Layered Security for Converged Rural Service Provider Networks

New services, new security challenges

Today's consumers expect seamless Internet experiences for their growing consumption of video, cloud, mobility, and Internet of Things (IoT) services. To meet the demand for these performance expectations, rural service providers are considering converged network architectures to simplify their network management, scale, resiliency, automation, and security.

As rural service providers look to secure new revenues by supporting new services, adding more devices and traffic flows creates additional points of vulnerability and increases the risk of network exposure. Poor security leads to network exploits used to gain access to, or steal, sensitive data sets. For the service provider it results in brand reputation damage, fines, and lost revenue.

As networks grow, so does their threat exposure

As bandwidth demand grows, it will be challenging to build secure networks unless the underlying infrastructure is built to circumvent threats and attacks. Some smaller network designs utilize more traditional and secure infrastructure locations, but as traffic demands grow, service providers may be forced to place infrastructure elements in less secure locations to bring content closer to consumers. These less-secure locations could introduce additional threats to the network.

Protecting critical infrastructure

Governments are recognizing the critical nature of communication networks and have gone so far as to label them 'Critical Infrastructure' – those systems that support integral services like healthcare, banking, emergency response, and national operations. Protecting them from hijacking and infiltration should be a paramount concern for service providers. Loss of integrity in the underlying infrastructure for any of these services could have a devastating impact, crippling emergency response operations or economic functions.

To build more cyber-resilient networks that protect critical infrastructure, service providers should focus on building layers of security, developing a trustworthy network, and verifying the network's trustworthiness.

Layers of security

Service providers today require holistic security protections integrated across multiple levels within the network. Key is a security architecture that provides defense-in-depth and is applicable to evolving parts of the network such as cloud-native services and other virtualized aspects, including orchestration and automation.

The layers of a security posture will vary based on the unique needs of the network. In general, they focus on the following places in the network:

1. Domain Name System (DNS) and IP layer protection
2. Peering exchange points and network access security
3. Internal Data Access Protection

1. DNS and IP layer protection

DNS layer protection maintains assurance that your Border Gateway Protocol (BGP) route broadcasts remain under your control and are working to automatically block malicious domains from being reachable or generating traffic to your network. If hackers hijack your BGP routers then traffic destined to your network will be compromised, damaging your services. Important or sensitive information will fall into the wrong hands, or your clients will fail to deliver on their business agreements.

Distributed Denial of Service (DDoS) mitigation services measure a baseline-normal traffic pattern within the gateways to the network. Once a statistical variation is noticed, the mitigation service can automatically intervene and remove false traffic. Because DDoS attackers use hijacked IP addresses of IoT devices to build a bot army, monitoring the integrity of your BGP routers can prevent your IP scope from being used maliciously. Aside from protecting your IP scope, DDoS mitigation's main purpose is to ensure that your network is still reachable at your public peering points. If a service provider's gateway is flooded with false traffic, then access to hosted cloud services becomes limited and customers of the operator's network also suffer reachability from outside networks. This situation can be catastrophic for e-commerce transactions or emergency response needs.

2. Peering exchange points and network access security

To meet the demands of hyper connectivity, service providers are building more localized peering points or Wi-Fi access points. These deployments are designed to improve connection access and end-user experiences. More access points into the network demand more effective security practices.

To protect traffic at the edge of the network, where equipment will be housed outside their physical security perimeter, service providers should consider implementing Media Access Control Security (MACsec). MACsec is an Institute of Electrical and Electronics Engineers (IEEE) industry standard security technology that can protect communications for traffic using Ethernet frames or links. Since it operates at Layer 2, it can be used to secure multiple different higher-level protocols. For example, MACsec can mitigate sniffing, man-in-the-middle, and replay attacks which are possible on IP edge networks between small cells and the carrier's core network. MACsec can be used to encrypt all traffic on an associated link, so any party attempting to monitor the traffic cannot see the Ethernet frames nor any of the data riding in them. It also provides data integrity and data origin authentication to ensure traffic isn't tampered with and is only allowed from other trusted switches and endpoints.

As traffic moves from the edge towards peering exchange points, it can be filtered from malicious traffic using next generation firewalls with capabilities such as Deep-Packet Inspection - Secure Socket Layer (DPI-SSL) for encrypted traffic flow. Leading firewalls use integrated cloud enhancements to receive near real-time signature updates for newly discovered threats which helps ensure their efficacy. Automated signature updates pushed out to your security devices by global threat response teams mean reduced Operating Expense (OpEx) and Median Time to Detect (MTTD) malware or other emerging threats. Using these live signature updates allows the firewall to quarantine questionable payloads and send them to a sandbox for investigation. The sandbox is connected to a global threat response center for review, and if a global update is needed then the manufacturer publishes the patch. A service provider's threat intelligence is then expanded to protect them not only from threats seen on their network, but also those seen by global network operators that use the same threat response center.

Once traffic is past the firewall and moving through the network, service providers can implement behavioral evaluation techniques to detect malicious activities. Most networks have a regular traffic flow pattern that can be seen throughout the day. A Security Information and Event Management (SIEM) system can detect traffic pattern anomalies on east-west traffic flow (traffic flows internal to the service provider network). Using this anomaly detection protects against bot agents that wait to be activated, or ones that use quiet hours to transmit data out. SIEM systems can also monitor traffic flows for irregular patterns that identify irregular machine-to-machine traffic to detect worms or other programs designed to infiltrate networks with a goal of gaining access and control.

3. Internal data access protection

Network slicing is an architecture allowing operators to run multiple logical networks as virtually independent business operations on a common physical infrastructure. Network slicing requires strong isolation between the slices and isolation within the components to prevent vulnerabilities from allowing malicious attacks to spread to other components within the slice(s).

A network slice architecture allows a quarantined slice of questionable traffic to be set aside and analyzed. Software-defined segmentation makes it possible to enforce unique access policies for users, applications, IoT, and Machine to Machine (M2M) devices as well as enterprise network devices. Security tags can be defined and managed by a centralized security policy server. This approach shifts the network security away from depending on long lists of IP addresses to a flexible, more easily managed, and more effective automated model that protects against new and expanding threat vectors.

Segmentation is a form of zero-trust policy for internal data protection and access control. Implementing a zero-trust framework around internal resources and applications allows micro-segmentation and fine-grained security controls. A zero-trust framework alerts you to a

policy violation through continuous monitoring and response to indicators of compromise. The framework includes maintaining software-defined access control over all the connections within your applications. The access control is based on user, device, and application context, not location, which helps prevent backdoor access to sensitive data because the device IP resides on the network. This model allows mitigation, detection, and response to risks across your infrastructure regardless of distribution or location.

Another area of focus for network-access protection is Multi-Factor Authentication (MFA) access. Implementing MFA as part of a zero-trust framework on internal network databases and applications provides more granular controls to restrict lateral exploits. It is the one-bad-actor instance that compromises sensitive data and destroys a provider's brand reputation. The extra step of token authentication, or a push-notice confirmation, could be the tool that prevents a data compromise.

Attestation for trustworthy networks

What if your critical infrastructure is hijacked from inside the hardware? This is more than a bad actor obtaining user credentials and gaining access to restricted elements; this is gaining persistent control of a network router from the day it is powered up. The concept of a trustworthy network relies on being able to verify and validate that the hardware and software used in the operation of the critical infrastructure are genuine and operating as intended.

With new cyber security threat vectors coming from manufacturing exploits, having a hardware and software partner that operates Secure Development Lifecycle (SDL) in the manufacturing process is critical. With SDL, products contain security features embedded throughout their product lifecycle and resiliency against today's sophisticated manufacturing supply-chain attacks. From concept to production, the network infrastructure platform products are designed for security based on a trustworthy framework.

The first step in establishing platform security is platform identity, which is performed using a Trust Anchor module (TAm). Originally developed to protect against counterfeiting and supply chain attacks, the TAm is a tamper-resistant chip providing secure on-chip storage, random number generation for encryption, and a secure unique device identity for authentication. The TAm is used to enable the following security features in hardware routing platforms:

- Secure boot and image signing: The hardware-anchored secure boot process is designed to ensure that only genuine, unmodified code can boot on the platform. Secure boot uses digital signatures and private keys to authenticate the code before proceeding. This creates a chain of trust from the micro-loader to the operating system, establishing the software authenticity and integrity. All signatures are verified using keys stored securely in the TAm at manufacturing time. If any of the digital signature checks fail, the device doesn't allow the software to boot.
- Runtime defenses: Using Integrity Measurement Architecture (IMA) ensures that executables preparing to run were not modified from their original form. IMA uses a runtime measurement list of the executables' integrity values and anchors them in the TAm. The benefit of anchoring these aggregate integrity values in the TAm is that any software attack on the measurement list is detectable and indicates a compromise to overall integrity.
- Supply chain security: An imprint database is a master list within the TAm that stores the unique identification of major components such as Application-Specific Integrated Circuits (ASICs) and Central Processing Units (CPUs), with their device types specific to that board. If the observed identification does not match the imprint database, then it is an indication of breach and is reported to the host for appropriate action.

Layered security for converged networks

Security, resilience, and trustworthiness are essential to converged service provider networks. Cisco uses a trustworthy framework that embeds security throughout the lifecycle of our solutions and enables a security architecture that can be integrated across multiple levels within the network. Our comprehensive approach includes DNS and IP layer protection, network access security, internal data access protection, and trustworthy technologies to enhance the security of rural service provider networks.

Learn more

Explore our security portfolio of products: Service Provider Security Solutions

Build a trustworthy network with Cisco Built In Trust

Explore all of our Rural Broadband Network Solutions