BORDERLESS SECURITY

WHY ZERO TRUST NETWORKS ARE THE NEW ESSENTIAL FOR TODAY'S ANYWHERE OPERATIONS

At a glance

- The evolution of networking
- What is a zero trust network (ZTN)?
- Why ZTN?
- How to transition smoothly to a ZTN?
- Questions to ask when starting your ZTN journey

A zero trust network (ZTN) is an internet-based intranet using which identities securely access apps as per defined policies.

Introduction: Time to evaluate security and performance gaps

No one could ever have predicted how 2020 would see such a drastic alteration in how people work and interact. This rapid shift has put tremendous pressure on CIOs and network administrators to enable new ways of working and accessing enterprise networks. The urgency of change has inevitably challenged even the most robust security protocols, increasing risk and aggravating existing performance issues such as increased latency.

In this paper, we'll look at how networking has evolved over time and how today's new paradigm demands advanced digital security strategies. We will also explore how zero trust networks (ZTNs) contribute to it – and what organisations need to consider before adopting a zero trust network approach.

The evolution of networking – and where we are now

Remember when work only happened in the workplace? Users and their devices were based exclusively within offices, with applications hosted in corporate data centres. In this discreet environment, assuming mutual trust between an app and its users made perfect sense; and MPLS worked well for users to access corporate applications.

Application and user landscape experienced a shift as a result of business demand for agility, user performance, and lower capex investments, Apps started to move to hybrid data centres on virtualised environments and users became mobile. Internet connectivity took precedence over MPLS and assumption of mutual trust between user and app became irrelevant and demilitarised and militarised zones concept gained momentum.

Then the pandemic hit.

Almost overnight, the vast majority of users stopped going to the office and began to work from home. Far from being a temporary, emergency measure, this has become the new normal. Even as restrictions lifted off over the past months, only a fraction of workers had returned to the office while the majority still continue to work from home for the foreseeable future. They will continue using the Internet to connect with cloud-hosted apps via their own devices, whether desktops, laptops or tablets. In this new world, perimeters have completely vanished.

Around the world, organisations are facing the challenge of maintaining security and uninterrupted access for apps and their users, while keeping a lid on capital investment. From this perspective, zero trust networks are a natural next step.

What is a zero trust network?

In simple words, a zero trust network (ZTN) is an internet-based intranet using which identities securely access apps as per defined policies. Bear in mind this is not a VPN or other traditional internet-based intranet with the usual defined perimeter, latency and agility issues – as we are about to see.

Here's a closer look at the key components of ZTN:

Micro segmentation

There is separate segment for every application and users use it to access the particular apps. This helps to isolate the segment during an attack, so the attack stays contained within the segment and stops lateral movement.

Relative trust

ZTNs in enterprise networks have a default networking security posture of default deny. Systems are hardened and isolated until a level of trust is established, before enabling network connectivity. The trust is not an absolute parameter but a relative one, so it's continuously monitored, assessed and adapted.

Session-based authentication

Every initiated session is challenged for authentication at an advanced level using PKI, host checker or adaptive trust. Sessions are end-to-end encrypted using advanced protocols such as AES 256.

Agent and agentless access

These are supported for either using client or browser.

Configuration and control

Administrator can handle administrative tasks via an orchestration layer. Role-based access control enables users to view, edit, add or delete content according to their access permissions.

Real-time monitoring

Web-based dashboards allow admins to monitor user and app parameters, such as bandwidth utilisation, number of sessions, etc.

Third party integration

Support for API and SDK is key for integrating with third party applications and tools.

Why should enterprises adopt a ZTN strategy?

ZTNs offer distinct advantages over existing network strategies, at all levels:

Users and networks

- Users are no longer stationed in offices and are working from home, thus, layer-3 based authentication is no longer relevant. User should be authenticated using location, time of the day, device ID, etc.
- As connecting back to office-based VPN gateways increases latency and diminishes the user experience. So, it makes sense for users to connect to apps directly using the nearest software-defined agile PoPs.
- Application of same policies across entire VLANs does not work well in changed application landscape and it should be application-specific policy.
- Demilitarised zones have either full or no trust. Now, trust has to be adaptive and evolve with time – ZTNs enable this.

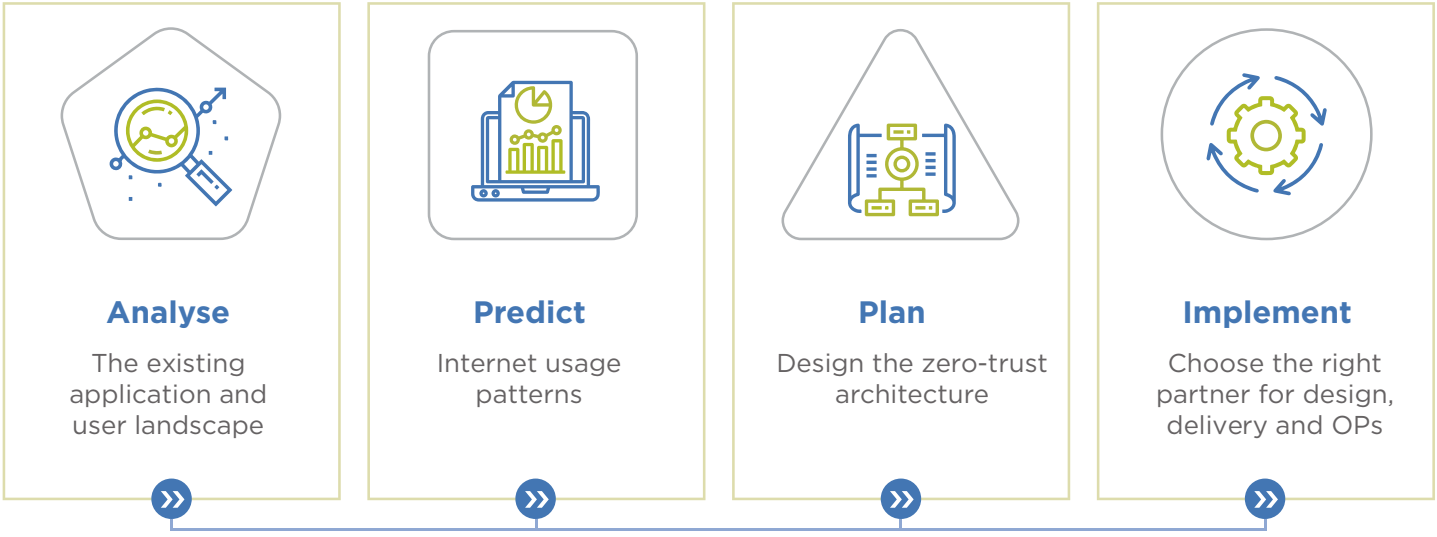
IT Service Management (ITSM) and reporting

- Manual intervention required to contain and remediate an incident, and this resulted in increased overall mean-times-to-detect and respond (MTTD and MTTR). Automation through incident response (IR) solutions such as Security Orchestration, Automation and Response (SOAR) results in reduced MTTD/ MTTR.
- Enterprises have invested in ITSM tools and look forward to integration with various security controls. The API and SDK-based integrations can enable it.
- The network level reporting is not sufficient for decision making. Real-time reporting at app and user levels offered by ZTN increases visibility to enable informed and faster decisions.

Analytics

- Anomalies were traditionally detected on the basis of static rules. The rise in new Indicators of Compromise (IOCs) demands dynamic intelligent detection. Hence contextual, real-time anomaly detection is becoming the norm.

How to transition smoothly from ‘as is’ to ZTN



Get your ZTN adoption off to the right start

As you evaluate your journey towards ZTN adoption, here are a few basic questions you'll need to answer:

 **Applications**	• What type of apps are there, and how many? • Where are they hosted (e.g. private or public data centre (DC), etc.)? • Are they all accessible via the Internet? • Any performance issues? If so, what are they?
 **Identity**	• How many users are there? • How many work from home, how many from the office? • Where are they? • How long do they spend logged in to apps? • Is a split tunnel used for browsing? • What type of authentication mechanism is used? • What types of devices are used by those working from home and those working from the office? • What is the device make and OS version for each?
 **Connectivity**	• What kind of connectivity is used for Infrastructure as a Service (IaaS) and apps hosted in private DCs? • How many locations use Multi-protocol Label Switching (MPLS)? Are any apps hosted at any of these?

 **Security**	• Do a posture check as follows:
	  ° What anti-virus availability do you have?
	  ° Is the device software-hardened?
	  ° Are the latest patches updated?
	  ° Is mac-binding in place?
	• What level of Role-Based Access Controls (RBAC) to the apps does the user need?
	• Is 2FA enabled as an add-on authentication layer?
	• How long should logs be stored? Maintain a log trail for forensics.
	• Is there SIEM integration for correlation and analytics?
	• Have you integrated an endpoint detection and response (EDR) solution?
	• How does traffic break out to the Internet? Via a split tunnel at user level, or from cloud gateway nodes?
	• What security controls do you need for internet browsing, e.g. firewall, proxy, Data Leak Prevention (DLP), sandbox?

Why it pays to partner with a Managed Security Service Provider (MSSP)

An MSSP has the expertise, scale and capability to design and deliver a ZTN that integrates with your existing network infrastructure. You benefit from the performance, agility and security ZTNs provide, without the burden of heavy capital investment.

Key components

- Endpoints / gateways for desktops / mobiles / locations / cloud
- Transfer nodes for relay of data
- Session controller via an orchestration layer
- Network controller via a control pane

Five layers of security

- Embedded software firewall
- Authentication
- Least privilege access
- Dark network using transfer nodes
- End-to-end encryption: AES 256

Multiple integrations

- API to integrate with third party tools
- SDK to embed into apps
- Posture check
- Endpoint detection response
- 2FA as an additional layer of authentication
- SIEM for log correlation and anomaly detection
- Threat intelligence

Conclusion: ZTNs are the new essential – but you need the right partner

An effective ZTN will close up the security and performance gaps that have inevitably opened up with the recent, seismic shift to more mobile ways of working. But its success relies on ensuring its design matches your existing infrastructure. That's both possible and viable with the right partner.

As an MSSP, Tata Communications has adopted a ground-up approach and developed a ZTN product from scratch. It's a truly agile, software-defined and programmable solution, which is network service provider-agnostic and enables API-driven integrations.

SINGLE SERVICE PROVIDER

for network traffic optimisation, endpoint-based security, identity and access management, network security and more

DARK NETWORK SECURITY

a software firewall and transfer nodes distance the attack surface for better security

FULLY MANAGED SERVICE

includes an at-a-glance dashboard for user and app-level visibility

OPTIMAL PERFORMANCE

our proprietary protocol enables up to ten times better traffic optimisation

MULTIPLE USE CASES INCLUDING IOT

apply it to intranets, secure data transfers for IoT and more

FLEXIBLE PRICING

only pay for what you use with an opex-based, pay-as-you-go pricing model

TATA COMMUNICATIONS

TATA

About Tata Communications

Tata Communications is a leading global Digital Ecosystem Enabler that powers today's fast growing digital economy.

The company's customers represent 300 of the Fortune 500 whose digital transformation journeys are enabled by its portfolio of integrated, globally managed services that deliver local customer experiences. Through its network, cloud, mobility, Internet of Things (IoT), collaboration and security services, Tata Communications carries around 30% of the world's internet routes and connects businesses to 60% of the world's cloud giants and 4 out of 5 mobile subscribers.

The company's capabilities are underpinned by its global network. It is the world's largest wholly owned subsea fibre backbone and a Tier-1 IP network with connectivity to more than 240 countries and territories.

Tata Communications Limited is listed on the Bombay Stock Exchange and the National Stock Exchange of India and is present in over 200 countries and territories around the world.

www.tatacommunications.com | @tata_comm
www.youtube.com/tatacomms | https://www.tatacommunications.com/blog/

For more information, visit us at www.tatacommunications.com