Zero Trust, Zero Touch
Enabling Security for Software-Defined Networking
November, 2019

Authors: Dave Dukinfield, Cisco Customer Experience Product Manager; and Pam Richardson, Cisco Technical Writer
Security, Integration, and Automation

Today, artificial intelligence, the cloud, expanding amounts of data, and increasingly complex cybersecurity threats are rapidly changing the technology landscape. Mobile users expect immediate, high-performance secure connectivity at all times, everywhere, and on any device. Security for these services must be integrated from the initial design and deployed as part of the orchestrated automation of these services thus ensuring the service provider’s security policies are implemented end to end.

Multi-Layer Security and Protection

Reliable, high-performance networks are essential for modern businesses. Every aspect of business is affected by network health and functionality, allowing employees and customers to access data and applications from multiple locations, with multiple devices.

Cybersecurity threats are becoming more sophisticated and dangerous across a broader attack surface—one that is no longer contained within well-defined perimeters. Figure 1 illustrates the necessity of even faster response and mediation to these increasing threats.

Figure 1. Slower Response = Greater Risk
Ensuring adequate security levels is not just a matter of deploying the right technology in the right place. It is critical to define proper procedures clearly, and make sure they are adhered to continuously throughout the entire security chain—particularly at an operational level.

Software-defined networking (SDN), a key to current Service Provider deployments, can simplify network control and operations by decoupling the control and data planes from the underlying hardware. By creating dynamic, programmable, logical network components, SDN can deliver dependable network services that are faster and easier to design, manage, and troubleshoot. This delivery needs to incorporate visibility into the control, data, orchestration, and management planes, raising alerts for abnormal traffic and allowing the operator to mitigate that traffic over an existing or dedicated plane. The goal is to reduce the time scale of threat/detection/response from days/weeks to minutes/hours while maximizing the agility of the operator tools to respond and mitigate.
Zero Trust, Zero Touch

Aligning to current Service Provider security policies, the SDN approach is a Zero Trust, Zero Touch network.

As a key enabler of business activity, the network must be designed and implemented with security at its foundation supporting the key business functions. To accomplish this, a complete, holistic approach is required—one that encompasses protecting networks, elements, services, and management, as well as data flows leveraging analytics, automation, and orchestration (Figure 2).

A defense-in-depth approach, where multiple layers of protection are established, driven by automation (see Figure 3). Security is about adoption of controls; the more controls that can be deployed and integrated into the network, the better our chance of mitigating potential threats.
• **Strong identity** is established to ensure that every network element (VNF, infrastructure, automation processes, people) that accesses the network has established the appropriate level of trust, including signed software and configuration.

• **Configuration compliance** to validate security posture for every network element, to ensure ongoing assurance as to status of security.

• **Segmentation of services** through security enclaves reflecting network structure, to secure data flows and contain potential security events identified.

• **Visibility** of activities of the management plane, control plane, orchestration/automation plane and resulting VNFs, OSS/BSS, and user activity for identification of potential anomalies.

• **Highly restricted access** to network elements contained through automated virtual management access layer.

• **Strong security perimeters** at the Internet and the RAN, to protect against external network attacks. Attacks can come from external networks and compromised users.
Network as Security Enforcer

Security Perimeter Gateway

Aside from traditional attacks against servers and caches (for example, via HTTP response splitting), new threat vectors arise in a mobile network. For instance, Distributed Denial of Service (DDoS) attacks can cause major disruption to the latencies on which service level agreements are based. DDoS would cause network outages with attacks on control plane (e.g. DNS or Policy functions). DDoS impact through disruption to the network and the service latencies is not unique to 4G. With 5G, peering is also distributed to the MEC (edge). Thus, DDoS capabilities need to be also deployed at the MEC to protect packet core functions (such as UPF), which have been moved out to this edges.

Vulnerabilities that might cause this would be through:

- Traditional attacks on hardware components of the infrastructure
- Application vulnerabilities
- APIs that are not properly secured
- Rogue nodes/elements within the architecture.

The core architectures of virtualized 4G or 5G also create entirely new security threat vectors arising out of virtualized mobile network components (including separate slices being created for various services), as well as exposure of the mobile network core components toward third-party applications and external Internet-facing interfaces. The Central Data Center (CDC) DMZ zone hosts an array of applications and services that communicate with services in the Internet—all of which must be protected.

Other aspects of the threat surface are external-facing interfaces (such as BGP peering points) and roaming interfaces that Mobile Network Operators (MNOs) use for interconnection between operators to allow their subscribers to roam between them. BGP monitoring is employed to perform route monitoring using key BGP
networking protocol metrics such as reachability and path changes in order to detect attacks like route hijacks or routing changes associated with DDoS mitigation (BGP flowspec). Roaming agreements are operator specific, but strong security procedures are needed to ensure protection on host network. Any malicious attack on the roaming partner’s network could compromise the host network.

Subscriber access to a safe Internet is vital in maintaining the network’s security posture. One way to keep this in check is to restrict access to malicious sites and applications by controlling DNS traffic queries. All DNS traffic must be checked for connections intended for malicious URLs.

All these threats can be mitigated by applying layered security, to protect and secure traffic to and from the Internet via the Internet-facing peering routers back to the DMZ.

A **Security Perimeter Gateway** offers many benefits:

- **Security in layers** (such as NGFW IPS and DDoS detection and mitigation) provides in-depth defense by containing threats detected in specific communication flows.
- **Integration of security control platforms** with network elements, which results in visibility and white-list control of known baseline communication.
- **Access on an as-needed basis** to the infrastructure for operations assures that windows of access are minimal at best.

**Secure Cloud Services**

Secure Cloud Services help make sure that an organization delivers and consumes cloud services with a high degree of security. For our current Service Provider solutions, we assessed data protection policies, user behaviors, and architecture to tailor a strategy that covers the following:

- VNF/Controller: Strong segmentation model, VNF security groups, isolation of functions and control flows, visibility into interfaces
- Infrastructure: Hardening NFVi, securing E-W traffic
• Network Services: Securing network interfaces, cloud interfaces, segmentation policy enforcement, peering and roaming interfaces
• Management: Securing application interfaces, cloud interfaces, segmentation policy enforcement, and visibility into interfaces
• Orchestration: Securing orchestration management and interfaces, visibility and policy enforcement into API access.

Securing the Mobile Backhaul

In our Mobile Backhaul (MBH) security design, we used the following principles to ensure strong design and implementation (see Figure 4):

• Segmenting/securing security planes:
  o User/Data Plane: Constitutes the transit data and addresses security of access and customer use of the service provider’s network. This plane also represents actual end-user data flows. End users may use a network that provides connectivity only. They may use it for value-added services such as VPNs, or they may use it to access SP network-based applications.
  o Control/Signaling and Orchestration: Protects activities that enable efficient delivery of information, services, and applications across the network. It typically involves machine-to-machine communications of information, which allows the machines (such as switches or routers) to determine how best to route traffic across the underlying transport network. Orchestration will be extended to the MEC and needs proper MBH defense.
  o Management: Protects OAM&P functions of the network elements, transmission facilities, back-office systems (such as operations support systems, business support systems, customer care systems), and data centers. This plane supports the fault, capacity, administration, provisioning, and security (FCAPS) functions.
• Confirming identity of communicating parties. Neighboring nodes should be regarded as hostile unless trust is established.
• Offering ACLs for flows between authorized end-points without being diverted or intercepted.
• Providing authorized access to network resources through Multi Factor Authentication (MFA)

Figure 4. Securing Mobile Backhaul through Slicing and CUPS Implementation

Mobile Services Overlay

Modern MNO architecture is considered as an underlying infrastructure for numerous service overlays – Mobile Services being one (see Figure 5). All network elements on the Mobile Services overlay must align with the following:

• Comply fully with 3GPP Standards–preferred release 15 (minimum release 13), ITU – T X.805
• UE to authenticate and access services via the network securely (including 3GPP and non-3GPP access), particularly to protect against attacks on (radio) interfaces
• Allow network nodes to securely exchange both signaling (control) and user plane data
• Secure the user access to mobile equipment
• Verify that applications in the user and provider domains exchange messages securely
• Ensure that the Service-Based Architecture (SBA) architecture network functions communicate securely within the serving network domain, as well as with other network domains
• Inform user whether a security feature is in operation.

Each service that Service Provider’s automated orchestration deploys must meet or exceed these requirements to ensure security of user/applications, as well as the four key network planes (User, Control, Orchestration, Management).

Figure 5. Mobile Services Overlay
Zero Trust

Common Security Services

Security as a Service (SaaS) gives cloud provider and managed security service providers the opportunity to create subscription-based, “as a service” offers based on Cisco® Security products into a corporate infrastructure. SaaS providers can:

- Drive adoption of controls through automation into enterprise infrastructure
- Create federated Security services to support technology of enclave (mutually enhance each federation member’s security posture)
- Leverage common investments of exiting functionality in network for visibility and control
- Inherit trust of shared service for Network solutions.

VNF Security Services

Figure 6 illustrates the VNF Security Services for a given MNO. SaaS encompasses a secure enclave around these user services. These services are based on secure standards and deployment.

- **Visibility services** ensure that only allowed endpoints can specifically communicate.
- **Prevention and detection systems** capture and mitigate malicious or suspect traffic with involvement from the Security Operations Center (SOC).
- **Secure access** based on strong identity services allow trusted engineers the ability to update and troubleshoot.
Identity Management

A Service Provider’s **Identity Management** systems (see Figure 7) give administrators the tools and technologies they need to change a user’s role, track user activities, create reports on those activities, and enforce policies on an ongoing basis. These systems are designed to provide administering of user access across an entire enterprise, and to certify compliance with corporate policies and government regulations. Administers can:

- Maintain asset management processes for all entities on the network
- Conduct strict management of local accounts
- Provide unique certificates for all entities for identification and authentication
- Leverage certificates for identification, verification and data flow protection.
Chain of Trust using PKI

Public Key Infrastructure (PKI) is built on the concept of a trust model. When presented with a new public key, an entity must have some basis for deciding whether to trust that the key presented is associated uniquely with the presenting entity.

With SSL-secured HTTP or SMTP, S/MIME, and similar services, this trust is based on a centralized, hierarchical trust model known as a trust chain. The presenter has had its public key validated and signed by a third party whose key is known to the recipient and trusted to make such decisions.

An on-premises Certificate Authority (CA) solution will be deployed at the providers data center (Figure 8). An offline root CA will issue certificates to a number of subordinate CAs. Certificates will be for a specific purpose:

- User certificates
- Devices and Services certificates for CDC
- Devices and Services certificates for non-CDC locations
All CAs will store their private keys in hardware security modules (HSM). Whenever feasible, certificates will be used to provide strong identity to hardware, services, and users.

This chain of trust solution covers the following:

- Trusted access for infrastructure, network endpoint, workload, and users
- Enforce controls across the entire operating environment
- Trust will directly influence what an entity can access
- **All** traffic, regardless of location, is *threat traffic* until it is verified (authorized, inspected, and secured)
- Least privilege strategy and strictly enforce controls
- Context-based set of smaller decisions. Give minimal trust to entities to complete requested action
- Implement inventory-based access control as a function of user requirements.
Secure Configuration Management

With Secure Configuration Management (Figure 9) we validate security posture for every network element to confirm ongoing assurance as to status of security. This process covers the following topics:

- **Hardware**: Does the device contain the hardware components that are expected? Includes checks of the hardware inventory. See Cisco Trustworthy Solutions to address this requirement.
- **Platform**: Is the device authentic? Includes verification of secure boot process and identity of the device using Boot Integrity Visibility. Again, Cisco Trustworthy Solutions utilizes secure boot of signed images and Trust Anchor module.
- **Software**: Is the software used by the device authentic? Includes checks of the software files (signed images verified against PKI) and in-memory contents.
- **Configuration**: Are there any unexpected changes in the device configuration? Includes checks of the running configuration (signed configuration verified against PKI).

*Figure 9. Secure Configuration Management*
Security Segmentation

Security Segmentation is the first step to intuitive networking for Security (Figure 10). It comprises the following six categories.

Enclave Architecture Strategy

Each service being deployed must be reviewed under the following security analyses to assure the service is fully understood. This protects both the user service and the underlying mechanisms that make up the functional service. These analyses are mandatory for each service to establish zero trust while enabling the service.

- Enclave definition
- Asset classification
- Use Case identification
- Threat identification
- Functional requirements for controls
- Security control inventory and gap.

Functional Approach

Once analyzed, the service is reviewed for functionally to confirm that it meets the intentions of the Service Provider, as well as its integration into the existing infrastructure.

- Network domain services
- Access technologies
- Business functions
- Mobile services overlay
- Traffic plane separation.
Intelligence

Analytics are key to detecting malicious traffic. They also help monitor control, orchestration, and management plane traffic for baseline white-listing control. Additionally:

- Active analytics enable effective response to threats
- Security metrics and reporting provide intelligence to inform security investment and possible future security solution requirements.

Policy Enforcement

Security policy exists in almost every function of an infrastructure. It is important to have a common enforceable policy that spans across all systems and their associated policy enforcement methodologies. Once implemented, this policy should be periodically reviewed and updated. From Cisco, these methodologies will include:

- Data masking and tokenization
- White-listing enforcement through ACI or Tetration
- ACLs (VLAN ACL/Router ACL/Port ACL)
- Secure group tags
- Firewall tech
- Application layer inspection: Application FW
- SGACLs
- Network Functional Virtualization

Isolation

Segmentation of the key data planes (user, control, orchestration, and management) ensures service continuity and infrastructure lifecycle protection. The segmentation architecture must deliver the service and be designed to implement the Service Provider’s security model.
Following are some methodologies that are used to deploy segmentation. These must be in coordination with the complete end-to-end design, including overall security policy. Automation of these methodologies ensures consistent implementation of the required policies.

- VLANs and PVLANs
- VRFs (MPLS)
- VDCs, VPCs, OTV
- [m]GRE / IPSec / DMVPN / GETVPN
- VXLAN (STT, NVGRE, NSH, etc.)
- Service Chaining

**Security Automation**

Inserting security safeguards throughout the service model should be instrumented along with automation of the service itself. **Security orchestration** should include elements of validation of new and updated hosts for best security practices. This process informs the monitoring and identity systems of these changes in order not to flag new but trusted system components. It also updates segmentation controls to let these endpoints communicate with the allowed hosts only (white list updates). Service Providers should see security automation as a process to:

- Develop operating model to support agile Security architecture
- Instrument for hyper-transparency
- Orchestrate and automate Policy and Response.
Visibility

Visibility across threat vectors is critical; you cannot find what you cannot see. Intrusion Protection Systems (IPS) accurately identify, classify, and stop malicious traffic, including worms, spyware, adware, network viruses, and application abuse, before they affect service offerings and their resiliency. This collaborative IPS should include:

- Cross-solution feedback linkages
- Common policy management
- Multivendor event correlation
- Attack path identification
- Passive/Active fingerprinting.
To ensure visibility across the network, one should construct the following controls:

- Implement a logging system that records events relating operation of the environment
- Implement regular monitoring to verify the expected behavior of devices (baseline)
- Set parameters to detect potential anomalies in behavior that suggest malicious behavior
- Analyse log information against known threat telemetry
- Undertake threat hunting to look for indicators of potential threats
- Conduct periodic audits and reviews of security controls to certify that controls are effective
- Apply multiple lenses of controls to increase detection and enable complex “what if” analyses.

**Zero Touch**

**Security Orchestration**

Security Orchestration safeguards secure hosts, secure segments, knowledge of those hosts and segments by monitoring systems, proper isolation and monitoring of those segments, perimeter protection from attacks, and mitigation of violations and attacks. Security orchestration for the project’s lifecycle provides the following advantages (Figure 11):

- **Posture**: Provides an accurate, up-to-date view of all network elements
- **Compliance**: Drives security policy consistency in controlled deployment
- **Reports and Metrics**: Known exemptions and potential areas of exposure
- **Prevention**: Management by exception focused on anomalies (e.g. white list enforcement)
- **Response time**: Known configuration, enabling easier action identification.
Integration leads to automation; automation leads to visibility and subsequent analytics for faster response time (Figure 12). This allows you to automate the following SOC tasks:

- Escalation and notification
- Advanced analytics
- Environment context
- Case management
- Data enrichment
- Adaptive response.
Next-Generation SOC

Security Operations Center

The SOC is established to help prevent, detect, assess, and respond to cybersecurity threats and incidents (Figure 13). It provides, at minimum, the following services:

- Aggregated dashboard and management platform for security operations
- Security Incident Response facilitation by providing relevant information and details
- Cyber security analytics
- Cyber threat intelligence
- Security service management.

Figure 13. SOC Architecture
SOC provides a broad range of services—from monitoring and management to comprehensive threat solutions and hosted security that can be customized to meet customer needs. The next-generation SOC requires more than basic SOC and/or Security Information and Event Management (SIEM) services (Figure 14). Massive amounts of telemetry data and event logging fed into multivendor event correlation, as well as attack-path identification and passive/active fingerprinting. This results in real-time analysis and mitigation for the Next Generation SOC.

Figure 14: Next-Generation SOC Requirements
Driving Cloud Native Customer Experience (CX)

The Cisco CX team has been instrumental in the incubation of the cloud-native architecture. The CX team has set-up a program and architecture management office (PAMO) that is responsible for the end-to-end design, solution validation, test automation, and deployment and management of workloads. The main focus is outcome-based program success. We are deploying new tools and methodology using continuous integration and continuous deployment.

Integrated automation is a key requirement to manage this next-generation network. The CX team has developed full-fledged, closed-loop automation with full lifecycle management using Network Service Orchestrator and Elastic Services Controller for more than 100 VNF types (10,000s of instances) in network. The team also implemented the world’s first fully automated virtualized RAN deployment, which reduces the time to deploy a radio site from weeks to a matter of minutes. It allows management of more than 150,000 macro- and small-cell radio sites without manual intervention.

CX is redefining the software delivery methodology of virtualized mobile network solutions to Service Provider Customers with a software-defined test framework. It integrates unified delivery of all VNFs from Cisco and our partners to Service Provider’s solution lab in an agile fashion. The KPIs captured in the portal include health, licenses, reservation of resources, and vendor score cards.

We are deploying on-premise software platforms for accelerated development and evolution leveraging the CI/CD tools used in CX with more than 300 customers as an extension to our customers. It gives the Service Provider access to the Cisco Engineering teams to refine and obtain innovative features using an agile delivery model.
Security is designed based on the principle of “zero trust, zero touch,” which implies invisible security with full automation. The CX team has deployed security tools integrated into VNF deployments so it is embedded into the overall solution. Security updates with workflow changes so all transactions between network entities are secured—while minimizing the operational burden by making these security constructs transparent to all end users.

There is finally an effort to define organization and models for cloud operations. The objective is to manage the lifecycle of the network while keeping a steady operational staff with a small footprint. We are using DevOps systems with site reliability engineering practices and distributed cloud operations to self-manage the entire infrastructure.
Learn more

To learn more, visit cisco.com/go/5g.