



ZERO TRUST NETWORKING RECONSTRUCTING NETWORK SECURITY

MAKING EVERY HOP SECURE

SUGAM RANGAN

Happiest Minds

Introduction **03**

What we do in "Zero Trust Networking" **04**

How we do "Zero Trust Networking" **05**

Single Trust Zone **06**

Dual Trust Zone **07**

Zero Trust Zone **08**

Four Dimensions - Zero Trust Building **09**

System/User Identification **10**

Traffic Movement Surveillance **11**

Design Zero Trust Network with Zero Trust Policies **14**

Monitor and Support **14**

User and System Behaviour Analytics **15**

Zero Trust Conclusion **15**

Introduction

This white paper explores modern Zero Trust Networking approach ensuring minimal threats on your network and aiming for higher security zones.

What we think is secured can be an open gate for others to enter the confidential or private zone where our data resides. Our sentinels may not be sufficient to overlook or protect our data until we fix the strategy of their positioning and deployment.

Can we protect our Data, Applications and Network 100% in today's time? Maybe not, but we can reduce the threat exposure of our Digital Infrastructure if we adapt the Zero Trust Networking Methodology.

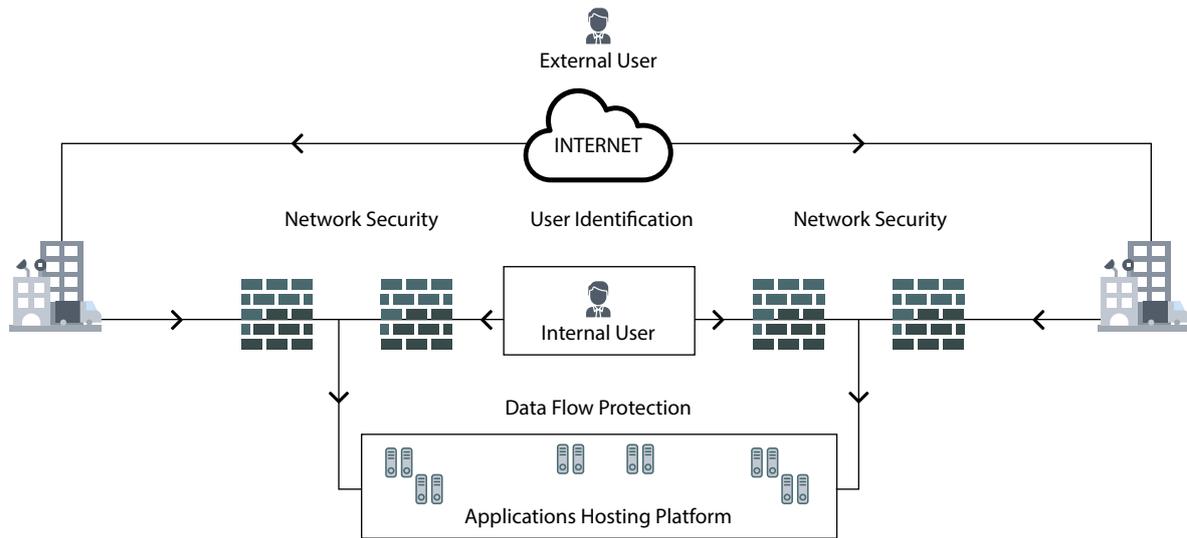
What is Zero Trust Methodology?

Zero Trust Methodology is where we trust no one and consider everybody as a threat for our Digital **Infrastructure** be it an external or internal user. Everybody is moving to next-generation security equipment's, but we must think for an effective approach to protect our data and applications that are exposed directly or indirectly.

Let's take a quick example, the figure shown below depicts two type of data users,

- 01 The external users who connect through a public network for accessing the application for which organizations usually do an inspection to avoid threats and attacks.
- 02 The internal users who connect through the office network, and whom we usually trust for not being an attacker.

Are we saying, consider employees of the organization as an attacker too? No, not at all. While we can trust our staff, we can't trust the digital platforms that they use today to get their jobs done.



Zero Trust Methodology marks everything as a threat holder irrespective of its location.

It might be an intentional attack or non-intentional one, however, in both scenarios, the major impact is on the data of organization. This document will explain how we can avoid maximum threats by applying Zero Trust Networking Methodology.

What we do in “Zero Trust Networking”

Maintaining Zero Trust Networking in any Infrastructure hierarchy is very important, and it becomes necessary to know what we do in this space to keep the Infra on high security.

While securing any data holding platforms it is all about resisting the exposure of the platform to threats. It doesn't matter whether the threat is residing externally or internally, protecting the platform from these attacks from both the directions is priority. We can secure these platforms in a simple and better way through network segmentation.

Network Segmentation is an excellent way of achieving Zero Trust Networking. Rather than having too many layers at network security, we can segment the network in a better way. Considering that the internal and external users possess threats to the data platform, network segmentation limits the flow of traffic by limiting the reach of the destination the user.

Segmentation Says, “Let’s have reachability only to what is required”, let’s not reach or allow to connect a Servers and data platform which is unintended for any user’s direct communication. We will read about the same in “How we Do it”.

Network Segmentation is one of its way of moving towards Zero Trust Networking. However, it's essential to follow a few more factors to deploy this practice to its best capabilities. Some of the most demanding factors of Securing Data today is:



User/System Identification



Data Flow Marking



Hybrid trust Policy -
Secure Architecture



Monitoring



Maintain and Upgrade

How we do “Zero Trust Networking”

As we understand, Zero Trust Networking is about considering every zone and user untrusted and non-secure. It is now good to understand how we deploy Zero Trust Networking. We have already mentioned the ways of achieving Zero trust Networking in the above section and in this section we will be detailing the boundaries of each category.

Before that, we should understand how all these methods work, and we should also understand the below defined network boundaries:

Single Trust Boundary

Dual Trust Boundary

Zero Trust Boundary

Every boundary has its secure trust Topology, and these models are driven from a legacy network to Zero Trust Secure Network in the last many years. All these boundaries carry a percentage of exposure on various network zones as below:

Internal Zone

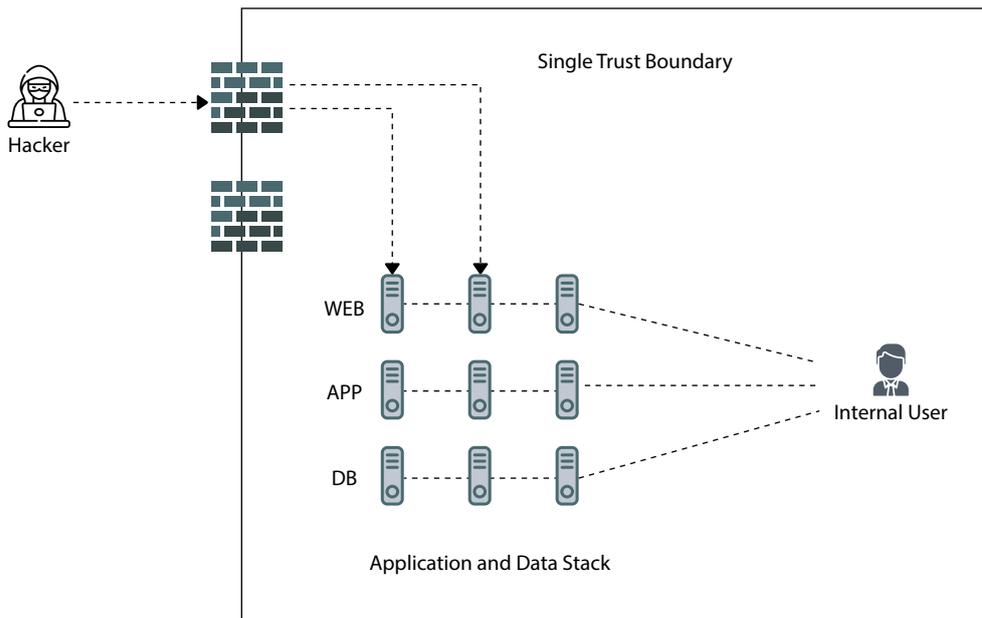
External Zone

Data Zone

Now let's take a deeper look at the different types of trust zones.

Single Trust Zone

In Single Trust Zone, we usually protect the perimeter edge of any IT infra to protect it from outside (Public Internet) Attackers. However, the internal users may not have any Security layer between Application - Server stack and Users. Let's take look at the diagram below:



In the image above, there is a stack of nine servers, hosting different services on each layers. Where the first layer is hosting the WEB, and the rest two layers are hosting the APP and DB services.

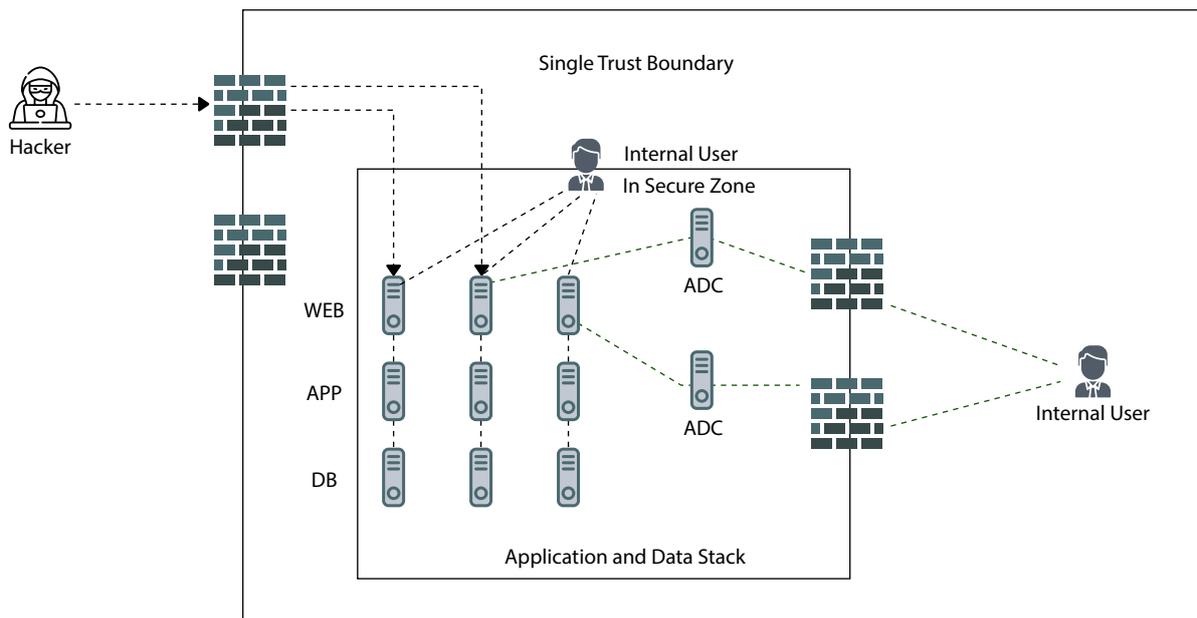
When an external user/attacker tries to connect with the application hosted on the shown stack, the services will only open to connect with the web layer, and the configuration will not allow the attacker to access any other layer in the stack. This means, the application is exposed to the webserver to the external world, and from the external world this infra is 22% vulnerable. (2 servers out of 9 Servers = 22%)

Similarly, if we try to check for internal network reachability, a user sitting on an internal network can reach any of the service in application stack which makes the internal infra 100% vulnerable.



Dual Trust Zone

In Dual Trust Zone, we usually protect the perimeter edge of any IT infra to protect it from outside (Public Internet) attackers. Here we also make an internal layer of security between User and Application/Data Stack. Let's look at the diagram below:



In the image, there is a stack of nine servers. We are hosting different services on different layers. Where the first layer is hosting the WEB, and the rest two layers are hosting the APP and DB services.

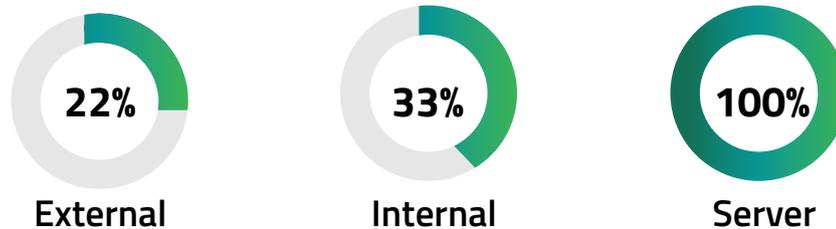
For the external users (Hackers), it is the same scenario. When an external user/attacker tries to connect with the application hosted on the shown stack, the services will only open to connect with the web layer, and the configuration will not allow the attacker to access any other layer in the stack.

This means, the application is exposed to the webserver to the external world, and from the external world this infra is 22% vulnerable. (2 servers out of 9 Servers = 22%)

Now, if we try to check for internal network reachability, a user sitting in the internal network have a layer of internal firewalls too, and he can only reach to ADC server to get connected with the web applications. In which case, the users get accessibility to only the first three web app server layer. This drastically reduces the threat exposure of the infrastructure by 33% from the internal users.

However, if we see a user sitting in a secure zone, as shown in the above diagram, he is again able to reach all the servers. Such kind of users are either present on the inside zone because of incorrect configuration of VLANs or Gateways and can be admin too. Which, makes the internal servers and the infrastructure vulnerable by a 100%.

Now let's look at the numbers again for Threat exposure calculation:

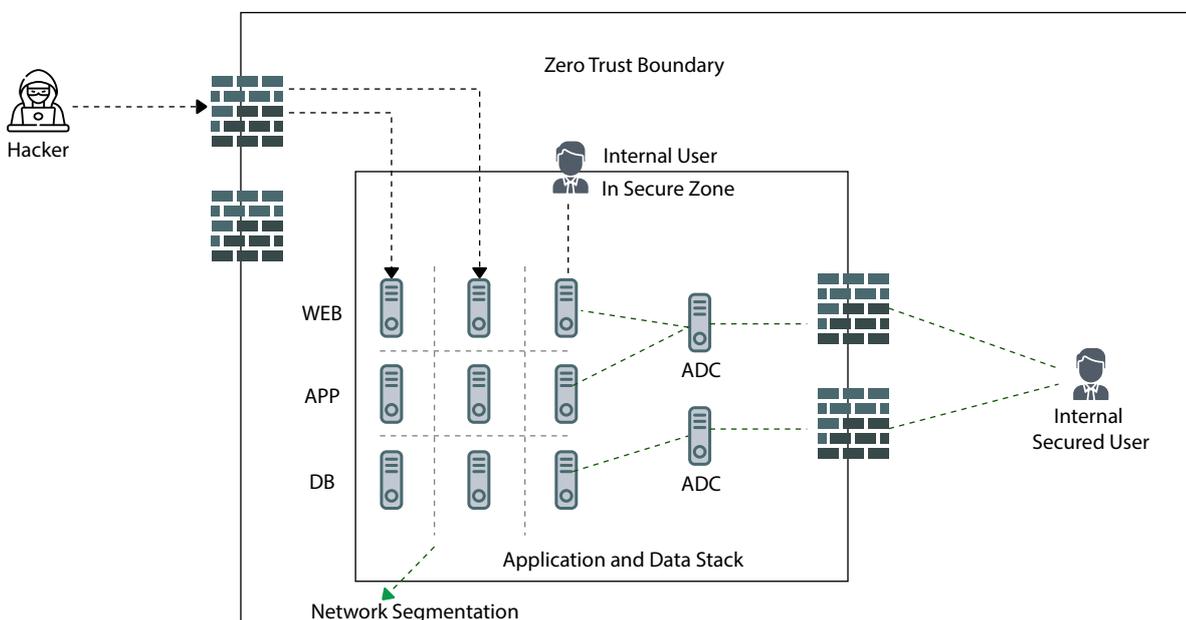


Zero Trust Zone

While we saw a great reduction of threat exposure on the internal network after adding the dual layer of firewalls, the server level threat still stayed at 100%.

To solve this, the concept of Dual Trust Zone or Dual Trust Networking was developed that reduced the threat exposure to minimum and made the infrastructure most secure than it was from ever before. As I mentioned earlier, any organization or admin cannot secure the Digital Infrastructure completely. Still, Dual Trust Networking can take us to maximum possible security level and minimize exposure to threats.

Let's take a look at the Diagram below:



Now analysing the same set of stack with ADCs in place and let's shift our focus to the most important factor call "Network Segmentation".

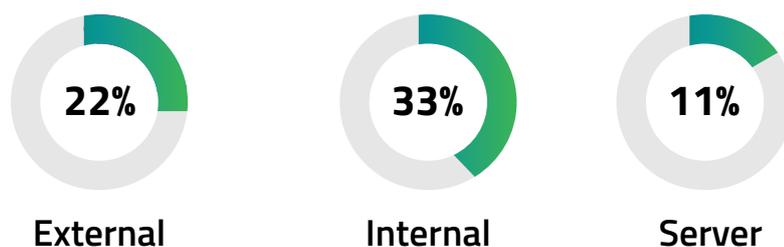
For the external users (Hackers), the scenario doesn't change. When an external user/attacker tries to connect with the application hosted on the shown stack, the services will only open to connect with the web layer, and the configuration will not allow the attacker to access any other layer in the stack.

This means, the application is exposed to the webserver to the external world, and from the external world this infra is 22% vulnerable. (2 servers out of 9 Servers = 22%)

While, the internal network reachability, the user sitting internally has a layer of internal firewalls too, and he can only reach to the ADC server in order to get connected with Web Applications. In which case, the users get accessibility to only the first three web app server layer. This drastically reduces the threat exposure of the infrastructure by 33% from the internal users.

But the best part comes here, with Network segmentation, user sitting in the secure zone (as shown in the above diagram) is now only able to reach one of the server hosting- web app on the server layer. By doing so, the service level segmentation created across every server in the application stack enables the communication between servers on the required channels and ports in the App stack. However, direct user access is stopped on the first web server itself. Which, reduces the threat exposure to the server layer to 11%, which is a huge reduction if we compare with the last two scenarios, where it was 100%.

Now let's look at the numbers again for Threat exposure calculation



Four Dimensions - Zero Trust Building

Let's take a quick look at the figures we calculated in our last sections:

Domain	Single Trust	Dual Trust	Zero Trust
External	22%	22%	22%
Internal	100%	33%	33%
Server	100%	100%	11%

Now that we agree that Zero Trust has minimum threat exposure and is the safest strategy to adopt, let's discuss on how can we build a Zero Trust Zone which comes along with the Four Dimensions Solution and covers the key points below:



System/User Identification



Traffic Movement Surveillance



**Design Zero Trust Network with
Zero Trust policies**



Monitor and Support

With all these Four Dimension Pillars, each Security Domain gets covered under them. When you try to secure any Data or platform, it always starts with the strategy of Risk/Threat holders' elimination. If we eliminate the things which can impose threats to Data Platform, we do direct Mitigation of the Risks.

System/User Identification

Our whole System/User **Identification management** world works around three key Security Principles below:

Identification

Authentication

Authorization

While a user can still have reachability to a lot of platforms, it won't work until a user have a correct set of permissions. User must pass through the stages mentioned above to ensure he is authorized to make a good or bad impact on the system. If we manage to control access of all platforms in a well-defined structure, we reduce the threat risk from internal/external users.



However, an application hosted on the same system can be accessed by all, which again imposes threats from both internally and externally. If you remember, we talked about the segmentation of the network, and none of the users can directly reach any other server or application on DB or APP layer. That's because we allow the webserver to talk to those layers via Web APP in a secure way.

Now, if a web app tries to communicate with the database, it should also happen in a well-secured manner. This is where mutual TLS connections come into picture when both sides verify their identity. To have data exchanges, these apps are bounded to communicate on encrypted channels. Those channels only open when the right set of Certificate Exchange takes place between both the systems. Hence making it more secure.

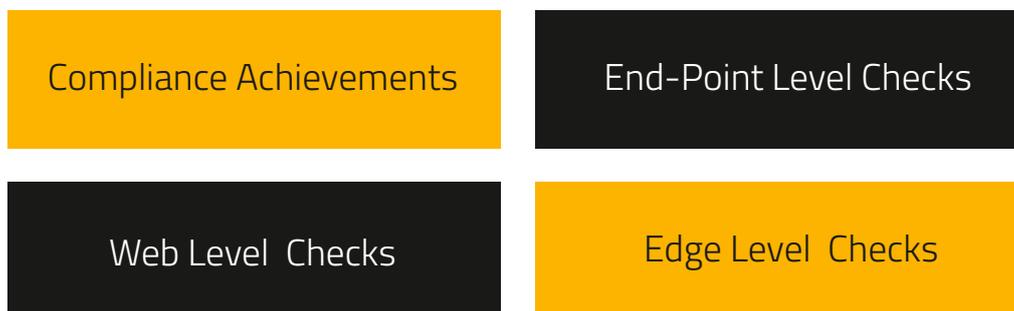
So now, it doesn't matter if you are a hacker or an internal user sitting on a network. Unless you have correct identification in the form of certificates, you can't get into the database.

While we have talked about security principles and certificate exchange, the other most important and easy to deploy method for user identification is MFA (Multi-Factor Authentication). Solutions like DUO, RSA, OTP and OKTA have made the process simpler today by giving an option of soft token for user authentication. Rather than allowing a user with single UID and Pass into the system, we can do dual authentication before landing to the main page.

Traffic Movement Surveillance

When we are talking about building a Zero Trust Network, it is not just about securing one platform or any application data, it is actually about securing the whole organization, and the data that resides within the organization. Be it a server, database, user-machine or any application, it is important to keep an eye on the data traffic movement from any machine.

This is where traffic movement surveillance comes into picture. IT traffic movement surveillance can be done with the help of many techniques. Some of them are listed below:



Can we protect data or secure the organization just by installing a lot of technology boxes? Maybe not, the **Data Security** & Preservation starts with complaining about the required standards and regulations necessary for an organization. While we know, many new rules are coming into places where individual's/personal data sharing across the countries or continents has become a real concern. To prevent the data breaches and customer data leaks, organisations need a robust security posture along with being complaint in nature too. While following standards and compliances can be very important, there is an additional set of security achievements required too. Let's take a look at the other three important factors.

End-Point Level Checks

We should understand that every **risk** starts or ends with an end-point, therefore it is important to secure the end-point first. In the market, we have lots of End Point security solutions, and every solution has its own moto. Be it, Malware protection, Data Leak Prevention, Mobile Security, Email + Web Protection, if we can make a user workspace secure, it can eliminate the number of threat holding risks from the End User Infra.

Web Level Checks

Today organizations understand that end level security systems cannot process a lot to secure their Data present on the systems which are travelling along with the users in the outside world. While work from anywhere option has become so easy for all of us with great connectivity solutions, it's very important that remote working should be protected more stringently.

When a user is inside the organization, they have a lot of security infrastructure in place to check, filter and act upon data movements. However, it really becomes uncontrollable when a user moves to the outside world and is sitting on an open internet full of threats.

Now we have an option of web security or web proxy with this any agent on open internet can still create a session with web-based proxy gateway. All traffic moves to that gateway before going to open internet, and hence it creates a layer of protection to ensure that the data movement happening is not insecure. While everything is accessible in an open network, it is still under observation and can be acted upon with the help of a set of permissions. Hence, the user may not be able to access to websites or applications which are listed to be malicious or insecure as per the web protection systems.

Edge Level Checks

This can be a favourite topic for any network security engineer. We should not even think of using legacy / Traditional Network Security Devices - Firewalls which works only on Layer 2 – 4.

Where in earlier days we had to install IPS and IDS separately, today we have next-generation firewalls. These firewalls not only works on stateful inspection concept, but also covers up all the important security layers factor to ensure safe movement of data across the segmented network.

While segmenting the network for achieving Zero Trust Security, next-generation firewalls plays a vital role. All next-generation firewalls can do:

Layer 2-7 Inspection: While most of the attacks are happening on all layer these days, a next-generation firewall helps us in determining whether the transferred traffic is malicious or not.

Application Layer control: The firewalls are now capable of working over and above layer four. Inspection on the layers 5-7 gives more application-level control to evade the attacks.

Stateful Inspection: While traditional firewall can do stateful inspection till layer 4 only, next-generation firewalls can inspect traffic on all layers allowing the possibility of creating extremely defined policies.

Deep Packet Inspection: Apart from Packet's header, footer, source and destination check, the next-gen firewalls allows to check the data level information as well by finding unwanted statements and based on already defined principles of search. Based on the content, traffic can be paused or stopped.

Intrusion Prevention System: The main job is also with IPS part of the firewall in detecting the attacks after analysing the data with threat signatures. Known attacks from an existing database and advances behavioural learning.

Sandboxing: Any new unknown threat which cannot be detected with existing firewall features with pre-loaded/ cloud available data for comparison, sandboxing is the feature to monitor the behaviour of suspicious programs by quickly stimulate it in the system.

SSL Inspection: These days, most of the data movement happens in an encrypted format, and we know almost all applications are secure today. Hence for the firewall it is important to understand the data resides in the packet and hence firewall uses the SSL decryption capability to read the content inside the packet and finally marking it as safe or dropping the same.

No Performance Degradation: After fitting all these options in a single box, the processing surely goes up and hence if we were using a traditional firewall for 100 users and now we have a next-gen firewall in place of it, the CPU processing on all levels and instances should be more than traditional firewall to perform all the operations.

Design Zero Trust Network with Zero Trust Policies

With all the available security solutions, one best suited Zero Trust Network can be designed for the organization. However, what's is more important here is to know what is configured in all those security solutions. Take an example of next-gen firewall, and this firewall is of no use if even after deploying it to the network we are not using or enabling its next-generation feature licences. Or using an email protection system with a default configuration which is not suitable for your kind of organization.

Or using a web proxy solution however even if we set up the customized security policies on the time of installation if we do not keep on updating it based on our observations and monitoring, its again is of no use. We must keep on updating the polices based on new threats and observations coming out of the analysis.

Monitor and Support

Once all the required solutions are deployed, it is necessary to do continuous monitoring of threats and traffic movement across the platforms to keep on evolving based on observed patterns. It is also important to upgrade the firmware and existing modules to the latest version, which can help us avoid the vulnerabilities in the protection systems.

Experts on monitoring job will always keep an eye on all the systems and take preventive measures accordingly. Especially the latest tools and systems working on AI/ML and automation helps us in automating a lot of the monitoring tasks and taking corrective actions on its own without human intervention. Hence this is the perfect time for the organizations to explore in the directions that they never looked.

User and System Behaviour Analytics

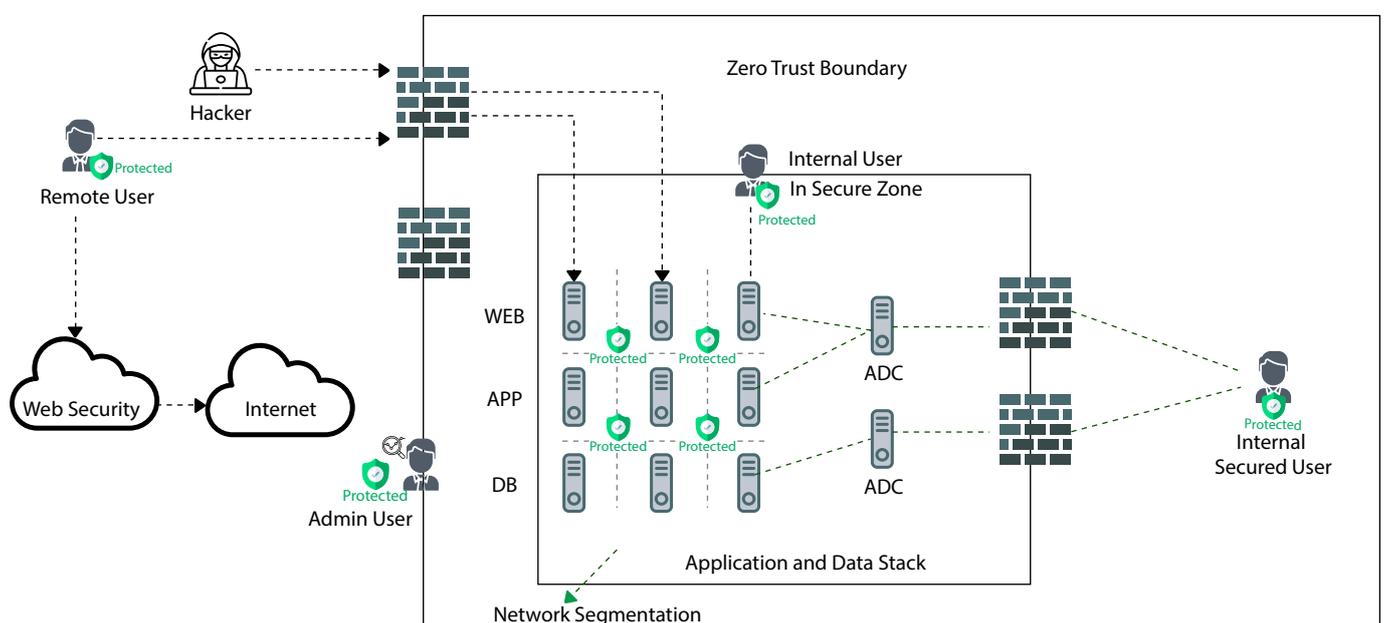
It's all about checking the behaviour and then picking up the activities that look strange and can be reported as a security incident. UEBA tools which work on User and Entity Behaviour Analytics (UEBA) helps us achieve the same. Understanding the behaviour of system to system, user to system and user to user communication is very important to avoid threats on any of the layers.

Zero Trust Conclusion

We all know the modules which are available and should be used to create zero trust security boundaries. Choosing the correct module based on the need of your organization is the most critical factor to avoid attacks and threats.

Also, some of the modules should never be skipped like end-point protection, and transactions flow monitoring which helps the organizations and platforms to stay secure on the ground level.

Let us try to imagine now on how a segmented network with various security options can help us in achieving Zero Trust Security.



We have seen a Zero Trust Network Model, which was described in section 3.3, and now all the end-users are protected with end-point security. All firewalls are next-generation firewalls and doing layer 2-7 filtration. The whole network is segmented into various security level boundaries, making threat exposure minimum. All remote users are protected with web proxy/security solutions, even when they are working from outside of the organization.

If we intend to create a network with minimum threat exposure, it is possible. We cannot eliminate threats 100%, but with the correct combination of Zero Trust Architecture, security measures in place and by updating the policies and architecture time to time and by keeping things under observation, we can prevent threats to our organization and data platforms.

Author Bio



Sugam Rangan has over 12 years of experience in Telecom and Enterprise IT services. He has spent Years working on Managed Network Operations Services, Planning, Designing, Consulting and Technical Pre-sales. He is currently a part of Infrastructure Management and Security Services business unit in Happiest Minds Technologies Pvt Ltd and working as a Technical Manager. He is responsible for handling Network Practice strategies, Solutions Offerings Development, Consulting and Pre-sales activities. Sugam has wide-ranging interests in Network Security, Data Center, automation and emerging technologies

Business Contact business@happiestminds.com

About Happiest Minds Technologies

Happiest Minds, the Mindful IT Company, applies agile methodologies to enable digital transformation for enterprises and technology providers by delivering seamless customer experience, business efficiency and actionable insights. We leverage a spectrum of disruptive technologies such as: Big Data Analytics, AI & Cognitive Computing, Internet of Things, Cloud, Security, SDN-NFV, RPA, Blockchain, etc. Positioned as "Born Digital . Born Agile", our capabilities spans across product engineering, digital business solutions, infrastructure management and security services. We deliver these services across industry sectors such as retail, consumer packaged goods, edutech, e-commerce, banking, insurance, hi-tech, engineering R&D, manufacturing, automotive and travel/transportation/hospitality.

Headquartered in Bangalore, India; Happiest Minds has operations in the U.S., UK, The Netherlands, Australia and Middle East.



Born Digital . Born Agile

www.happiestminds.com