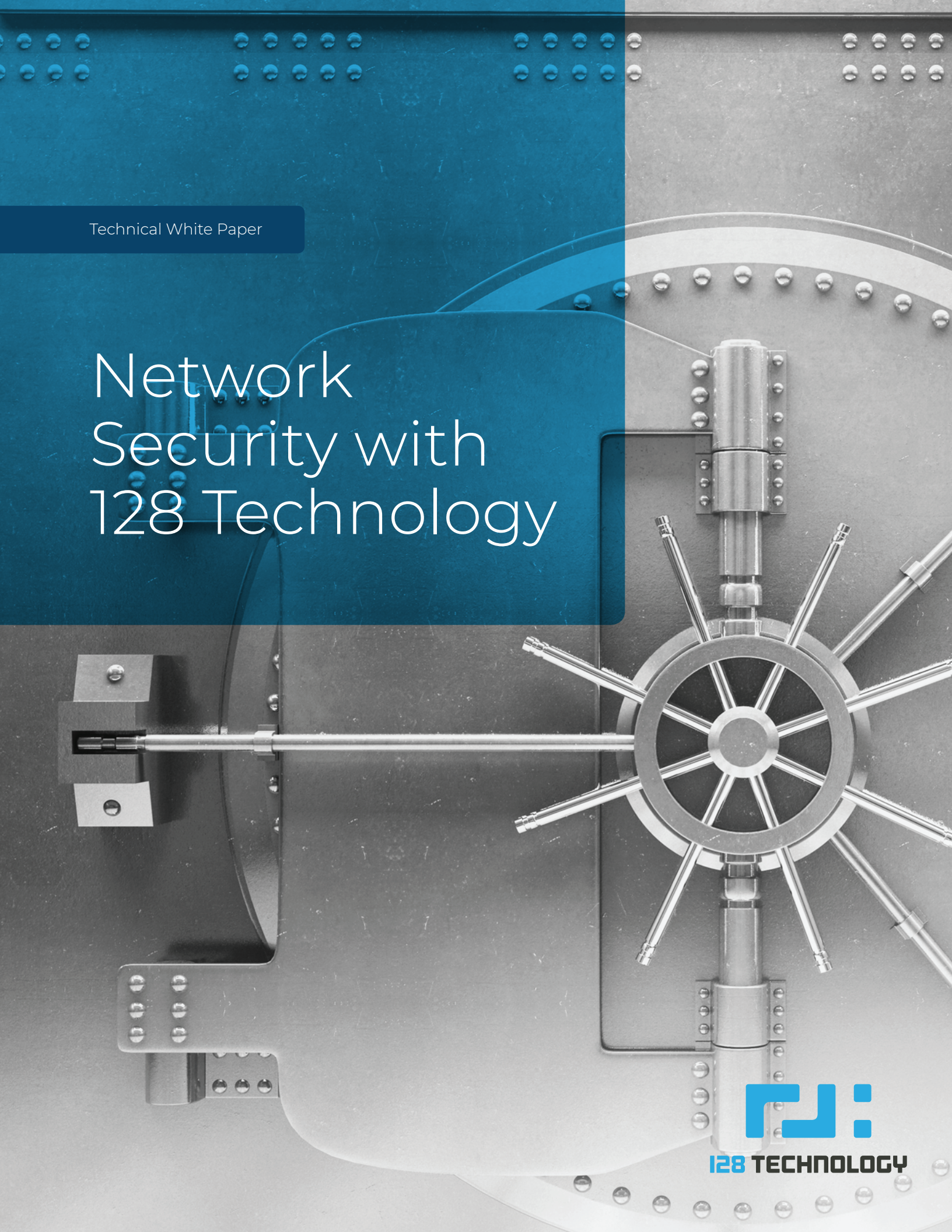
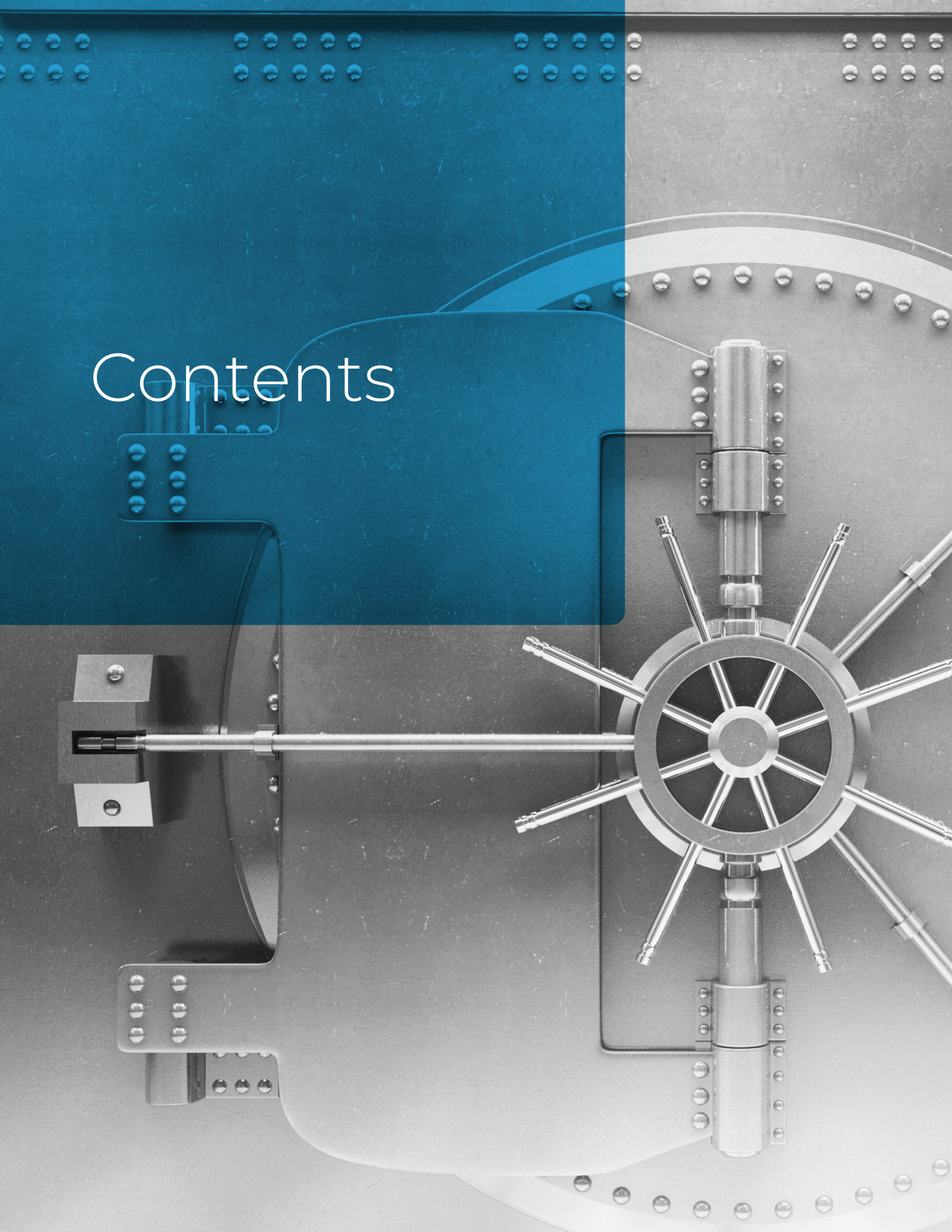
Technical White Paper

Network Security with 128 Technology



128 TECHNOLOGY

Contents



INTRODUCTION

This document is targeted for network and security architects who are looking to better understand Zero Trust Security (ZTS) and the 128T Networking Platform for delivering ZTS. Whether it's a Software-Defined WAN (SD-WAN) or a Software-Defined Data Center (SDDC), 128 Technology's solution provides integrated security, network isolation, segmentation, load balancing, and firewall functions.

Unlike solutions that supplement existing routed networks with yet another third-party middle-box that grafts security into an insecure network, our approach embraces what Forrester Research dubbed the "Zero Trust architecture" . The advanced design of the 128 Technology Session Smart™ Router replaces the traditional routing plane with one built from the ground up with security principles at its core.

Today's networks are built using foundational technology that has changed very little since the inception of the routed IP network in the 1990s. ASIC-based switches and routers were designed to facilitate an "any-to-any" model for packet exchange, where computers can freely communicate with each other using paths built hop-by-hop by the networking equipment between them. Networks are inherently insecure because they pass network traffic by default. Broadcasts and default routing enable compromised devices to talk to other devices on the network. An access control list (ACL) is then used to restrict where traffic can go. As a result, network operators have grown accustomed to configuring complex sets of ACLs, deploying third-party hardware to gain functionality like firewall, IDS/IPS, load balancing, and segmenting traffic using overlay technologies like VxLAN, IPSec and NVGRE, or any number of tunneling techniques. Yet despite the proliferation of various techniques to secure, restrict, or segment the network, the number of security breaches, denial of service events, and other cyber attacks continue to affect service delivery. Enterprises are struggling to protect their networks, intellectual property, and their customers' confidential information.

For true Zero Trust Security, a network must be built at a minimum with the following capabilities:

- Session Smart™
- Hop-by-Hop Authentication
- Adaptive Encryption
- Deny-by-Default Access Policies
- Distributed Stateful Firewall
- Route Directionality
- Secure Routing Fabric
- Centralized Policy Management
- Hypersegmentation

[1] https://www.nist.gov/sites/default/files/documents/2017/06/05/040813_forrester_research.pdf

SESSION SMART™

According to the Computer Security Institute, based in San Francisco, approximately 60 to 80 percent of network misuse incidents originate from inside the network[2]. Often, the severity of these attacks is intensified because traditional firewalls and IDS are ineffective against attacks that originate internally. The default behavior of the 128T System is to treat and apply security controls to sessions, regardless of whether the session has originated internally or externally. Modernizing the network with inherent security, enhanced visibility, and simplified management is at the heart of Secure Vector Routing (SVR[3]) technology invented by 128 Technology. SVR is designed to keep your data safe, yet simple and flexible to make sure the data is accessible. It all begins with a unique set of key principles and capabilities that transform the network into an asset for enterprises that need to compete in today's data-driven landscape.

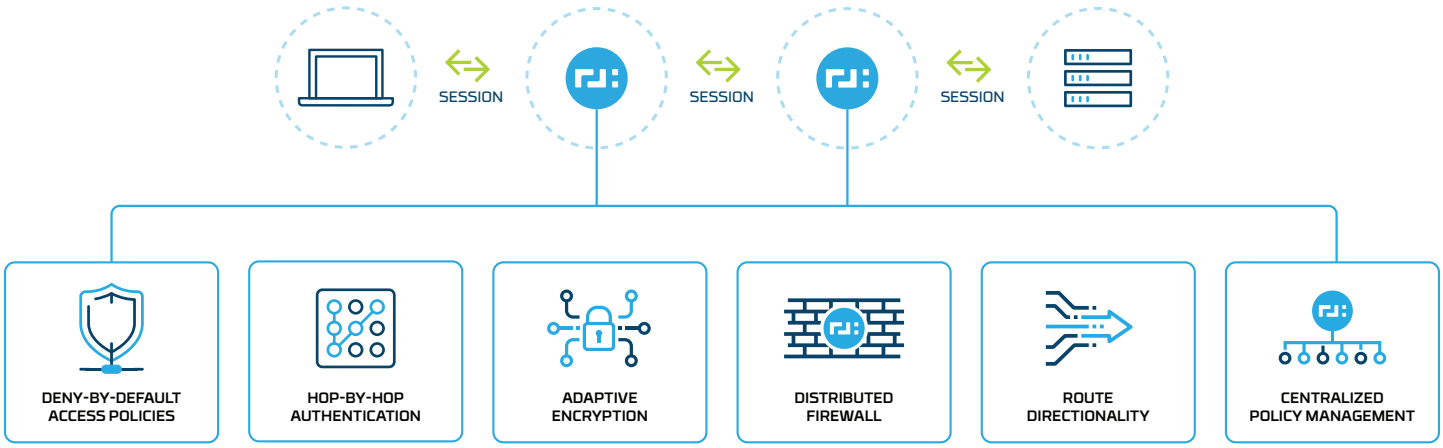


Figure 1

[2] https://www.techrepublic.com/blog/it-security/myth-or-not-most-security-breaches-originate-internally
[3] https://www.128technology.com/blog/fixing-internet-using-secure-vector-routing

DENY-BY-DEFAULT ACCESS POLICY

128T Session Smart™ Router uses an innovative data model that lets network architects describe how their network will be used in a whole new way. It starts with the services that form the raison d'être of the network: things such as your CRM system, ERP system, mail, voice, and web resources. Access to these services is granted based on what we call tenancy: each tenant in the 128T data model represents a collection of users and their devices that share common policies—things such as access policies and security policies. Unlike zone-based schemes, tenancy is applied and enforced at every 128T instance, network-wide:, our tenant's policies "stretch" across your network.

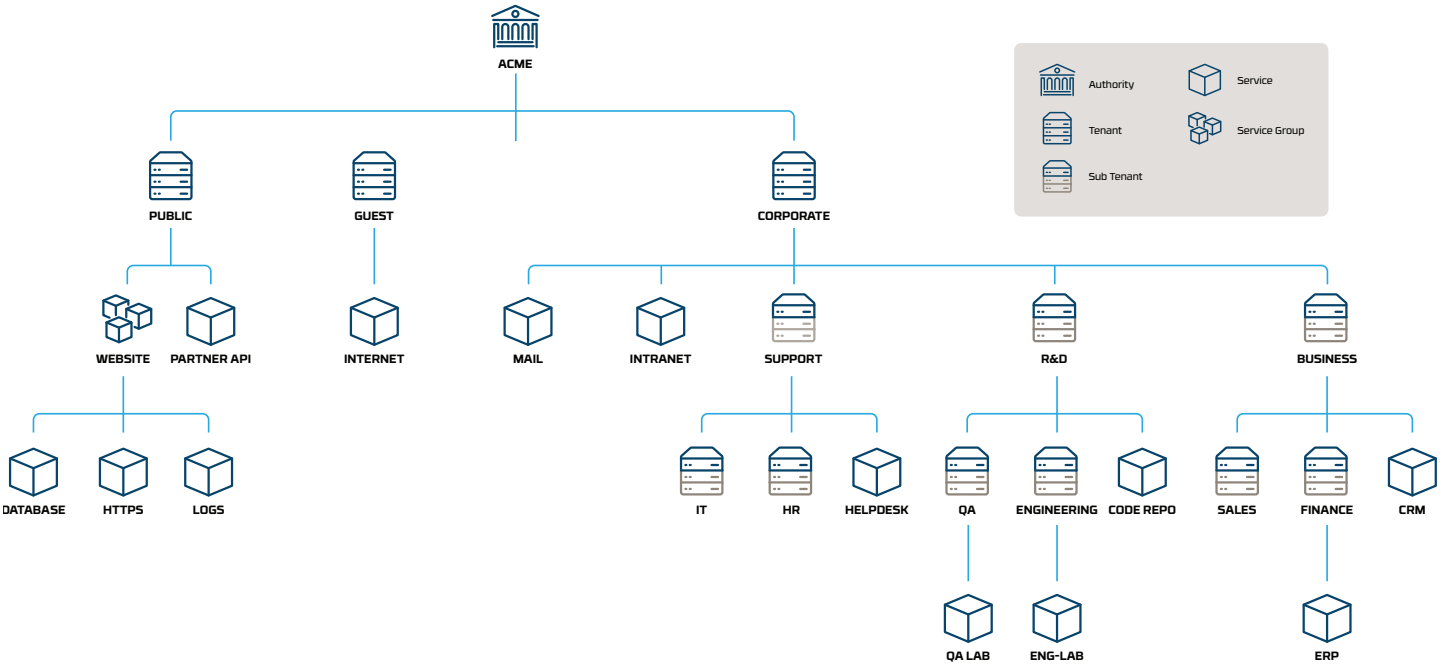


Figure 2

Administrators define the tenants (user populations) that use the network and the services that the network offers. Using an intuitive, text-based, associative language, administrators grant or deny access to those services for members of the various tenants on the network. These tenants and services are shared among all the 128T Routers within an administrative domain (what we call an authority), along with security properties such as authentication and encryption keys. This ensures network resources are offered only to those permitted to use them. Under the hood, these tenant and service definitions govern the construction of each 128T Router information database (RIB) and forwarding information database (FIB).

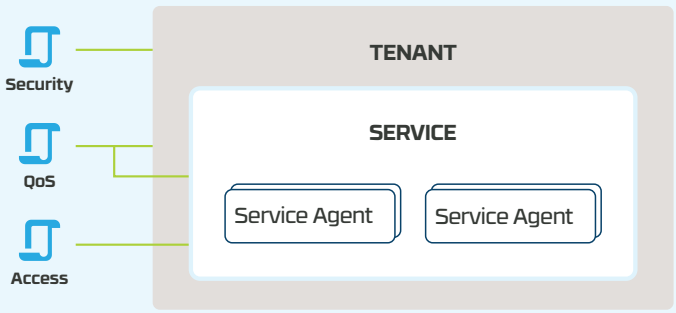


Figure 3

A tenant functions as a network partition used to group services together.

As sessions are processed through 128 Technology's solution, the tenant becomes an important construct for route determination, segmentation, classification, policy, and many other capabilities.

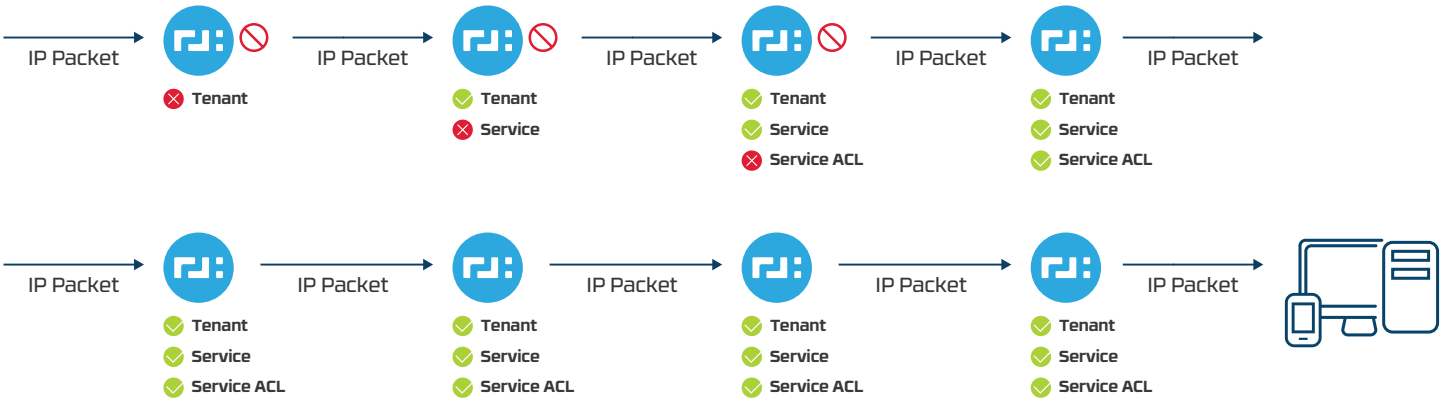


Figure 4

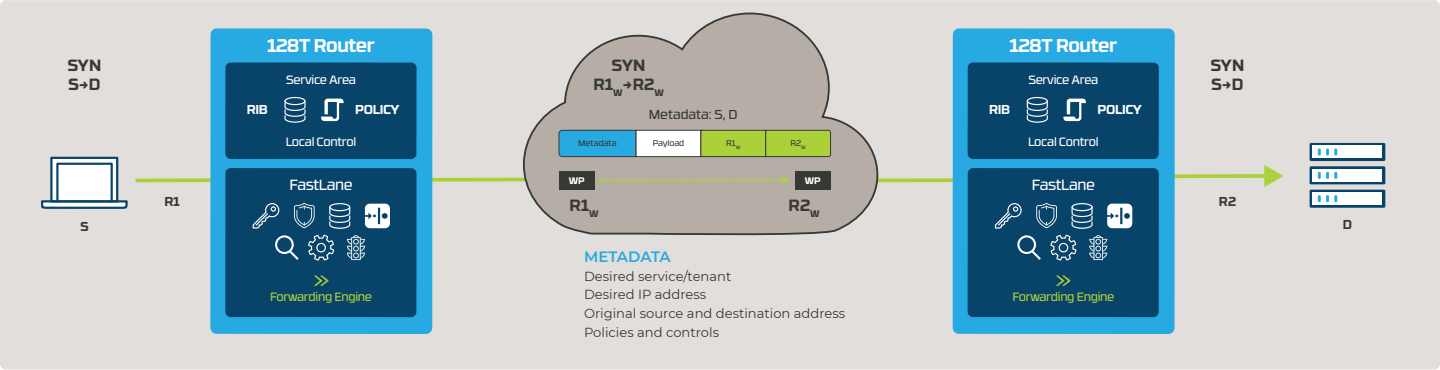
Unlike a traditional router, which has the default policy of "allow-by-default", 128 Technology's Session Smart Router follows the principle of "deny-by-default". This means, when a packet hits the 128T Router, the first thing it does is to check whether the packet belongs to a tenant. If the packet does not belong to a tenant, the packet will be dropped. If the packet belongs to a tenant, the next step is to check whether the packet is destined to a service defined within the tenant. If the destination of the packet does not correspond to any service within the tenant, the packet will be dropped. If the destination of the packet belongs to a service, the 128T Router will further look at the context-specific ACL defined within the service to see whether the source of the packet is allowed access to the service. If the source is denied access to the service, the packet will be dropped. Finally, once the packet passes all the above checks, the packet will be forwarded to the next hop towards the destination. Please note that while performing all these checks with every packet, the 128T Router still maintains the traffic rate to match with the line-rate.

With a deny-by-default approach, unless an enterprise explicitly enables a session to traverse through the network, the 128T Router will drop all the packets belonging to the session. This tight control of the packet flow within the network is very powerful and can limit, and in some cases completely eliminate, network attacks.

HOP-BY-HOP AUTHENTICATION AND ADAPTIVE ENCRYPTION

The 128T Session Smart™ Router is built on the principles of Zero Trust Security. One of the primary requirements of Zero Trust Security is to support policy-based inter-router traffic encryption and authentication. Every packet exchange between 128T Routers is authenticated and encrypted by default using HMAC-SHA256-128 and AES256, respectively.

As part of the flow setup process, the 128T System exchanges metadata in the first packet. The metadata exchanged is signed using HMAC-SHA256-128. Optionally, the metadata can be encrypted using AES256. By signing and optionally encrypting the metadata exchanged in the first packet, it creates a secure fabric in which the 128T System's routing fabric is reserved for its own exclusive use. This helps defend against insiders and eavesdroppers.



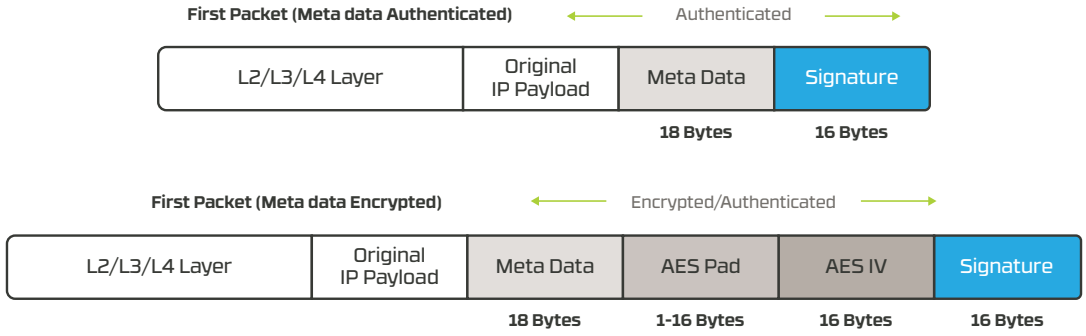


Figure 4

The keys for encryption and per-packet authentication are dynamically generated by the 128T solution at boot time and are securely stored. Per-session encryption is supported between all 128T instances, and protected using FIPS 140-2[4] based AES256 encryption and per-packet authentication based on the HMAC-SHA256-128 algorithm.

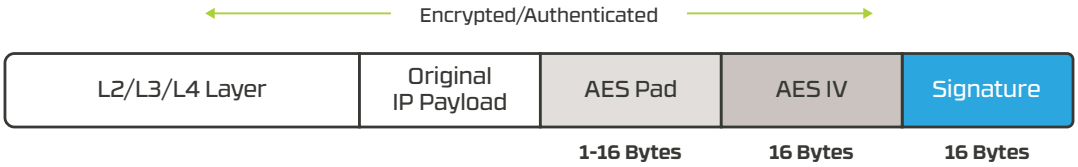


Figure 5

Encryption is done in a stateless manner by explicitly carrying an initialization vector (IV) in each packet. The IV is generated using the FIPS140-2 DRBG[5] method. The DRBG method of generating IV allows the 128T Networking Platform to generate a true random number, thus providing complete protection from the Man in the Middle and replay attacks.

[4] https://csrc.nist.gov/csrc/media/publications/fips/140/2/final/documents/fips1402.pdf
[5] https://csrc.nist.gov/publications/detail/sp/800-90a/archive/2012-01-23

	IPSEC	TLS	128T
Strong Encryption (AES256)	✓	✓	✓
Strong Per packet Authentication (HMAC-SHA256-128)	✓	✓	✓
Low per packet overhead	✗ 78 Bytes	✓ 52 Bytes	✓ 32-48 Bytes
Does not require a control protocol	✗ Require IKEv1/IKEv2	✓	✓
Simple key exchange	✗ Can require up to 14 control packet exchange for key generation	✗ Can require up to 14 control packet exchange for key generation	✓ Keys are automatically generated and distributed
Easy to configure and Manage	✗	✗	✓
Easy to Deploy and Troubleshoot	✗	✗	✓
Does not require Certificate/PKIX support	✗	✗	✓
Stateless Encryption	✗	✗	✓

The table above compares 128T encryption/per-packet authentication schema with IPSec and TLS 1.2. As shown in the table, 128 Technology provides FIPS 140-2 level encryption and per-packet authentication with minimum overhead (32-48 bytes) compared to IPSec (78 bytes) and TLS (52 bytes). Also, since encryption and authentication keys are automatically generated and distributed, the 128T Networking Platform eliminates the need for complicated key exchange protocols like IKEv1 and IKEv2 required by IPSEC or PKIX[6] based X.509 digital certificates.

Because of the session-oriented nature of 128T Routers, they can detect whether the traffic is already encrypted using TLS/HTTPS or by IPSec, while performing encryption of the application. If the application traffic is already encrypted using IPSec or TLS, the 128T Router will not re-encrypt the packet (adaptive encryption), thus eliminating the overhead associated with double encryption. Double encryption is a significant issue in networks where IPSec is used between branch offices or data centers for interconnect and multi-site VPNs. Since voice and video traffic are latency and jitter sensitive, double encryption with IPSec can have an undesirable impact on business operations.

To conclude, the 128T Networking Platform provides a simpler, more cost-effective FIPS 140-2 compliant encryption and authentication mechanism compared to what is provided by IPSEC and TLS. Also, the adaptive encryption mechanism provided by 128 Technology's solution eliminates risk of fragmentation and double encryption of a packet, thereby minimizing latency and jitter, as well as cost.

[6] https://tools.ietf.org/html/rfc5280

DISTRIBUTED STATEFUL FIREWALL

Most current enterprises implement perimeter-based security, which uses standalone firewall devices at the edge of the network. Firewall technology heavily relies on ACLs and VLAN's to control access to various segments of the enterprise network. As the network grows, the number of required ACLs and VLANs for access control grows exponentially. This makes the firewall ACL rules unmanageable and error prone, exposing the enterprise to various security threats and network attacks. Even when enterprises move from perimeter-based security to a micro-segmentation approach, firewall devices are still deployed at the edge of every segment, having the same complexities associated with ACLs and overall manageability.

The 128T Networking Platform behaves as a session-aware firewall, eliminating the need for a global ACL list and error prone configurations, with access control tied to services with a tenant. By default, only members of a tenant are allowed to access its services within, thereby minimizing the complexity of configurations, while maintaining a high security standard in terms of access control. When a non-member wants to access the services of a tenant, the access control policy is specified within the service. This leads to an access control rule that is very context-specific and pertinent to the service.

In addition to tenant-based segmentation and access control, the 128 Technology solution provides complete L2/L3/L4 session-aware capabilities through a standard firewall, which eliminates the need for standalone firewalls.

In addition to tenant-based segmentation and access control, the 128 Technology solution provides complete L2/L3/L4 session-aware capabilities through a standard firewall, which eliminates the need for standalone firewalls.

SERVICE FUNCTION CHAIN (SFC)[7]

With Network Function Virtualization (NFV), more and more service functions (SFs) are virtualized and run on COTS platforms. Running SFs on a COTS platform allows enterprises and carriers to service function chain (SFC) these functions when building a network. In addition to supporting built-in service functions, the 128T Networking Platform can service function chain standalone service functions like firewalls and load balances from other vendors. 128 Technology has partnered with Zscaler and Palo Alto Networks to provide next-generation firewall capabilities through SFC.

Networks with a NFV strategy can utilize the 128T Router for routing, ZTS, load balancing and then add on layer 5 and above security through next-generation firewall partners. The infused firewall, load balancing, and DPI capabilities built within the 128T Router eliminate the need for a third-party SF for layer 3/layer 4 protection.

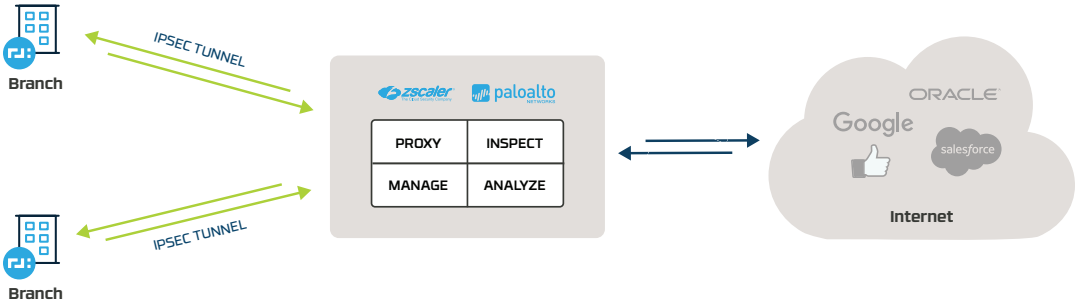


Figure 6

[7] https://www.sdxcentral.com/nfv/definitions/whats-network-functions-virtualization-nfv

ROUTE DIRECTIONALITY

There are a few profound implications of the session-oriented nature of the Session Smart™ Router. Through the administration of routes based on directional sessions and traffic symmetry management, the network itself becomes much simpler. At the same time, security is enhanced because instead of being painted on, it's baked into the network capabilities.

Most of the legitimate traffic on an IP network has packets that flow bi-directionally, creating a session between two endpoints. Sessions have directionality in that they are initiated from one endpoint (e.g., a client) to another endpoint or endpoints (e.g., a server). They consist of two flows, one in the forward direction and one in the reverse direction. After a session becomes established in one direction, subsequent packets in the session transit through two unidirectional flows that are instantiated. In traditional switching and routing infrastructures, forward and reverse flows may take asymmetric paths through the network. In a session controlled by 128 Technology's solution, the flows have path symmetry. The 128T Networking Platform is built with an orientation around the sessions that exist between endpoints over an IP network.

This is the first step in delivering simplicity afforded by the administration of routes in the network. It contrasts from traditional destination-based routing, where routes for the forward and reverse paths must be expressed throughout the network in order for any traffic to occur. With session-orientation, routes can be expressed in terms of the directional sessions, which automatically include the two unidirectional flows that comprise a given session. This combines the functions of a router and a stateful firewall, into a single function to simplify networks and improve security.

Flows in the forward and reverse direction for a session follow the same path through the network for traffic symmetry across the network. This becomes extremely useful for analysis and troubleshooting of network traffic. Traffic symmetry also allows for optimal traffic steering and path selection.

SECURE ROUTING FABRIC

With the built in ZTS capabilities, the 128T Session Smart™ Router allows an enterprise to build security controls into every segment of the network to create a secure routing fabric. In traditional routed networks, because of the allow-by-default policy, most of the packets are transported across the networks without any controls. In a network built with 128T Routers with a deny-by-default policy, the overall role of the network shifts from transporting all the packets across the network, to transporting only those packets that are verified to be safe and properly encrypted, and which are legitimately required to run the enterprise.

Instead of relying on ACL lists and rules to determine which traffic may not be transported (and transporting all else), with 128T Routers, the only traffic that is transported is that which has been expressly green-lighted.

So, thus with 128T Routers, security is baked into the network itself rather than simply painted onto the perimeter, making the network fabric and routing algorithms the tools necessary to mount a more effective, simple, less expensive, distributed defense against increasing security threats.

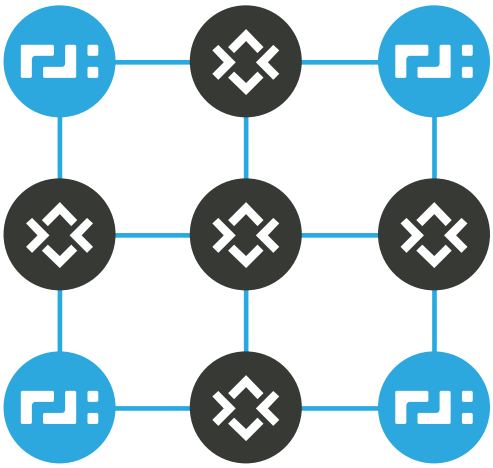


Figure 7

CENTRALIZED POLICY MANAGEMENT

128T Routers provide centralized policy management, administration, provisioning, monitoring, and analytics through the 128T Conductor. It provides a single "pane-of-glass" view for all 128T Routers running in the enterprise network.

With traditional firewall devices, the difficulty with managing policy grows exponentially as the network grows. A powerful and flexible feature on the 128T Router is the ability to perform service-level policy enforcement, thus making policies context-specific. Also, since the definition of the services is global within an authority, policies defined within the services are globally applied to all the routers under an authority, thus eliminating the need for defining custom policies per router.

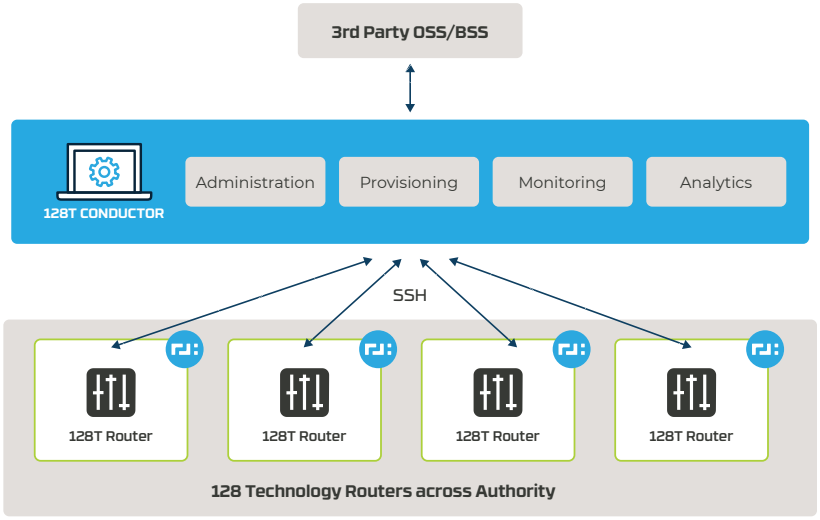
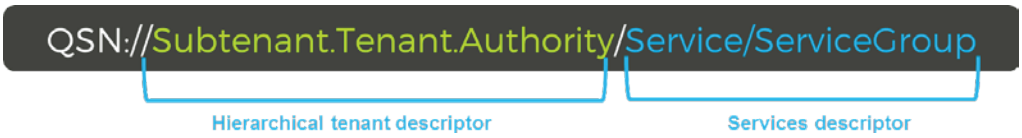


Figure 8



The access control rules within a service can be specified in terms of IP prefix or by making use of qualified name service (QSN). A QSN provides a mechanism to address the resource using a hierarchical uniform resource identifier (URI) name instead of an IP address. The concept of QSN is very powerful as it minimizes the errors, which can be caused while defining access policies in terms of IP prefix and ports.

HYPERSEGMENTATION

128 Technology has developed a way of segmenting networks down to single endpoints and services on those endpoints, while providing a named-based hierarchy, enabling easy and effective administration and enforcement of security policies.

Traditional network segmentation is zone-based, defining users into trusted and untrusted zones and providing many security layers within that network or sub-network. All the users, computers, and servers within a given zone can freely talk with each other. In a LAN environment, this would equate to sharing an Ethernet broadcast domain. To go between zones requires going through a firewall, which requires an explicit policy to allow the IP traffic through. The firewalls control the so-called "north/south" movement of network traffic into and out of the zone, and allow "any-to-any" communication within a segment.

Additionally, the concept of micro-segmentation[8] marketed by many vendors, relies on overlay networks (based on VxLAN and NVGRE) and partnerships with third-parties to implement security and network segmentation. Given the fact that the overlay networking technology is not inherently secure, micro-segmentation depends on third-party firewalls and DPI devices for securing the boundary of the network segments. This painted on security makes the overall solution complicated, expensive, and difficult to manage. Also, since overlay technology is oriented around tunneling and multicast technologies, it's difficult to implement and maintain, as well as costly because it has considerable per-packet overhead.

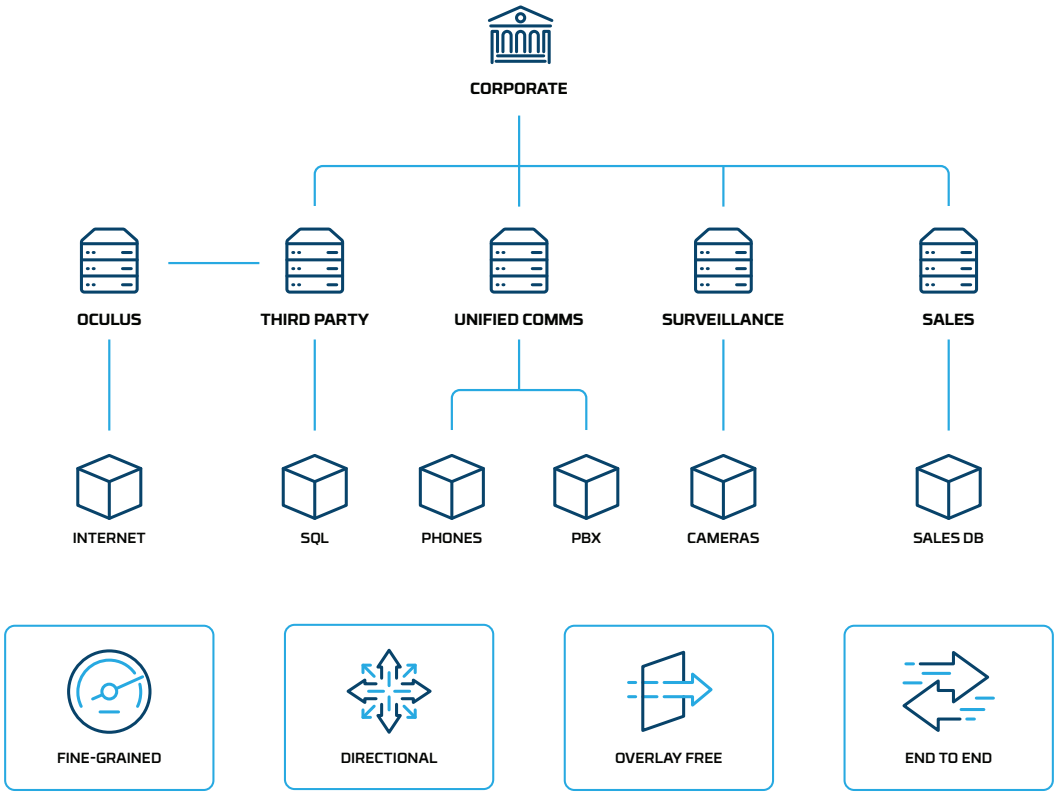


Figure 9

The 128T Networking Platform has security built in from the ground up, providing hypersegmentation of the network based on sessions, services, and tenants. The session-oriented nature of 128 Technology's solution allows the platform to treat every session like a segment and grants the ability to apply unique security rules, firewall, DOS/DDOS prevention, and DPI at every session level. The resulting hypersegmentation becomes a very powerful and unique technology that enables organizations to avoid expensive and complicated overlays and simplify management, while also enhancing security.

[8] https://www.128technology.com/blog/fixing-internet-using-secure-vector-routing

The major components of hypersegmentation include:

Fine-Grained

Micro-segmentation aligns segmentation with applications. However, hypersegmentation takes segmentation a step further to align with sessions, thus providing complete session-level isolation for a deeper level of security.

All segmentation with hypersegmentation is based on how traffic is classified across the enterprise branch, data center, and into the cloud. All traffic is classified at each 128T Router based on a combination of local network characteristics such as IP address/prefix or VLAN, and application/session type identification. The classifications are grouped by tenants that define access control and membership for each segment along with the corresponding services belonging to this segment. Unless explicitly configured, members belonging to one tenant will not be allowed to access services belonging to other tenants.

Directional

When directionality is attached to session creation, it prevents rogue programs on the server from sending sensitive data to the external world, effectively eliminating many of the high-profile attacks we have seen in the recent past. Session initialization is tightly controlled within each segment and attaches directionality to the created session. This means, if a policy is configured to allow session creation from the client to the server only, the 128T Networking Platform will not allow a server to initiate a session back to the client or to the external world, thus attaching strict directionality (vector) to session creation process.

Overlay/Tunnel Free

Traditional approaches to segmentation depend on an outdated perimeter security model, constructing network segments with complex firewall rules, and static VLAN or tunnel configurations. The 128T Networking Platform provides isolated virtual L3 networks as a function of SVR. Furthermore, network services (L3, ACL, stateful firewall, QoS, and load balancing) are natively integrated into the 128T Networking Platform, distributed to every branch, every data center, and every hypervisor. This improved simplification means firewall-specific configurations, and error-prone VLAN or complex tunnel configurations, are no longer needed.

End to End

Since micro-segmentation makes use of multiple tunneling technologies (VXLAN in data center [DC] and IPSEC between DCs), achieving end-to-end (E2E) segmentation is very complex and difficult to manage.

Because no overlays are required, hypersegmentation allows segmentation to stretch from DC to DC, DC workload to the branch, and ultimately to devices, treating multiple networks and network islands like a single unified fabric, allowing seamless E2E segmentation.

SUMMARY

For decades, routed and overlay networks have been designed around an increasing amount of prefixes, tags, labels, identifiers, and encapsulations that are only significant to the networks and their topology. “The tail wagging the dog,” is a fitting expression. The 128 Technology approach to ZTS and segmentation is entirely distinct, introducing a whole new set of tools for network design intended to allow operators to build the network around the services it is meant to deliver, rather than around the network itself. It enables the routing and policies of the network to be expressed in terms, allowing for semantic meaning to be applied to businesses and applications, not network topology.

Furthermore, tenancy is not just some useful abstraction of the same archaic techniques behind the scenes. Subscribing to that theory would be perpetuating the same incrementalism that has gotten networks into the overly complex state they find themselves in today. Rather, tenants are present in the very forwarding tables and packet pipelines of the 128T Networking Platform, making them a foundational component of the routed network itself. The ability to partition service availability—afforded by the network using tenants—is one of the many ways 128 Technology is fixing the network, by fixing the router.

To learn more about 128 Technology, visit www.128technology.com.

ABOUT 128 TECHNOLOGY

128 Technology makes your network do what your business needs, by changing the way networks work. Our professional grade software teaches routers the language of applications and services, letting them understand the requirements of individual services and segments, and adapt the network dynamically to deliver what the business needs, when and where it needs it. We make routers Session Smart™, enabling enterprise customers and service providers to create a service-centric fabric that's more simple, agile, and secure, delivering better performance at a lower cost.

781.203.8400 | www.128technology.com | 200 Summit Drive, Suite 600, Burlington MA 01803