use case 06

ZoneGuard

Secure remote desktop connections

advenica

Providing secure and selective access to a system from a remote network is a challenge. The access must be adapted based on defined policies and tuned for the specific systems. It is critical that the sensitive information stays within the protected network and that malicious code cannot spread. ZoneGuard with remote desktop capability mitigates the threats in a remote access scenario.

Secure remote desktop connections

Enabling access to systems

Connecting systems or networks of different security levels, where one of the system may be untrusted and outside the organisational control poses a great security risk. Products for bridging this security domain gap must mitigate security threats by:

- stopping any sensitive information from leaving the protected network.
- stopping malicious code, e.g. trojans, viruses or zero-day attacks from entering the protected network.
- limiting permitted remote access methods.

ZoneGuard employs a well-defined information access methodology to reduce attack exposure. It safe guards both confidentiality and integrity of the interfaced systems by:

- transforming the Remote Desktop Protocol stream into single bitmap images, keystrokes and mouse movements at the cross domain point.
- validating the bitmap images, the keystrokes and the mouse movements to ensure correct information types.
- applying flexible filters, e.g. noise on the bitmap images, adding variables to mouse movement or restricting valid keystroke codes.

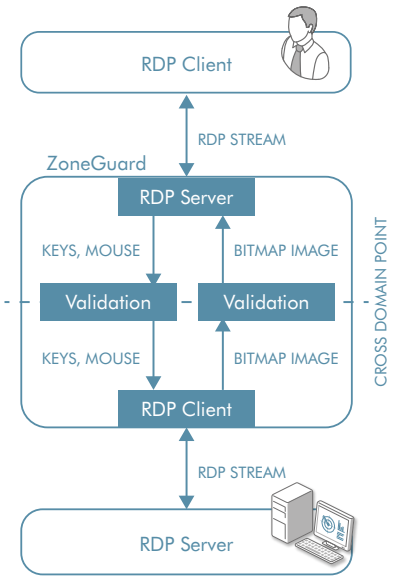

Illustration: ZoneGuard RDP Information flow

Scenarios

Examples of ZoneGuard scenarios for remote desktop connections include:

- providing secure access to several different systems in diverse security domains from a single computer.
- enabling users in a protected network to access resources in a lower classified network including Internet.
- safe guarding jump servers and providing secure remote access for suppliers of equipment or off-site consultancy.

Remote Desktop Protocol support

ZoneGuard supports the remote access case by utilising the Remote Desktop Protocol (RDP).

Validated information flow

Users on Security domain 1 connects to a RDP server located inside the ZoneGuard. ZoneGuard terminates the protocol and extracts keystrokes and mouse movements from the stream. The extracted information will be forwarded

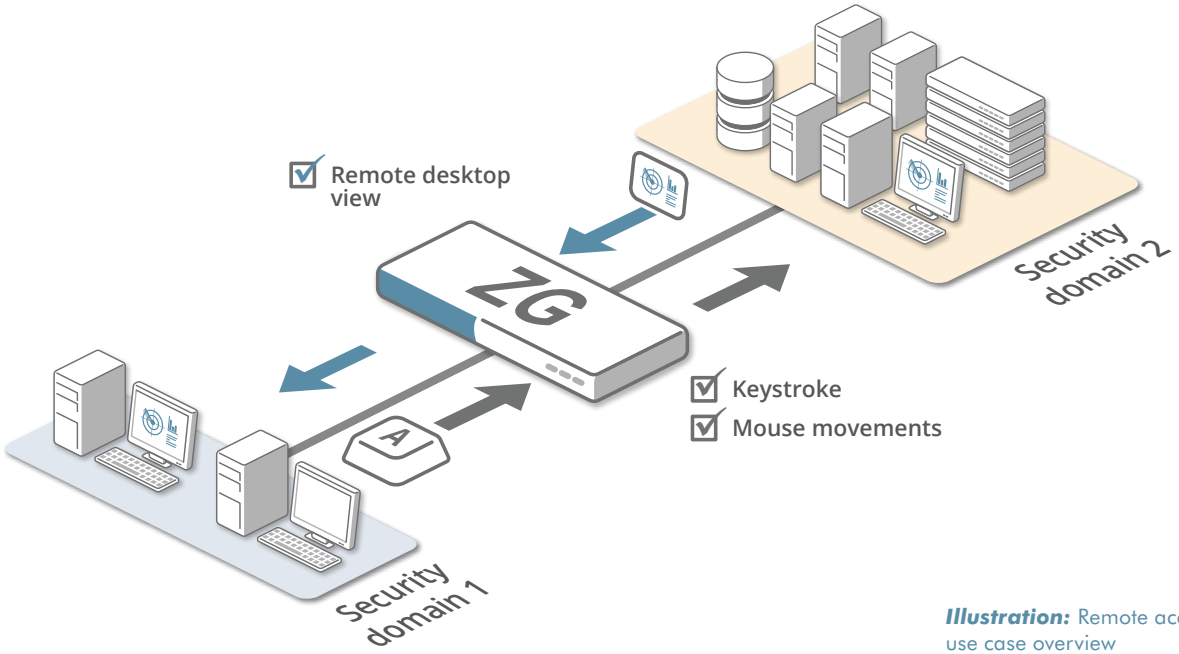

Illustration: Remote access use case overview

by ZoneGuard if an information policy is fulfilled. It is possible to restrict the valid keystroke codes in the information policyif necessary. The validated information is sent from a RDP client insidethe ZoneGuard to a receiving RDP server located on Security domain 2.

In the opposite direction, the RDP server on Security domain 1 sends the information to the RDP client inside the ZoneGuard. The RDP image stream is terminated and transformed into single bitmap images. ZoneGuard validation node ensures that the image is true bitmap image by fingerprinting the encoding. It is possible to modify the bitmap image inside the validation node to add or subtract information. The validated image is send to the RDP client on Security domain 1 though the RDP server inside ZoneGuard.

Simultaneous RDP connections through the ZoneGuard may exist by defining multiple message paths.

Benefits

By using ZoneGuard the remote access is controlled by a policy defined by the stakeholder's authority. Threats towards a remote desktop solution is effectively mitigated in the cross domain point by ZoneGuard's validation and transformation of all information.

ZoneGuard technology

Advenica's ZoneGuard technology reduces potential attack vectors by enforcing an organisation's information policy to achieve secure information exchange between two separate systems by:

- *Full message inspection and termination of the Remote Desktop Protocol (RDP) provides protection on all information levels, including the application layer*
- *Information within the RDP is transformed to mitigate direct attacks aimed at the application layer on the target system*
- *Safeguards which information that will be passed on to the receiving network and only allows for well-defined information to pass the boundary of the security domain*

The RDP information flow may be combined with other information flows to support more use cases e.g. file exchange or email transfer

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

advenica

ISO 9001 CERTIFIED
ISO 14001 CERTIFIED