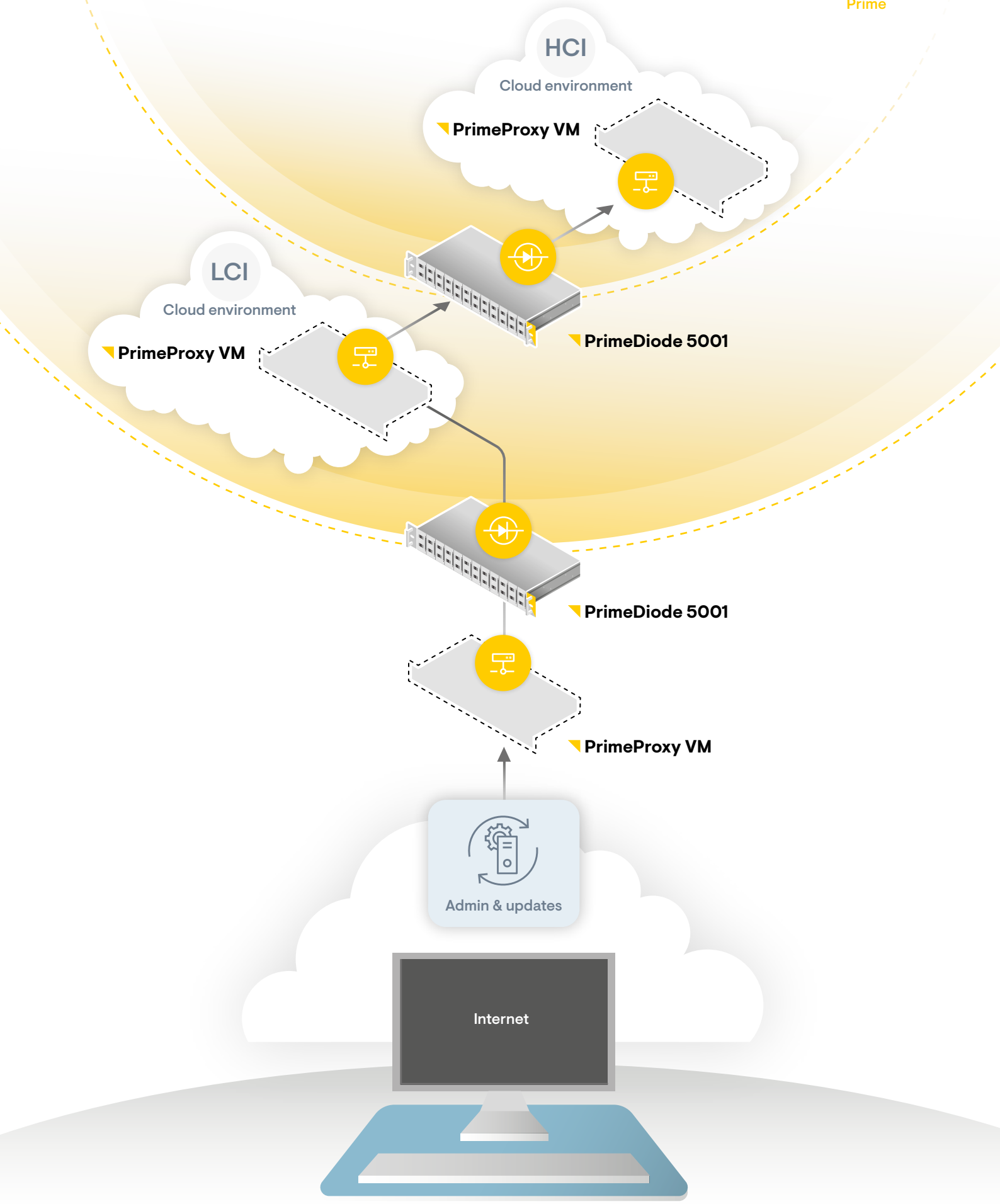
The cloud environments are fully virtual, from network servers to applications. Users work with the cloud applications through Remote Desktop and a VPN.

INFORMATION EXCHANGE GATEWAY

The IEGs between the management systems and the cloud environments are secured with a PrimeDiode 5001. This will prevent the leaking of classified data from the cloud environments. The exchange of highly classified files with environments cleared for lower classifications will be blocked.

The PrimeProxy servers will be deployed as virtual machines. They will the run PrimeDocks platform that implements all functional chains.

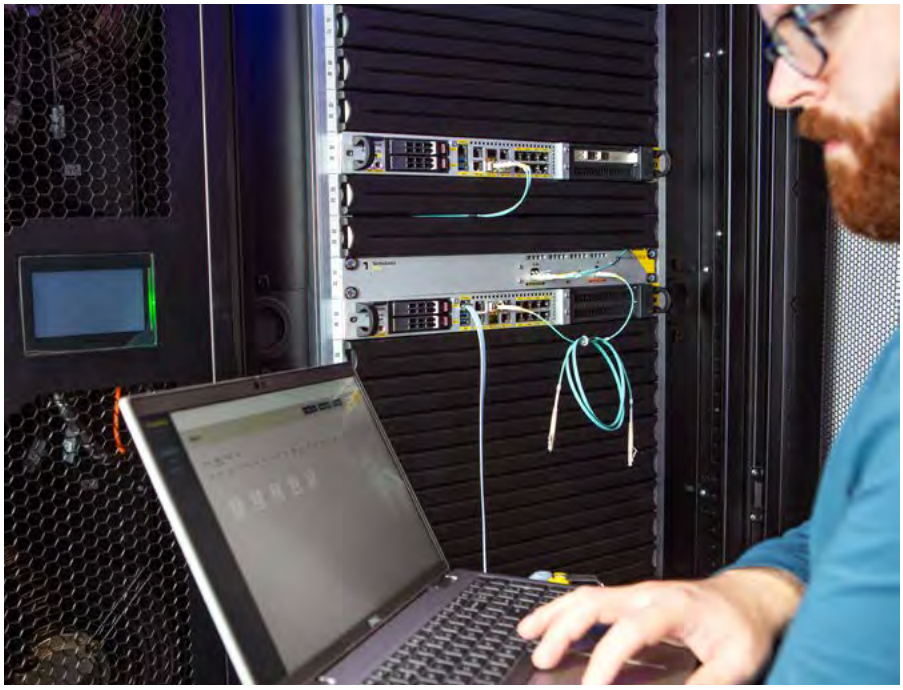
Technolution
Prime



Focus areas for Cross-domain solutions

Are you considering using Information Exchange Gateway (IEGs) in your ICT infrastructure? Many aspects enter into play in the development and implementation of a IEG.

Security and the protection of classified information, important assets, and systems are the main priority. These goals depend strongly on the physical environment and security of the location, the nature of the digital data, and the make-up of your ICT infrastructure. To find the optimal solution, it is important to map all relevant aspects clearly. Read here about the main focus areas.



1. Security

What are the assets that need to be protected?

An IEG can protect information, but also for example a production facility, or a military object. Inventory the *data, systems, and objects* that require protection. Then determine where they are located: in a data center, a network environment, a vehicle, somewhere else?

What are the main threats and risks?

For instance, that confidential information becomes known, or external interference in the control of mission-critical systems. Will the IEG have to protect the *confidentiality* (no sensitive data must go out) or the *integrity* (no attacker can get in) of the assets?

2. Functionality

Which systems and applications are involved?

Map what applications and systems will exchange information through the IEG. Determine what communication protocols will be used for this. Make a full *inventory of systems, applications, and communication protocols*.

What performance level will be required?

Determine the performance requirements for the IEG with regard to *bandwidth and latency*.

3. Physical environment

Where will the IEG be installed?

Calculate *how much space is available* for the cross-domain devices and the proxy equipment that the IEG requires. Also include the required *power supply* in your calculations.

What are the physical conditions?

Certain *environmental factors* can affect the functioning of the IEG equipment, for example *weather conditions*, dust, humidity, or hazardous substances. Also take into account any *physical security requirements*, such as alarm systems and required locks.

4. Certification

What certifications or permits are required?

In many cases an IEG will have to meet certain *(legal) requirements*. Identify what *authorized agency* will verify this and which regulations the IEG must meet.

Does the IEG you have selected meet the requirements?

Determine what *additional measures* must be taken, if any.

5. Management

What support will be required?

Determine whether the IEG will be maintained and supported *internally or by an external party*. Choose the right *service level, the required availability and continuity*, and find out how error notifications will be processed. Determine what kind of *monitoring* will be needed and who has access to the monitoring data.

How will change happen?

An IEG is usually not static. It should *adapt* to the changing needs of your organization. Determine the frequency and steps required in case of *updates, changes, or extensions* of the IEG.

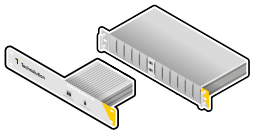
Overview **Information Exchange Gateways**

Below you will find an overview of possible Information Exchange Gateways (IEGs).
D1 – D5 are Diode IEGs: data traffic is restricted to one direction only.
F1 – F5 are Filter IEGs: data trafic is filtered according to policies.

Diode IEGs

D1

PrimeProxy 19"

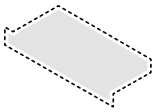


PrimeDiode
3010 / 5001

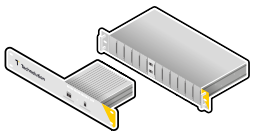
PrimeProxy 19"

- 3U or 4Urack space
- Full functionality
- Case 1
  Drone observation
- Case 2
  Flood Barrier

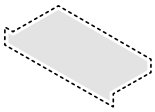
D2



PrimeProxy VM



PrimeDiode
3010 / 5001

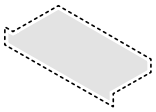


PrimeProxy VM

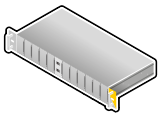
- 1U or 2U rack space
- Proxies in VM platform*
- Case 5
  Cloud environment

* *Direct connection between proxies and diode required*

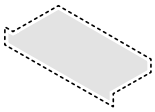
D3



PrimeProxy VM



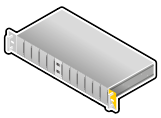
PrimeDiode 5001
+ PrimeProxy Micro



PrimeProxy VM

- 2U rack space
- Proxies in VM platform

D4

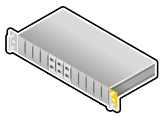


PrimeDiode 5001
+ PrimeProxy Micro

- Smallest housing
- Specific protocols (NTP , HTTP)
- Case 4
  Time synchronization

D5

PrimeProxy Flex



PrimeDiode 5001

PrimeProxy Flex

- Compact
- Limited number of chains
- Development in progress

Technolution
Prime

Filter IEGs

F1

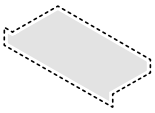
PrimeProxy 19"

PrimeCross
FD60

PrimeProxy 19"

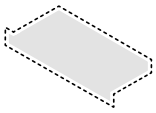
- 3U rack space
- Full functionality
- Case 3 Simulation

F2



PrimeProxy VM

PrimeCross
FD60



PrimeProxy VM

- 1U rack space
- Proxies in VM platform

F3

PrimeProxy
Integrated

PrimeCross
FS60

PrimeProxy
Integrated

- 1U rack space
- Integrated proxies
- Limited number of chains

F4

PrimeProxy
Integrated

PrimeCross
FV40

PrimeProxy
Integrated

- Smallest housing
- Suitable for vehicles

Technolution

Founded
1987

Technology company

Multi-disciplinary – software, electronics and programmable logic

- Solutions that matter
- Reliable technology
- Thinking outside the box

300
Motivated employees

8,4
Employee satisfaction

8,2
Customer satisfaction

75 mln.
Turnover

17e
In Dutch top 50 engineering companies

10-15%
Of turnover spent on R&D

30e
In Dutch top 30 R&D

Locations

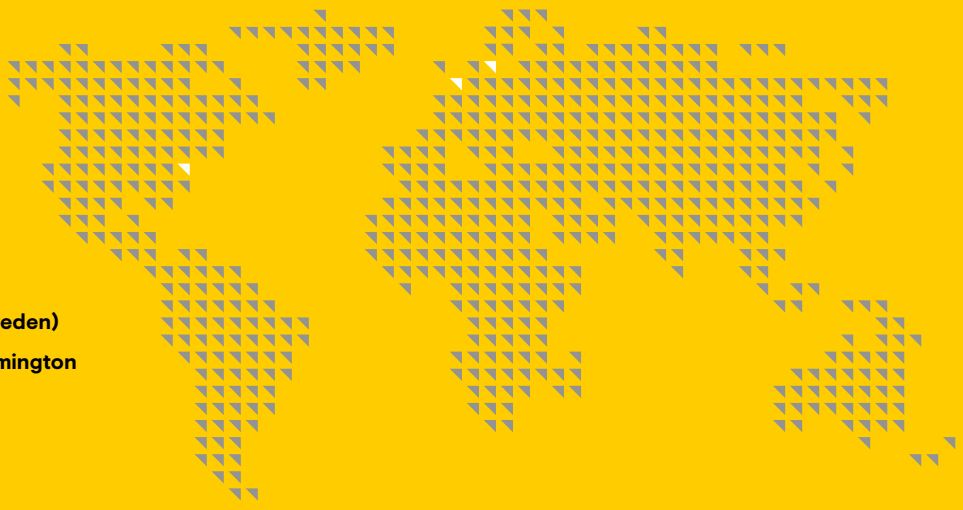
Technolution - **Gouda**

Technolution Deventer - **Deventer**

Phase to Phase - **Arnhem**

Technolution Nordics - **Stockholm (Sweden)**

TNL USA Inc. & TNL Nanotech Inc. - **Wilmington**



Sub-brands

- Technolution Move
- Technolution Perform
- Technolution Prime
- Technolution Spark
- Technolution Advance

Certifications

- **ISO 9001** Quality
- **ISO 27001** Information security
- **ISO 14001** Environment
- **CO_2** Performance Ladder level 5

COLOPHON

DESIGN, LAY-OUT AND INFOGRAPHICS
Studio Piraat, The Hague

Redefining
solutions

11. 2024

Technolution
Prime

About Technolution Prime

Technolution Prime is the leader in the Netherlands in preventive high assurance solutions for classified data. We develop our products and solutions entirely in-house. We stand for high quality cyber security where it is needed most.

Technolution
Burgemeester Jamessingel 1
2803 WV Gouda
The Netherlands

+31 (0)182 59 40 00
prime@technolution.com
technolution.com/prime
Technolution Prime

technolution.com/prime