advenica

SOLUTION DESCRIPTION

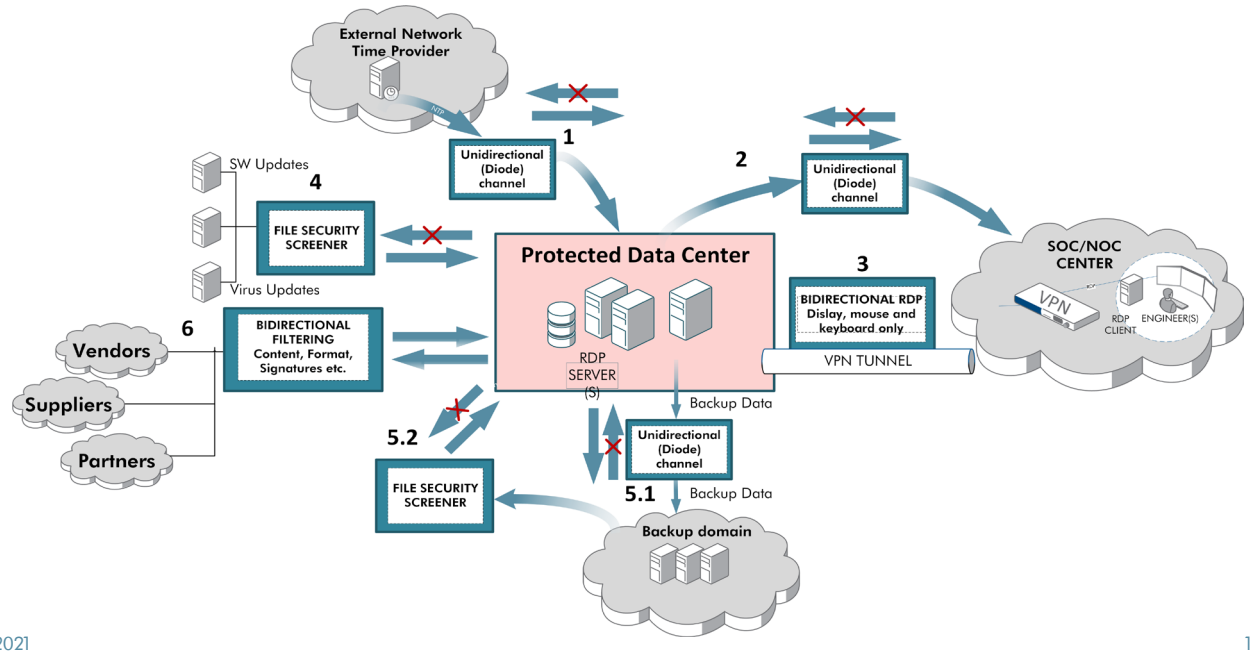
How to Secure your Data Center

It can be a challenge to run and operate data centers. This solution description provides you with the tools you need to manage them in a secure manner.

Challenge

Running a Data Center in a Secure Way

Running and operating data centers keeps getting more challenging, particularly from a cybersecurity perspective. The ever-increasing need for networking with external systems, remote administration requirements as well as extraction of performance and network management data, to mention just a few, is also increasing the number of possible attack vectors. In addition, wireless networks, and a growing range of IoT devices across the board can potentially provide attack channels that are not even visible today. Traditional network segmentation and firewalls provide some protection but are all ultimately vulnerable, especially facing state sponsored hackers with vast resources. Throughout history, the military defence sector has been highly security aware and cybersecurity solutions developed for this market are the strongest available today. These solutions are now being made available to the private marketplace, both enterprise and critical infrastructure.



Solution

Prevent Data Extraction and Protect Domain Integrity

The most obvious points in and around a data center that needs high level cybersecurity protection are:

- Importing network time
- Extracting performance and reporting data
- Performing remote administration
- Importing SW and OS updates
- Performing data backup and restoration
- Exchanging data with suppliers, vendors and partners
- Segmentation in shared data centers

Solutions for providing the highest level of cyberprotection can be divided into two main categories: VPN Encryptors and Cross Domain Solutions consisting of products for unidirectional traffic control and bi-directional traffic control. In conjunction with these, there are highly effective file screening and sanitation solutions as well as content disarming and reconstruction.

Here are a number of suggestions of how to effectively secure the various channels to and from a data center:

1. Importing Network Time

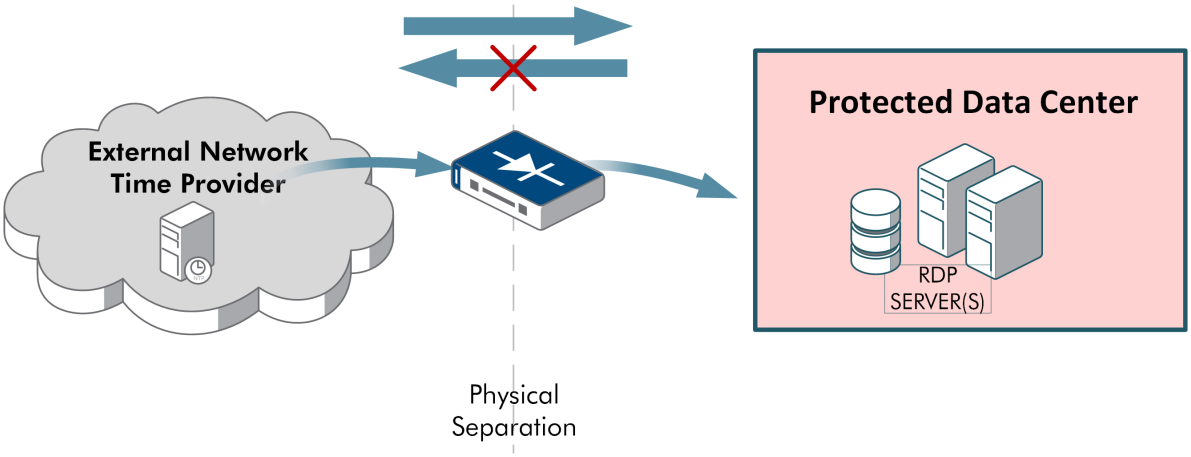
Every data center needs to import Network time in order to synchronise all servers to use exactly the same time. Securing the channel used for NW Time import, making it impossible to use for extraction of any data. Handled by Data Diode DD1000i including NTP service.

Functions:

- Accurate and synchronised time for all servers and devices inside the data center
- Secure NTP import from external source without sacrificing the integrity of the data center domain

Benefits:

- Securing the channel with a unidirectional data diode prevents any possible data extraction from the protected domain using this channel



2. Extracting Performance and Reporting Data

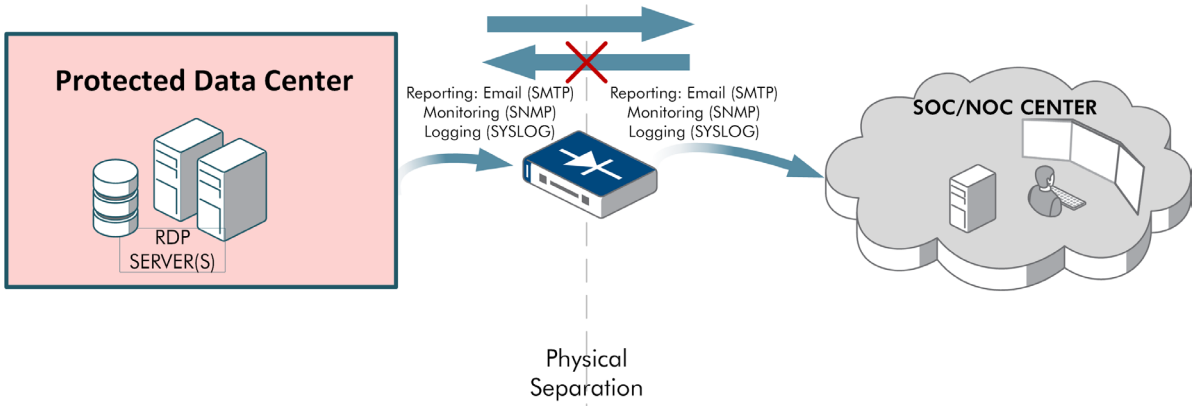
Providing a secure way to export performance values, monitoring and network management data without opening any channel that could compromise the servers in the data center. Handled by Data Diode DD1000i including SMTP, SNMP and SYSLOG services.

Functions:

- Data center reporting and monitoring data to SOC (Security Operations Center)

Benefits:

- Secure one-way data transfer without sacrificing domain integrity
- No malicious reverse traffic or access physically possible
- Allows more flexible role-based operation



3. Performing Remote Administration

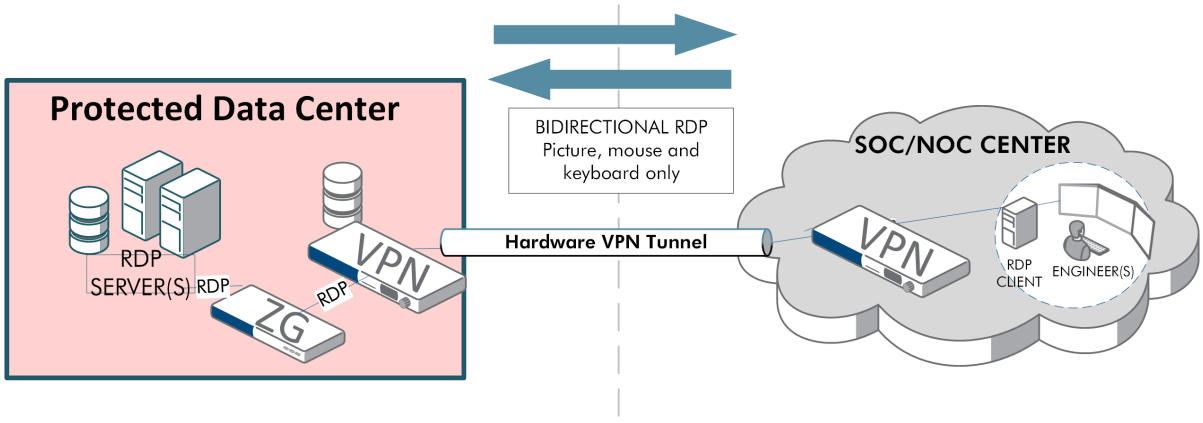
Providing a secure channel for system administration, with real time filtering of allowed traffic in both directions. Handled by ZoneGuard over a VPN encrypted connection.

Functions:

- Remote management of data center systems through high secure VPN-tunnel (up to level SECRET)
- Access Control and content filtering by ZoneGuard RDP-services

Benefits:

- Secure two-way remote management services ensuring integrity of managed domain
- Safe-guards both the confidentiality and integrity of the interfaced systems
- Provides secure access to several different systems in diverse security domains from a single computer
- Enables users in a protected network to access resources in a lower classified network including Internet integrity, protecting the secure domain from unwanted internet traffic



4. Importing SW and OS Updates

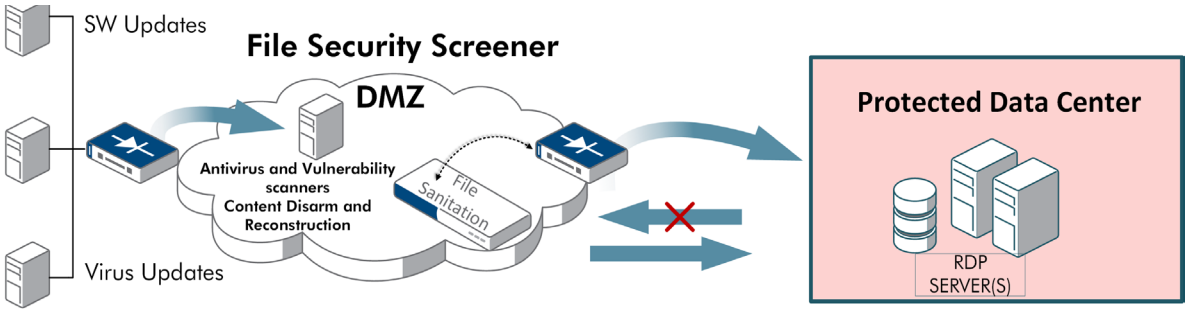
Even the most secure environments have to import OS and other SW updates. This poses a risk of malware being imported as part of the update package. This risk can be eliminated by using a sanitation solution that cleans all files before sending them on. Handled by File Security Screener including multiple Data Diode DD1000i's, File Server, Anti Malware Scanning, Content Disarm & Reconstruction and Solution Engine.

Functions:

- Cleaned and sanitised SW and other data imports to the secure domain
- Data center integrity assured by physical one-way isolation

Benefits:

- Supports multiple source networks where files should be imported in to a single security domain
- High assurance protection from malware infections
- Caching of data to be scanned, allowing service on the central equipment without data loss
- Scalable solution with ability to increase the number of connected source networks



5. Performing Data Backup and Restoration

A data center requires safe ways to backup its data, as well as a way to safely restore the data into production should the production environment be compromised.

5.1 One-Way Production-Backup Data Replication

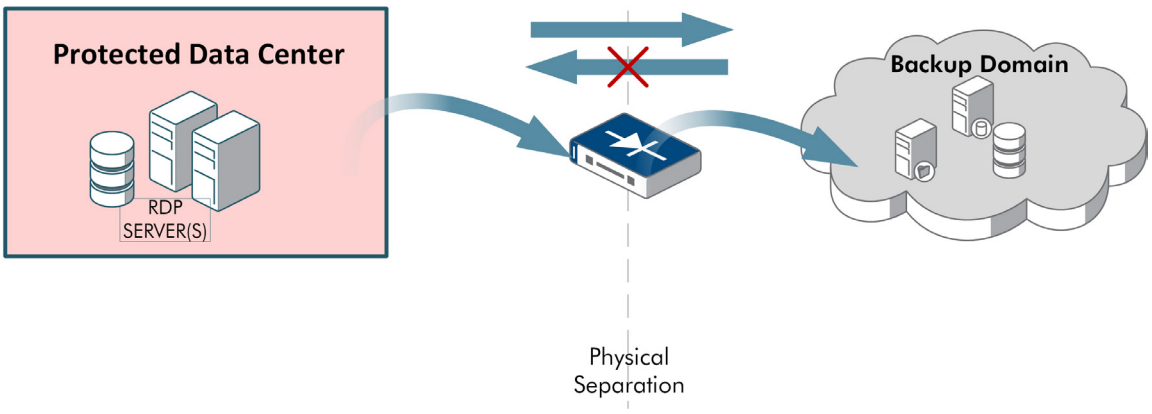
Handled by Data Diode DD1000i including needed proprietary protocols.

Functions:

- Secure, one-way production-backup data replication

Benefits:

- A failsafe way to protect your confidential data when moving it
- No malware, destructive data or simple administrative mistake can change the information flow
- Can safely connect two networks of the same or different security levels



5.2 Secure Backup Data Restoration

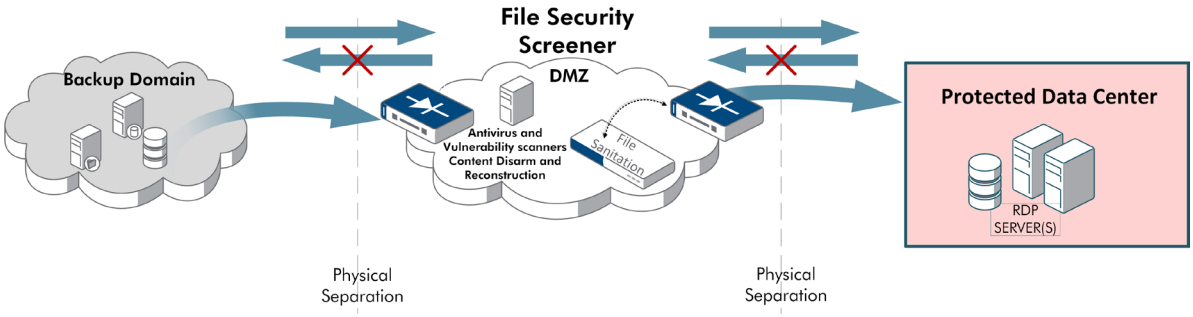
Handled by File Security Screener including multiple Data Diode DD1000i's, File Server, Anti Malware Scanning, Content Disarm & Reconstruction and Solution Engine.

Functions:

- Cleaned and sanitised data restored, even in the event of malware contamination
- Backup domain integrity assured by physical one-way isolation

Benefits:

- A failsafe way to protect confidential data when moving it
- No malware, destructive data or simple administrative mistake can change the direction of the information flow
- Can safely connect two networks of the same or different security levels



6. Exchanging Data with Suppliers, Vendors and Partners

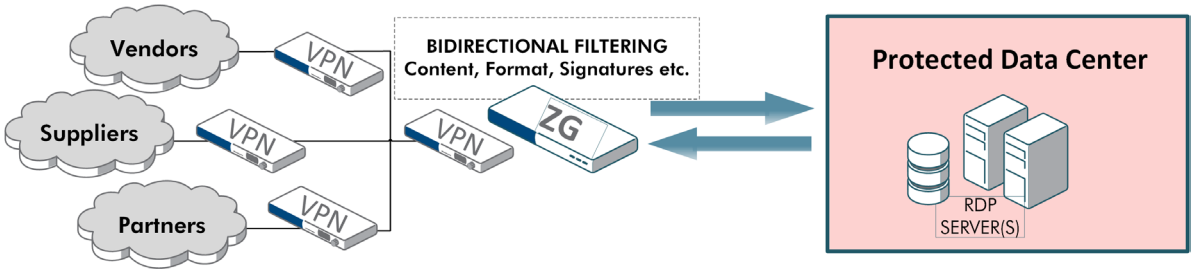
Practically all data processing facilities communicate with outside partners, suppliers etc. All these communication links should be protected from enabling malicious attacks. Depending on the nature of the connection various security solutions can be used from VPN encryptors to bidirectional gateways that filter traffic and block unwanted content.

Functions:

- Secure HW encrypted data channels between all domains
- Bidirectional filtering and verification

Benefits:

- Simple future-proof key management
- Silent mode reception to avoid detection
- Low bandwidth and jitter resilience
- Versatile high-availability including failover
- Power outage resilience



7. Segmentation in Shared Data Centers

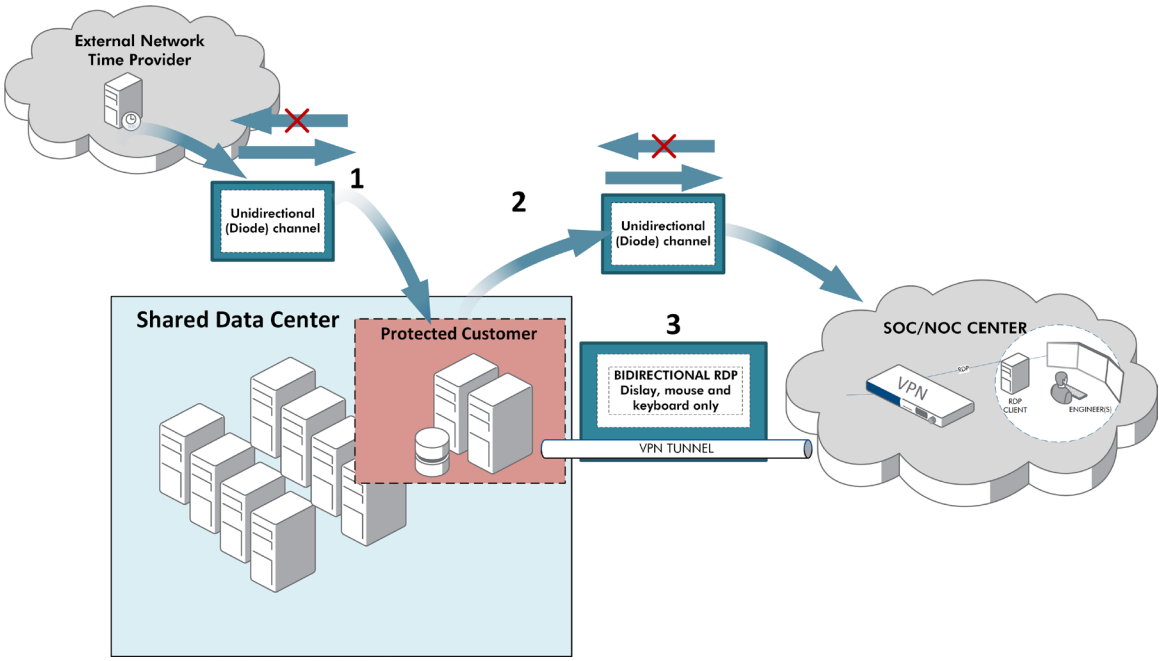
These solutions can be used if you are locating your servers in a third-party shared data centre and want to make sure your connection is isolated from the data center host as well as other customers using the same shared infrastructure.

Functions:

- Secure the NTP Source from manipulation
- Secure channel for reporting and analytics from your infrastructure
- Secure remote management from SOC/NOC and administrator access

Benefits:

- Secure two-way remote management services ensuring the domain integrity of the data center
- Provides secure access to several different systems in diverse security domains from a single computer
- Enables users in a protected network to access resources in a lower classified network including Internet
- Allows more flexible role-based operation



advenica

Advenica provides expertise and world-class high assurance cybersecurity solutions for critical data in motion up to Top Secret classification. We enable countries, authorities and companies to raise information security and digitalise responsibly. Founded in 1993, we are EU approved to the highest level of security. Our unique products are designed, developed and manufactured in Sweden.

Read more at advenica.com

ISO 9001 CERTIFIED
ISO 14001 CERTIFIED