White Paper

White Paper:
Common Network Segmentation Strategies for Production Environments

Importance of Network Segmentation

Business needs for all company sizes increasingly require managed production environments to perform critical computational and data storage roles that are often administered by company IT professionals, as well as potentially providing services to both internal and external entities. As a preamble, most common production environments tend to be heavily Linux-based, while most corporate environments are either predominantly Windows or a mixed environment with Windows and MacOS machines.

While it should be obvious that the production environment should be heavily protected from arbitrary access from the internet, it can be easily overlooked that protecting company and customer data also necessitates security measures against the corporate and other internal networks.

Basic Network Segmentation

Particularly in smaller environments, the simplest method of network segmentation is to simply separate the production environment into its own subnet or VLAN (virtual LAN) in the case of physically disparate environments. Network services that are required to perform business needs can then be individually whitelisted (via Acces Control List (ACL) or similar) and then the point of access can be monitored for malicious activity via SIEM. Meanwhile connections are recorded to assist in forensic efforts in case of a discovered, but previously occurring network breach.

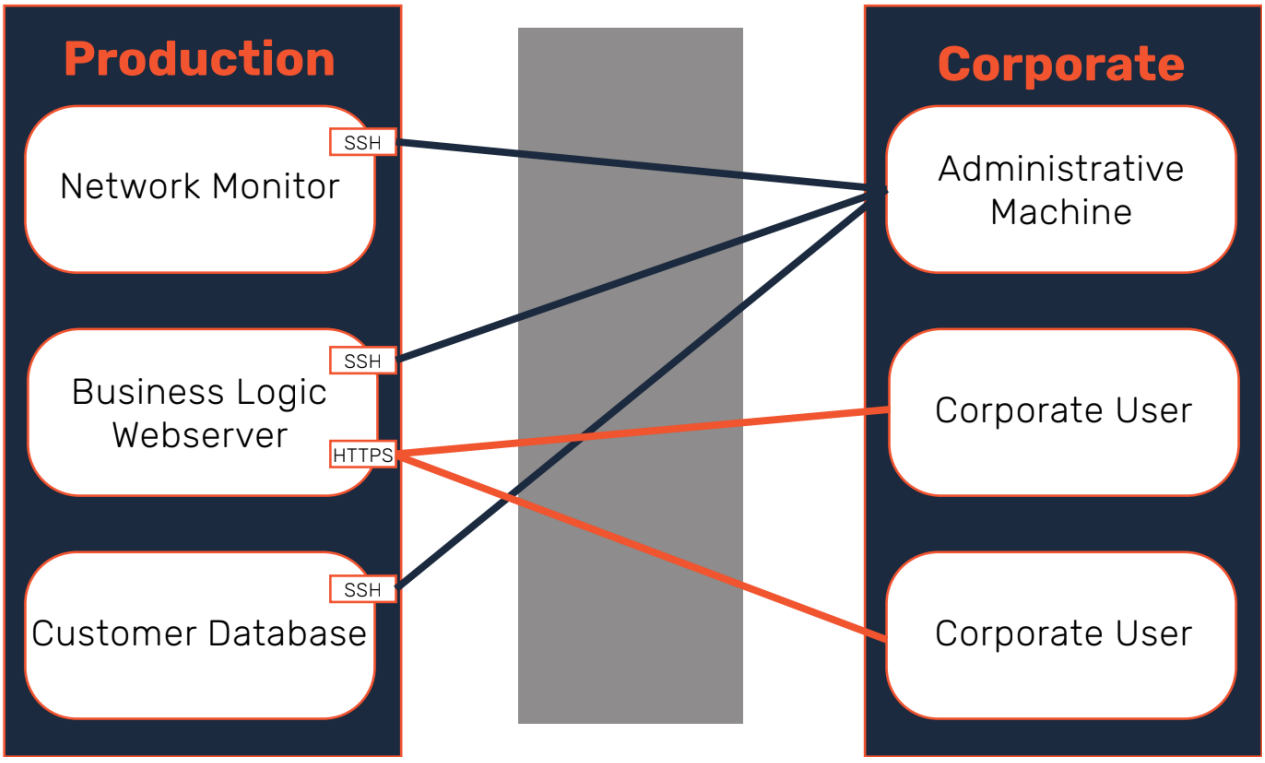
This architecture should be considered the lowest minimum “secure” arrangement, as it requires very little additional hardware. As an example, some potential network services that are likely to be required to be whitelisted in this arrangement are administrative traffic (SSH, RDP, etc) as well as connections to perform business logic such as web services (HTTPS, etc) for normal users.

This arrangement can be considered fairly secure, but it has flaws that can be potentially exploited by an attacker with an understanding of the network. In the case of a breach of a non-production network, all whitelisted paths should be considered to be potentially vulnerable as an attacker with the ability to fully compromise the non-production network will also likely have the ability to use whitelisted connections to the production network. In most cases, this will occur by compromising network resources that have remote administration access to the production network.

Exploitation of production servers through service ports are a potential alternate vector, but are much less likely when proper patching and updates are being performed. The detection of such a breach would most likely occur through proper monitoring in the non-production network, but could also be discovered through anomaly detection in time of access or actions performed, as access to the production network would use legitimate credentials from legitimate sources.

Additional hostbased logging and anomaly detection is advised on production servers to limit the extent of the damage in case of a breach.

Basic Network Segmentation Diagram



Jump and Bastion Host Accessible

A more mature, and similarly more difficult to administer, solution to improve security is to employ a series of Jump Hosts (for administration) and Bastion Hosts (for network service proxying) to provide fewer points of access to the production network requiring monitoring. When these intermediaries are being used, the production network should be thought of as fully separate from non-production networks, likely with no possible route between them as opposed to a simple ACL blocking communications.

Any interaction with the production network should require first connecting to an intermediary host requiring additional authentication measures. Once connected to the intermediary, only then should it be possible to interact with the production network via whitelisted connections, much like in the basic network segmentation case.

The security of production networks is greatly improved in this arrangement; even if the corporate environment is breached, an attacker must successfully exploit a jump host or compromise credentials that grant access to it before possibly interacting with production. The intermediary hosts, being themselves non-user machines, should be subject to much greater level security hardening, patching, and monitoring. Additionally, they can be subject to access measures such as MFA, time-of-use monitoring, and stricter antivirus policy than are typically employed on corporate user machines.

In the case of bastion hosts providing access to services, the intermediary should be used to detect potential exploitation activity through the use of a WAF (Web Application Firewall) or similar technology, depending on the service. This system is more secure, but is also not completely infallible. As an example, if an administrative user in the corporate network is compromised, an attacker could monitor for a legitimate connection by that administrator to the jump host, and then either simply steal that connection or potentially leak secrets and generate a new connection. Upon gaining access to the jump host, an attacker could then proceed as in the previous example.The complexity and therefore difficulty and resource requirements are increased, decreasing the likelihood of a successful attack as well as increasing the time for detection to possibly stop it.

Air Gapped Administrative Hosts

Because one of the highest risks to a production network involves the compromise of an administrative machine in the corporate network, an additional step that could be taken to increase security is to require all administrative traffic to originate from administrative systems that are not used for any other purpose, and are isolated from the corporate network as well as the internet. This increases security by requiring administrative file transfers to the production network to employ removable media and completely removes the ability for C2 (Command and Control) to use administrative systems, outside a selection of very unique and targeted malware. This solution is not often used as the restrictions placed on administrative systems in this case will often suffer from user workarounds such as illicit network bridging, as the security controls get in the way of efficient use of the network.

Attacks on a correctly implemented network of this type are both rare and very targeted; a breach of the production network is much more likely to occur from another vector, depending on the configuration of the rest of the network.

For additional information, visit www.nisos.com or contact info@nisos.com.