Enterprise Cloud Network Architecture Risks

Introduction

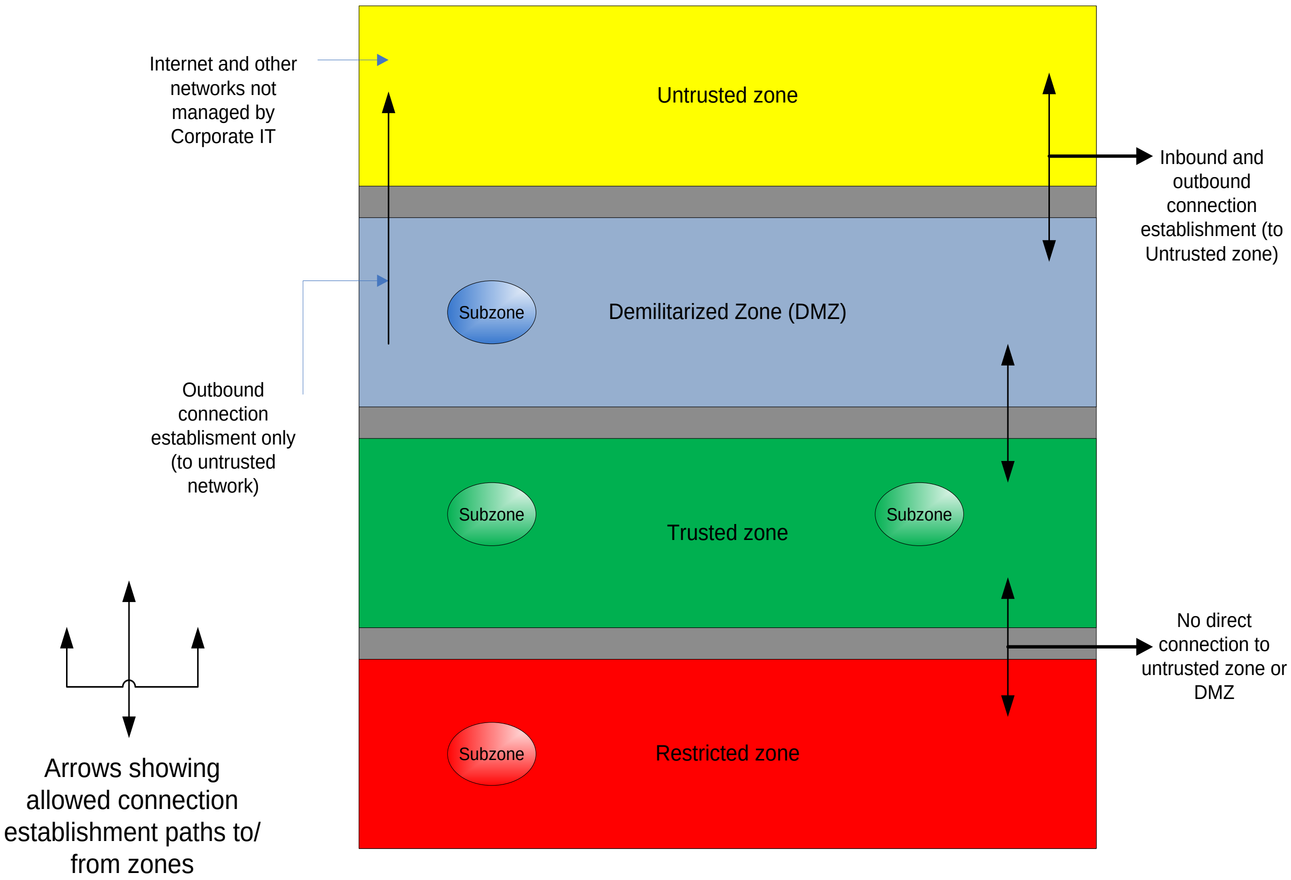
Today effective security network control is declining due to de-perimeterization, an emerging term used to describe the erosion of the enterprise firewall as a single point of control due to many trends including workforce mobility, smarter mobile devices, business partnerships, wireless access, Service Oriented Architecture (SOA) and Software as a Service (SaaS).

New technologies, products and services, customers, and user behaviors will continue to drive significant changes to our enterprise network infrastructures and its management.

Some of the more significant Enterprise trends that will continue to pose challenge to the Corporate Enterprise Network include:

1. Externalization: Use of IT productsand services outside of the enterprise
2. Consumerization: Desire of individuals to choose personal devices / services / apps
3. Democratization: Rise of social networks within / external to the enterprise
4. Business Process Transformation: Aligning Corporate people, process and technology iniatives more closely with the Corporate business strategy and vision.

Zones



Internet and other networks not managed by Corporate IT
Untrusted zone
Inbound and outbound connection establishment (to Untrusted zone)
Subzone
Demilitarized Zone (DMZ)
Outbound connection establisment only (to untrusted network)
Subzone
Trusted zone
Subzone
No direct connection to untrusted zone or DMZ
Subzone
Restricted zone
Arrows showing allowed connection establishment paths to/ from zones

Sample - Cloud Zoning Architecture

Zones are defined by the sequences of protective measures employed at their perimeters. Zones that do not allow direct connections from outside the organization are considered further inside the organization than zones that allow connections from the outside.

Zones that do not allow any traffic (inbound or outbound) to systems outside the organization are considered the furthest inside. In effect, the perimeter protections of a zone build on those of zones farther outside create a defense in depth.

Thus, as we move into the organization, the susceptibility of each zone to successful attack and exploitation from outside the organization is likely to be lower than that of each zone to successful attack and exploitation from outside the organization is likely to be lower than that of the next zone out on the ring of trust.

Conversely, outer zones are subject to more attach and must provide appropriate security for resisting those attacks.

However, all else being equal the larger the zone, the more risk of unauthorized penetration. For many organizations, replacing the “flat-network” architecture (i.e., where a small number of centralized firewalls control access to thousands of end user devices, offices, etc.,) with a logically and physically sub-zoned network is the answer.

The replacement strategy is to retract the network firewalls that really matter to the data center edge, equip endpoints to self protect, but don’t trust them too much.

Risks

1. Political considerations require strong sponsorship and clear (initial funding).

2. Multiple stakeholders and IT groups will need to be involved.

3. Technology risk associated with being an early adopter:

4. Standards are immature, and few organizations have deployed cloud network architecture.

5. Vendor product roadmaps are aggressive, and product cycles are accelerated.

6. Interdependencies lead to complexity; will require careful planning
    a. Multiple interdependent IT initiatives’ create potential for project slippage delays.
    b. Prioritize foundational projects to lay groundwork.
    c. Troubleshooting is more complex when so many changes are being made over a relatively short period.

7. Multiple solutions can lead to inconsistent controls:
    a. A combination of technical approaches may be needed to support all of the identified use cases.
    b. Each approach involves an administrative process for defining and managing controls, which could get out of synch.

8. Trade-off between secure communication and policy enforcement:
    a. Encrypted traffic may prevent inspection and enforcement of controls needed for compliance.

9. Risk of malware from unmanaged and lightly managed endpoints continues to increase:
    a. NAC-style scanning and enforcement may be needed.

10. Maturity and migration risks:
    a. Some of the technical mechanisms have seen limited use and may experience typical early product life cycle problems.

11. Support for the added complexity involved with mixed IPv4 and IPv6 will be required for a long time.

Characteristics of the Cloud Network of the Future

While perimeter defenses may remain in place, they will play a lesser part of the overall protective function and become more distributed. Above depicts scenarios in which the combination of network firewalls and security overlays allows implementation of a typical zone model across the multiple organizations, sites, users and mobile devices that perform the work of the enterprise.

While cautioning that much of the vision of de-perimeterized is not yet practical, there is a clear value in adopting a layered model approach as a targeted security model for the future. The reality of de-perimeterization shifts the emphasis on risk mitigation and investment in policy enforcement mechanisms to resources-hosting systems and applications.

Fundamentals

1. The scope and level of protection should be specific and appropriate to the asset at risk.
    - Business demands that security enables business agility and is cost-effective.
    - Whereas boundary firewalls may continue to provide basic network protection individual systems and data will need to be capable of protecting themselves.
    - In general, it’s easier to protect an asset the closer protection is provided.

2. Security mechanisms must be pervasive, simple, scalable, and easy to manage.
    - Unnecessary complexity is a threat to good security.
    - Coherent security principles are required which span all tiers of the architecture.
    - Security mechanisms must scale; from small objects to large objects.
    - To be simple and scalable, interoperable security “building blocks” need to be capable of being combined to provide the required security mechanisms.

3. Assume context at your peril.
    - Security solutions designed for one environment may not be transferable to work in another. Thus, it is important to understand the limitations of any security solution.

4. Problems, limitations, and issues can come from a variety of sources, including geographic, legal, technical, acceptability of risk, etc. Devices and applications must communicate using open, secure protocols.
    - Security through obscurity is a flawed assumption - secure protocols demand open peer review to provide robust assessment and thus wide acceptance and use.
    - The security requirements of confidentiality, integrity, and availability (reliability) should be assessed and built in to protocols as appropriate; not added on.
    - Encrypted encapsulation should only be used when appropriate and does not solve everything.

5. All devices must be capable of maintaining their security policy on an un-trusted network.
    - A "security policy" defines the rules with regard to the protection of the asset.
    - Rules must be complete with respect to an arbitrary context.
    - Any implementation must be capable of surviving on the raw Internet; e.g., will not break on any input.

In the Cloud - The Need for Trust

All people, processes, and technology must have declared and transparent levels of trust for any transaction to take place.

- Trust in this context is establishing understanding between contracting parties to conduct a transaction, and the obligations this assigns on each party involved.
- Trust models must encompass people / organizations and devices / infrastructure.
- Trust level may vary by location, transaction type, user role, and transactional risk.
- Mutual trust assurance levels must be determinable.
- Devices and users must be capable of appropriate levels of (mutual) authentication for accessing systems and data.
- Authentication and authorization frameworks must support the trust model.

Identity, Management, and Federation

Authentication, authorization, and accountability must interoperate / exchange outside of your locus / area of control.

- People / systems must be able to manage permissions of resources and rights of users they don't control.
- There must be capability of trusting an organization, which can authenticate individuals or groups, thus eliminating the need to create separate identities.
- In principle, only one instance of person / system / identity may exist, but privacy necessitates the support for multiple instances, or one instance with multiple facets.
- Systems must be able to pass on security credentials / assertions.
- Multiple locations (areas) of control must be supported.

Access to Data

Access to data should be controlled by security attributes of the data itself.

- Attributes can be held within the data (DRM / metadata) or could be a separate system.
- Access / security could be implemented by encryption.
- Some data may have “public, non-confidential” attributes.
- Access and access rights have a temporal component.

Data privacy (and security of any asset of sufficiently high value) requires a segregation of duties / privileges.

- Permissions, keys, privileges, etc. must ultimately fall under independent control, or there will always be a weakest link at the top of the chain of trust.
- Administrator access must also be subject to these controls.

By default, data must be appropriately secured when stored, in transit, and in use.

- Removing the default must be a conscious act.
- High security should not be enforced for everything; “appropriate” implies varying levels with potentially some data not secured at all.