Background information:

Firewalls, segmentation and islandization

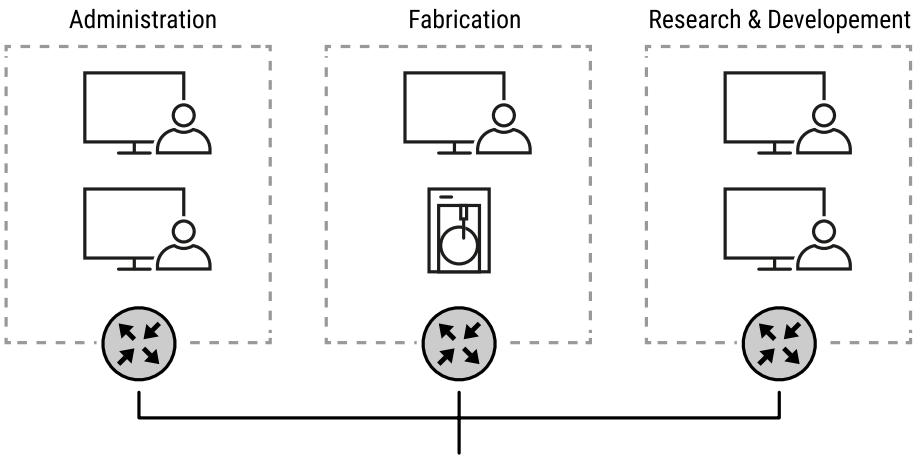
One widely used technique for improving security in corporate networks is to subdivide them into smaller segments by department. Communication between these subnets is monitored, controlled and logged by firewall routers. Attackers and malware that succeed in penetrating one of the subnets are prevented from further spreading by packet filters. One way of further increasing security is targeted isolation of individual systems and function units into their respective own network segment. This effectively protects even highly vulnerable devices.

Segmentation: Subdivision into secure subnets

The internet protocol (IP) makes it possible to exchange data beyond network borders. The information encapsulated in IP packets is sent to its destination through various routers.

Network administrators take advantage of this routing property to divide corporater networks into sub-networks which are linked to each other. The administrative computers are assigned to the management subnet, and even production machines are given their own network segment, just as with the desktop machines in the R&D department.

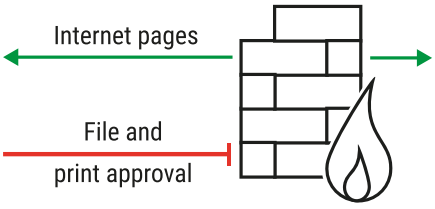
Each of these network segments is attached to the surrounding corporate network through a router. All communication between the subnets is passed through the routers.



Packet filters for greater security

It makes sense to analyze the passing data packets at the router and send on only permissible data packets.

It could be in the interest of company management for example to allow employees in the administration department to have free access to web sites in the Internet, but at the same time have their sensitive data, such as salary statements or contracts, remain inaccessible in the corporate network and Internet. These are made available in the Windows network via file and printer sharing.



A packet filter installed on the router analyzes whether the passing network traffic contains connections which could be used by the file and printer sharing. These are TCP connections to ports 139 and 445. If the packet filter detects IP packets which contain TCP communication with these ports, they are not passed along, but rather rejected. Whereas file and printer sharing continues to function within the subnet for administration, it cannot cross segment borders. Nor is there access to files such as salary statements from other network segments.

A router which filters data flow in this way is called a firewall router, or simply firewall.

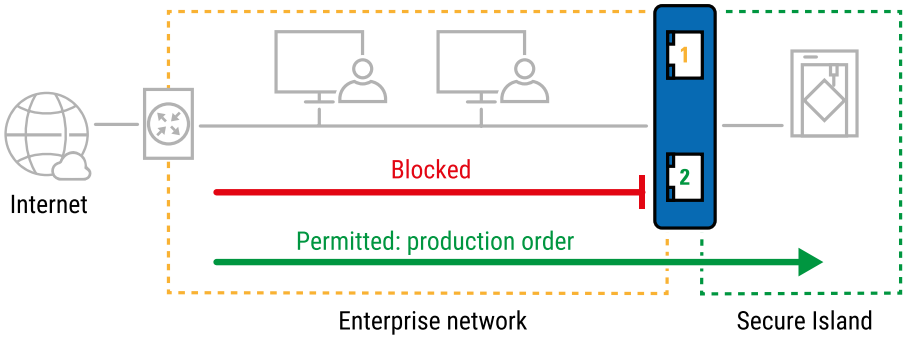
Islandization: Targeted segmentation of individual systems

The firewall rules for large subnets can quickly become confusing and complicated. If they are to generously dimensioned, they can be exploited by attackers. If they are made too narrow, function limitations can result. Each terminal device in a segment is also a possible source of undesired access.

Especially devices and systems with a high need for protection - such as machine tools, medical equipment, but also older control computers or those with outdated software - often have known, exploitable security holes which are no longer detected by rules.

Islandization means that these especially vulnerable systems in the network are identified and with the help of firewalls such as Microwall isolated in their own network segment - a secure island. The necessary connections between systems on the island and the surrounding network are determined in advance and described by means of a positive list of rules. Only expressly permitted data packets are passed along, all others are rejected and logged if needed. Isolated systems are therefore effectively protected from attacks by hackers or malware as well as from human error.

Only a small number of systems are located on these secure islands. Because they are protected by a narrowly described and task-targeted set of rules, islandization ensures significantly enhanced security.



Islandization with the Microwall is easy to implement and effectively increases the security level in the corporate network. This is especially beneficial for smaller companies for which cumbersome segmentation by department is not worth the effort.

The proof of the pudding is in the eating!

Thomas Clever
t.clever@wut.de

You can reach our engineers by phone at+49 202/2680-110 (Mon.-Fri. 8 a.m. to 5 p.m.)

W&T
www.WuT.de

We are available to you in person:

Wiesemann & Theis
GmbH
Porschestr. 12
42279 Wuppertal
Phone: +49 202/2680-110 (Mon.-Fri. 8 a.m. to 5 p.m.)
Fax: +49 202/2680-265
info@wut.de