Fred Cohen & Associates - Analyst Report and Newsletter

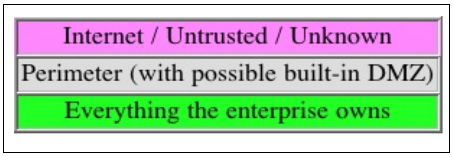
Welcome to our Analyst Report and Newsletter

Security Decision: Zoning your network:

Zoning of networks has become increasingly popular as an approach to separation in enterprise networks. The advantages of zoning come from an economy of scale related to using a smaller number of mechanisms to provide protection for a larger number of systems. In essence, a firewall is a way to aggregate protective function and risk in a single device which is more heavily managed than the end points it separates from other systems. In exchange for the increased cost of running the firewall, the effort to protect individual systems is reduced, and the amount of traffic sustained within the enclosure doesn't include the undesired traffic blocked by the firewall. If the firewall is inexpensive enough and the loss plus cost reduction in managing and operating the systems it protects is high enough, it is a good tradeoff. Taken to its logical conclusion, this means that the size of the zoned area(s) within an enterprise network can be optimized based on the reduced cost plus loss balanced against the cost of the zoning mechanism.

In taking on this design decision, architectural options should be explored. Here are some overarching approaches we have seen put in context:

No zone separation

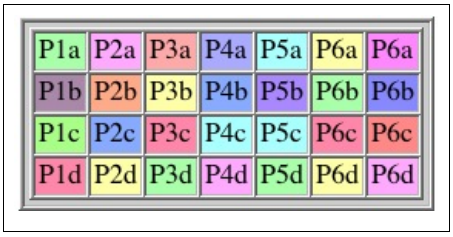


Most small businesses have relatively few computer systems and they all work together to facilitate the same effort. Separation takes time, effort, and expertise. Little physical separation is typically in place, little expertise is available, and the cost is substantial, so at best there may be an Internet network address translation firewall in most small businesses. The computer-related issues are typically not so great that adequate backups and restoration times of days are not devastating to the business, so the costs do not justify the benefits for complex network separation.

Several zones for different business functions

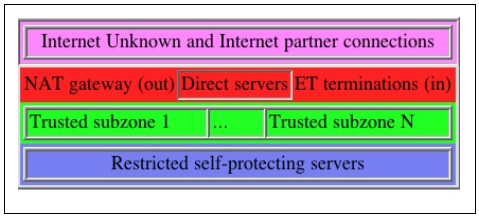
Several zones for different business functions typify medium sized businesses. They may have a manufacturing function, a financial function, a sales and marketing department, an HR department, and several other similar areas, each with its own user base and little common functionality crossing these boundaries. In this case, each department can have its own local area network (LAN) that runs more or less on its own. There is typically enough information technology expertise to allow for at least one full time employee dealing with networking issues and that employee can easily deploy a small number of internal network segments using VLAN technology, firewalls, or switch configurations to make the networks relatively independent of each other. This also limits the spread of viruses and reduces debugging.

Many small zones for individual projects



As the number of zones increase, the management complexity also increases, especially for enterprises that grow to larger sizes. Sheer numbers make departmental separation as the sole means of protection hard to do. The need for internal applications to more highly integrate drives less separation between departments and even more complexity in dealing with the interactions. The management complexity also goes beyond what can be handled by a single individual, necessitating more group efforts and more unified and standardized approaches. At some point the transition has to be made to the large enterprise model.

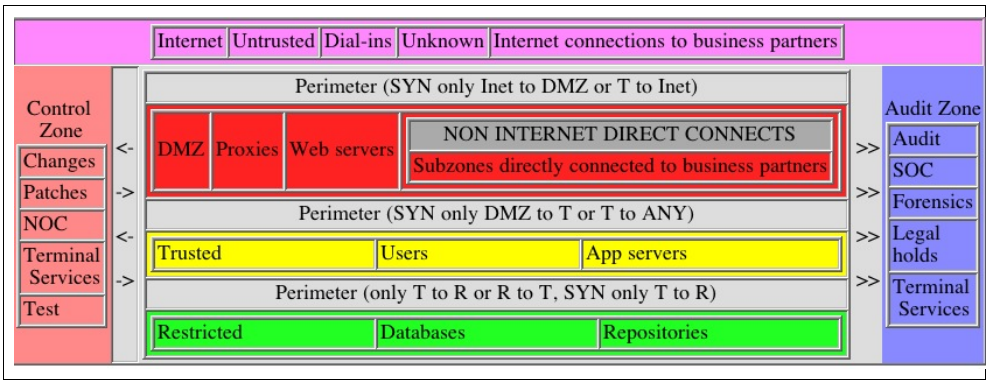
Limited zoning with trusted mechanisms



For organizations that have the ability to create medium and high surety special purpose mechanisms and in cases where those mechanisms are cost effective and/or improve reliability and/or availability, it is often more efficient and at least as effective to use higher surety mechanisms and place them directly in harm's way than to try to create larger infrastructures and support them in the hope that many layers of protection can be as effective as fewer layers of stronger protection. This is a tradeoff between fault tolerance and fault intolerance that more advanced organization often make. In these situations, commodity computers are put in subzones of the Trusted zone, which sits behind a NAT gateway and, optionally, allows inbound encrypted tunnels to contact internal assets. Direct servers provide direct Internet or external services and must protect themselves. Internal assets that need to communicate with Direct servers, do so through encrypted tunnels, usually through the NAT gateway, which is associated with an IP address for use by the Direct servers, which differentiate services based on this address as well as other mechanisms. Internal Restricted servers then protect themselves from Trusted systems based on subzoning and their own protective mechanisms. No internal perimeters are used other than possible Trusted zone separation mechanisms because self-protecting systems and servers have their own protective mechanisms adequate to meet the surety mandates.

A small number of layered zones with subzones

When enterprises are large enough to justify the time and effort of doing long-term zone architecture, they tend to have 6 major zones:



- An Internet zone that is untrusted
- A demilitarized zone (DMZ) for front-end servers that face the Internet
- A trusted zone where most workers work most of the time
- A restricted zone with high-valued databases and storage
- An audit zone used to retain audit records produced throughout the enterprise
- A control zone to control the network and manage its critical functions

Within these zones, which are typically separated by high complexity and heavily managed firewalls, reside subzones that are used for additional separation to limit the aggregation of risk, to group like with like, and to prevent outages or packet floods from interfering with other business functions.

Picking a zoning strategy

As a basic approach to determining the proper zoning strategy, we start with this decision:

> **IF** the enterprise is small and does not have differentiated services on dedicated platforms, **THEN** do not use zone separations,
>
> **IF** the enterprise is not large and has distinct enterprise-wide business functions, **THEN** use several zones for different business functions.
>
> **IF** the enterprise is composed of many small entities that work independently on different projects without centralized systems, **THEN** use many small zones for individual projects,
>
> **IF** the enterprise has the ability to build medium or high surety trusted mechanisms and costs or reliability favor such mechanisms, **THEN** use limited zoning with trusted mechanisms,
>
> **OTHERWISE** use a small number of layered zones with subzones for functional separation and risk disaggregation.

Of course this is a starting point, and not an end-point in architecting a zoning strategy for an enterprise. In many cases, combinations of these approaches are used. For example, large enterprises with a lot of expertise might well combine trusted mechanisms with the layered architecture, and many enterprises combine control and audit zones, despite the lack of separation of duties that result. Subzoning is also problematic for many enterprises and may involve complex renumbering of address spaces and VLAN design. This is often done as part of mergers and acquisitions, and the resulting complexity of large networks may make zoning a necessity for management purposes. Many large enterprises operate unzoned networks and pay a heavy price in network problems and have increasing difficulty in meeting regulatory and other similar external mandates for separation. And the worst of all worlds comes when companies have hundreds of internal firewalls, each custom designed for specific applications. In these cases they don't get the economies of scale that zoning can bring, and they also pay a heavy price in both equipment and operations.