128T PCI COMPLIANCE

INTRODUCTION

The Payment Card Industry Data Security Standard (PCI-DSS) was written by the payment card industry to help merchants around the globe to secure and protect stored, processed, transmitted Primary Account Numbers (PANs) and associated personal credit card holder information. Achieving compliance with the PCI standard can help an Enterprise to minimize fraud and theft of credit card data. If an organization is not PCI complaint, right to access and process credit card data may be denied. Even worse scenario for an Enterprise not having PCI compliance is the decline in customer loyalty and loss of brand value after the theft of sensitive credit card data.

The core of PCI compliance includes 12 principles and corresponding requirements. The 12 principles highlighted in the standards are:

1. Build and maintain a secure network
2. Configure system security parameters
3. Protect cardholder data at rest
4. Protect sensitive data in transit
5. Implement tools and protect against malicious software and viruses
6. Develop and maintain secure applications
7. Implement a process to authorize system access based on need-to-know
8. Implement strong user authentication
9. Physically secure systems and network devices
10. Implement authomated audit logs and protect log data
11. Monitor and test security controls
12. Maintain an information security policy and incident response plan.

128T Session based Networking platform provides a

Compliance Challenges

A credit card accepting business must have a PCI-DSS complaint architecture to secure and protect stored, processed and tramsitted credit card data.

Solution

128T Session based Networking Platform provides native zero-trust security and hyper-segmented routing architecture allowing organization to achieve and exceed PCI compliance requirements. 128T solution integrates multiple middle-box functionalities (security, routing, firewall, VPN and load balancing) into a single platform thus simplifying the overall network architecture while minimizing the cost to achieve PCI compliance.

Key Benefits

- Provide optimal cost effective network architecture to achieve PCI-DSS compliance requirements
- Build from ground up to be a Zero Trust Security complaint device with security and network segmentation built into the service aware data model
- FIPS 140-2 complaint security with support for AES256 encryption and HMAC-SHA256 per packet authentication
- Simplification of the network architecture by eliminating middle-boxes in the network

native Zero Trust Security (ZTS) and hyper-segmented network architecture allowing organization to achieve and exceed PCI compliance requirements. Also, 128T solution integrates multiple middle-box functionalities (security, routing, firewall, VPN and load balancing) into a single platform thus simplifying the overall network architecture while minimizing the cost and time to achieve PCI compliance.

Highlights of the features supported by 128T Session based Router to achieve PCI compliance include

- **Zero Trust Security Model** - 128T adopts a Zero-Trust security model which guarantees that only authorized sessions traverse the network. This ensures access control for each route and authentication of all communication, policy based inter-router traffic encryption, and fully distributed stateful firewall protection.
- **Hyper-segmentation** – Custom security policies, per packet authentication/encryption, firewall, DOS/DDOS protection, and load balancing are applied per session basis thus providing true network segmentation at the session level.
- **Simplified and automated provisioning** - Configure and manage security and segmentation policies centrally through a central controller or using central management platform (called Conductor) and through DevOps[1] tools.
- **Improved visibility** - Fine-grained session-based security statistics and analytics
- **Reduced cost and complexity** – Innovative utilization based pricing providing utmost flexibility for multiple deployment models. Integrated security functions in the IP routed network replace complex and expensive network appliances.

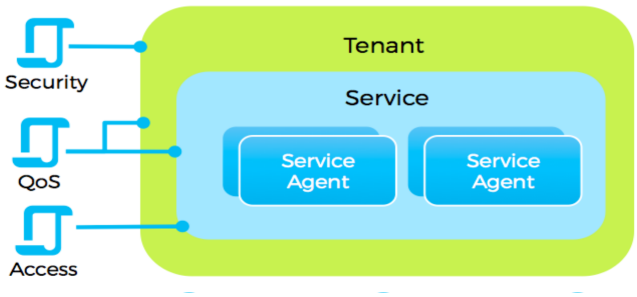
128T SESSION BASED NETWORKING PLATFORM

128T Session based Networking Platform (router) innovatively combines routing and security under one platform. Security is the DNA of the 128T Session based router and every aspect of this product is built with keeping security as the central focus.

Key principles behind 128T Session based router include:

SERVICE CENTRIC TENANT BASED SECURITY ARCHITECTURE

The traffic in 128T platform is processed, routed, and controlled in a service-centric manner. Therefore services make up a fundamental building block for the operation of the 128T router. Services can be made to model a given application, reachable at a given address, set of



[1] https://en.wikipedia.org/wiki/DevOps

addresses, or subnets.

A tenant functions as a network partition used to group services together. As sessions are processed through the 128T solution, the tenant becomes an important construct for route determination, segmentation, classification, policy, and many other capabilities.

128T provides the unique capability to specify security policy, Quality of Service (QOS) parameters, and access control policies on per service per tenant basis. This means, it is possible to have unique encryption/authentication keys, custom traffic engineering parameters and tight access control per service per tenant basis thus providing a flexible way to **segment** and isolate the traffic and apply different traffic profiles on a per service per Tenant basis.

SECURE VECTOR ROUTING (SVR)

The 128 Technology solution introduces a breakthrough session-based , service centric and security-infused networking paradigm called Secure Vector Routing. Secure Vector Routing is fully compatible and interoperable with existing data and control plane architectures. The Secure Vector Routing replaces and augments complex out-of-band routing protocols, tunnel-based network overlays and cumbersome provisioning systems with centralized control, simple intelligent service routes and in-band (data plane) signaling.

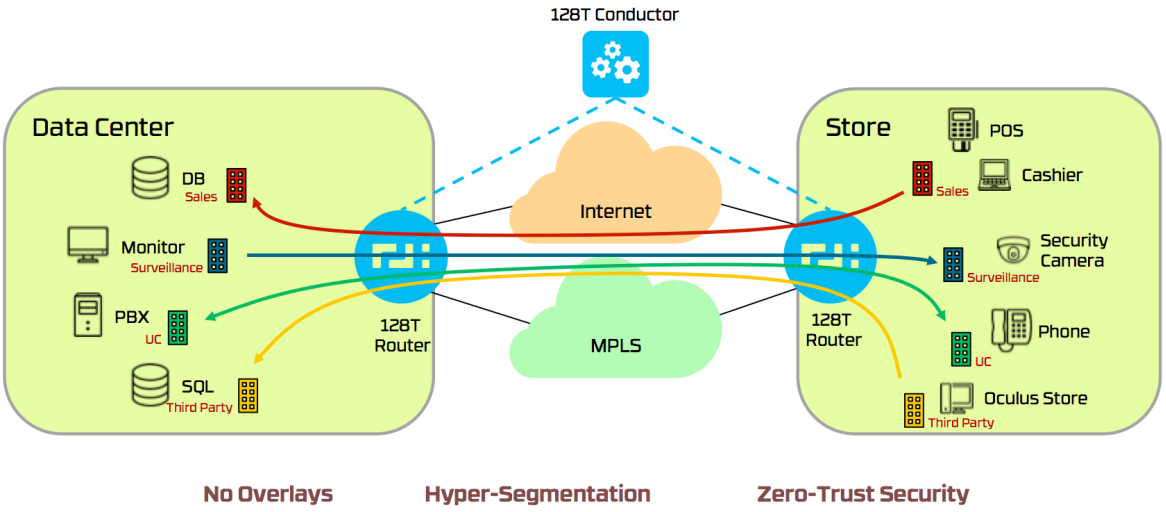
TENANT BASED HYPER-SEGMENTATION AND ISOLATION

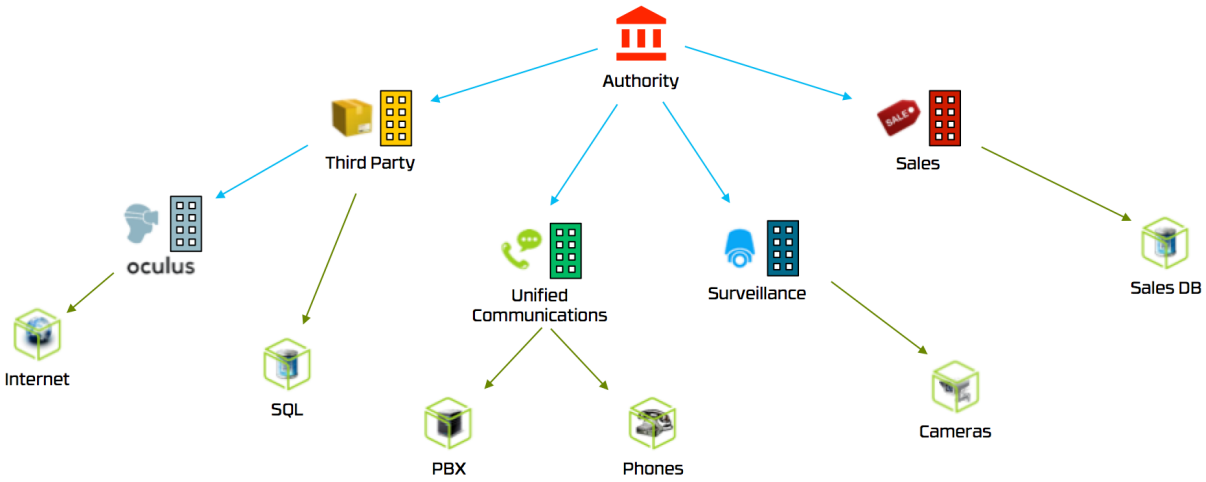
Over the period of last few years, because of all the high profile security breaches, segmenting the network is becoming more prominent in the way networks are built. Segmenting the networks allows to limit the spread of network attacks and security breaches within the segment thus isolating the rest of the segments from these attacks and security breaches. The concept of Micro-segmentation[2] marketed by many of the networking vendors as the new way of doing segmentation, relies on overlay networks (based on VxLAN and NVGRE) and partnership with third party security vendors to implement security and network segmentation. Given the fact that an overlay networking technology is not inherently secure, Micro-segmentation relies on third party firewalls and DPI devices for providing security at the boundary of the network segments thus making the overall solution complicated, expensive and difficult to manage. Also, since overlay technology relies on tunneling and multicast technologies, it is difficult to implement and maintain and has considerable per packet overhead.

---

[2] http://www.networkcomputing.com/networking/three-requirements-true-micro-segmentation/1151379004

128T platform provides hyper-segmentation, a unique way of segmenting the network based on sessions, services, and tenants. The session oriented nature of 128T solutions allows 128T platform to treat every session as a segment and allows to apply unique security rules, firewall, DOS/DDOS prevention, and DPI at every session level thus making hyper-segmentation a very powerful and unique technology.





Above picture shows one of the practical use case of hyper-segmentation, route directionality and centralized policy management capabilities of 128T platform. The scenario above shows a retail store deployment for an Enterprise. In this deployment, there is a data center in Boston and a retail store location in Atlanta. This Enterprise has segmented their traffic into four main tenants: Sales, Surveillance, "Unified Communications" [UC], and "Third Party." This segmentation ensures that services are only available to the hosts that are classified as being within that tenant.

In each tenant, there is one or two services. The sales tenant has the sales_db service and the surveillance tenant has the Security Camera service, The UC tenant has two services: PBX, in the Boston data center, and UC phones, the LAN segment on the Atlanta router where the Atlanta UC phone is connected.

As shown in the above picture, unless a host is a part of a specific tenant, host will not have access to the service under that tenant. For example in the above picture, only Sales tenat has access to Sales DB. Also, because of the vectored nature of 128T routing, there is directionality attached to the router. For example in the above example, the Point Of Sales (POS) device can connect to the Sales DB, however, the Sales DB cannot connect to the POS. Thus, with hyper-segmentation and Secure Vector Routing, many of the attacks and security breaches are automatically eliminated by architecting the network based on 128T platform.

ZERO-TRUST SECURITY (ZTS) MODEL

The Zero Trust Model promotes "never trust, always verify" as its guiding principle. With Zero Trust there is no default trust for any entity — including users, devices, applications, and packets — regardless of what it is and its location on or relative to the corporate network. 128T platform architecture's inherent network virtualization and infused security functions are leveraged to create Zero Trust boundaries that effectively compartmentalize different segments of the network to protect critical intellectual property from unauthorized applications or users, reduce the exposure of vulnerable systems, and prevent the lateral movement of malware throughout a network.

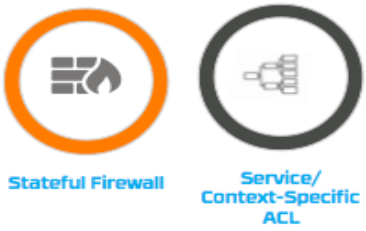
ACHIEVING PCI COMPLIANCE THROUGH 128T PLATFORM

As it is clear from all the recent attacks, hackers are targeting retailers and Government entities in an attempt to steal credit card data and personal information of employees and customers for financial gains, espionage, and political gains. Enterprises and Government entity should be able to securely process, store, and transmit credit card data and associated personal information without being exposed to theft. Hence, it is highly critical for these organizations to implement the Data Security Standards as specified by the PCI Security Standards Council. Table below shows PCI-DSS subsection requirements addressed by 128 Technology.

Req	Descriptions	Subsection	128T Capability
1	Install and maintain a firewall configuration to protect cardholder data	1.1, 1.2, 1.3, 1.4, 1.5	Firewall capabilities, SVR and ZTS
2	Do not use vendor supplied defaults for systems	2.1, 2.2, 2.3	FIPS 140-2 and

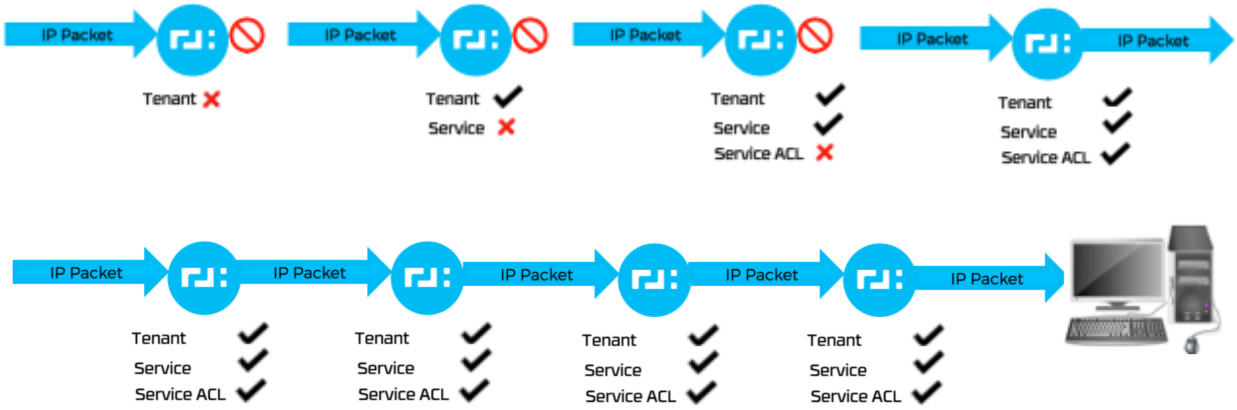
	passwords and other security parameters		Fedramp compliance
3	Protect stored cardholder data	3.5, 3.6	Secure key storage and rekeying
4	Encrypt transmission of card holder data across open, public network	4.1, 4.2, 4.3	SVR
5	Protect all systems against malware and regularly update anti-virus software or programs		N/A (This requirement applies to end points (mostly applies to personal computers)
6	Develop and maintain secure systems and applications	6.1, 6.2, 6.3, 6.4, 6.5, 6.6	Firewall and SVR support
7	Restrict access to cardholder data by business need to know	7.1, 7.2	Firewall and SVR
8	Identify and authenticate access to system components	8.1, 8.2, 8.3, 8.4, 8.5	Firewall, SVR and Two factor authentication
9	Restrict physical access to cardholder data		N/A
10	Track and monitor all access to network resources and cardholder data	10.1, 10.2, 10.3, 10.4, 10.5, 10.6, 10.7	Firewall
11	Regularly test security systems and processes	11.3, 11.4	Firewall
12	Maintain a policy that addresses information security for all personnel	12.1, 12.2, 12.3, 12.4, 12.5, 12.6	Firewall

Requirement 1: Install and maintain a firewall configuration to protect card holder data



128T innovative Secure Vector Routing[3] technology allows 128T routers to behave as a session-aware firewall along with the capability for defining context specific ACLs which eliminates needs for global ACL list and error prone configuration thus allowing a true Zero Trust Security network architecture.

128 Technology's (128T) session based router follows the principle of "deny-by-default". This means, when a packet hits 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, 128T 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, 128T router still maintains the traffic rate to match with the line-rate.



With "deny-by-default" approach, unless an Enterprise explicitly enables a session to traverse through the network, 128T router will drop all the packets belonging to the session thus exceeding the requirements in "Requirement 1" of PCI-DSS.

---

[3] http://www.pund-it.com/blog/128-technology-secure-new-vector-routing-solutions-across-network-boundaries/

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

As a part of the Installation process, 128T routers requires the administrator to change all the default passwords to a complex password, as required by 128T password Fedramp compliance procedure. Management access is provided through SSH which makes use of AES256 for encryption and HMA-SHA2 for per packet authentication.

Requirement 3: Protect stored card holder data

Cryptogrphic keys used for encryption (AES256) and per packet authentication (HMAC-SHA256) are generated using NIST 800-9A Deterministic Random Bit Generator (DRBG) mechanism. The keys are stored in a secure store on the router in an encrypted form using a system key. The system key used to securely store the encryption and per packet authentication key is as strong as the keys stored. Also, the system key is not stored on the router itself to prevent theft of keys.

128T routers provides a mechanism to rekey the encryption and per packet authentication keys on a timely fashion. Once the keys are rekeyed, the old keys will be replaced with the new keys on all the routers and the old keys will be invalidated.

Requirement 4: Encrypt transmission of cardholder data across open, public networks

All communication between 128T routers can be encrypted using AES256 and per packet authentication using HMAC-SHA256. Configuration of the encryption and authentication parameters are done at the tenant level. Any packet belonging to any service under the tenant with cryptography enabled will be automatically encrypted (using AES256) and per packet authenticated (using HMAC-SHA256).

Requirement 5: Protect all the systems against malware and regularly update anti-virus program

This requirement applies to end points like Personal computers and Mobile end points. This requirement requires that the definition of anti-virus and malware is kept up to date on these endpoints.

Optionally, 128T can be Service Function Chained (SFC) with multiple industry standard Next Generation Firewalls (NGFW) for providing malware and anti-virus protection at the network level.

Requirement 6: Develop and Maintain secure systems and applications

128T follows strict coding standards and every line of the code is manually code inspected by multiple developers to find security weaknesses and to make sure that the best secure coding practices are followed. Every line of code written goes to unit test, system test, security vulnerability test (using tools like Codenomicon and Nessus) and performance test on a daily basis. All 128T software code is written by developers in-house based in the US. There is no development or test that is outsourced to other companies or countries.

Requirement 7: Implement strong access control mechanism

128T routers provide strong access control mechanism based on user roles. Only users with the highest privilidege are allowed to make changes to the system security parameters. Most of the users are created with the least priviledge and will require approval from the admin user to elevate the priviledge level.

Requirement 8: Identify and authenticate access to system components

128T routers have strict control on the creation and role of a new system user. Only an admin user can create a new user to access the router and by default the new user get the least priviledged role.

The user access to the 128T router are strictly controlled using well defined roles. If a user fails to login after 4 attempts, the user will be locked and will not be allowed to access the system until an administrator re-enables the user. An idle user session will be logged out after 15 minutes of idleness. Users are only allowed to access 128T routers using SSH or HTTPS thus providing a secure mechanism for the transmission of the user password and other sensitive data. 128T also provide a mechanism for two factor authentication using the combination of password and single sign on (SSO) token or using LDAP/Active Directory.

Requirement 10: Track and monitor all access to network resources and cardholder data

128T platform supports Security Audit Log capability which will allow an Enterprise to track all the activities performed on the 128T platform, some of the activities tracked include:

- Login and Logout attempts
- Configuration adds, modify, commit or delete.
- Save and activate configuration

All the activities will be tracked irrespective of whether 128T platform is accessed through CLI, GUI, REST, NETCONF, SSH, or through SFTP. The security audit logs will be stored on the 128T platform on a secure fashion. 128T also provides a mechanism to transfer these audit logs securely to an external Audit Log Server.

Requirement 11: Regulary test security systes and process

128T routers goes through penetration testing on a regular basis with Industry standard pen testing tools like Codenomicon and Nessus. Also, 128T Product Management/Engineering team keep track of all the security vulnerability [CERT] and patch the software on a regular basis to address these vulnerabilities. 128T system is FIPS 140-2 level 1 certified and ICSA certification compliant. 128T router is also penetrated tested on a regular basis by a third party pen testing lab.

Requirement 12: Maintain a policy that addresses information security for all personals

128T follows a strict and a well defined mechanism for code delivery, code inspection, security vulnerability testing, pen testing with an external lab and follows a stringest process for testing the code for security vulnerability on a regular basis. 128T Product Management and Engineering team goes through security training on a regular basis to make sure that the best practices followed by the industry is adopted at 128 Technology.

SUMMARY

128T session based routers is the only platform in the Industry which provides true ZTS and hyper-segmented network architecture allowing organizations to achieve and exceed PCI-DSS compliance requirements. Given the fact that 128T solution integrates multiple middle-box functionalities (security, routing, firewall, VPN and load balancing) into a single platform, the overall network architecture will be simplified while minimizing the cost and time to achieve PCI compliance. With our software-defined, session-based and service-centric approach to routing, the 128T Networking Platform, delivers both Enterprises and Service Providers breakthrough results in end-to-end security, agility, cost and performance.