Securing and Automating Smart Cities

Cities are getting smarter. And they need to be.

Faced with population growth, growing economic disparity, fears about climate change and an increasing digital divide, cities across the globe are looking at digital transformation in order to achieve better environmental, social and financial outcomes (IDC).

Smart Cities help achieve these objectives by linking devices, applications and people to streamline city functions, enhance communications and provide better services to its citizens. The proliferation of Internet of Things (IoT) devices/sensors is making it easier to monitor and control municipal functions like parking, traffic, lighting, policing, water and energy flow and garbage removal. However, the real power lies within the data collected from these IoT devices which offer a much more granular and in-depth understanding of city functions. This data can be invaluable in future planning initiatives and in achieving the desired long-term outcomes.

Public safety is an important component of the Smart City, with many cities expanding their deployment of video surveillance to both deter crime as well as collect invaluable information from specific locations or events. Enhanced public safety can also include connected policing — with videos from dashboard camera, body-worn cameras and other feeds — to give those in command a multi-dimensional view of what is happening on the ground.

Throughout the Smart City are Smart Buildings which deliver energy and costs savings by using automated processes to control buildings' operations including heating, ventilation, air conditioning, lighting, security and other systems — while at the same time improving the comfort for its occupants.

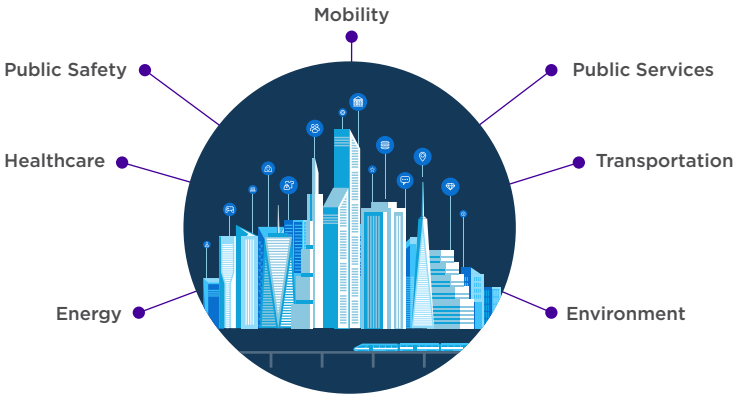

Figure 1: Smart City

The interconnection of IoT devices, applications and people for the Smart City implementation is highly dependent on the right network infrastructure. And that dependence increases as more and more critical services, data, devices/and sensors are brought onto the network — demanding new levels of efficiency, performance, availability and security.

Extreme Networks' Secure Automated Smart City Architecture offers a number of key attributes to help local governments implement their Smart City initiatives. This paper will examine each of these:

- Simple and Automated Network; Increasing efficiency and reducing costs
- Inherent Network Security through secure zones and stealth networking
- Scalable and High Performance Video Surveillance that can be deployed with ease
- High Performance Wireless that is simple to deploy and manage
- Visibility, Control, and Security for IoT devices
- Centralized Management, Control and Analytics — with a true 360 degree view of the network

Simple and Automated Network; Increasing Efficiency and Reducing Costs

As the goal behind Smart City initiatives is to increase efficiency, improve municipal services and reduce costs, it's important that the network infrastructure also support those goals. The foundation of Extreme Network's Secure Automated Smart City Architecture is an innovative networking technology called Fabric Connect. Fabric Connect represents a simpler way to design, build, manage and troubleshoot networks that has been field proven to reduce operations costs by as much as 66% while at the same time increase time to service by 11x[2]. It is standards-based, network virtualization technology that enables multiple isolated, secure virtualized networks to run as "ships in the night" over a single physical network. These virtualized networks are inherently secure and can be set up and changed very quickly with edge-only provisioning, eliminating instability and the risk of errors.

In short, Fabric Connect offers cities network-wide automation that provides simple "plug and play" operation — while at the same time improving both the stability and the security of the network. Specific attributes of Extreme's Fabric Connect technology include:

- **Just 1 protocol, instead of 4-6:** Extreme Fabric Connect delivers the full breadth of L2/L3 networking services via a single protocol. The result is a dramatically simpler, single technology network, which is far easier to build, manage, and troubleshoot.
- **Single network-wide technology with a simplified end-to-end service delivery model:** Services can be easily deployed through end-point provisioning only at the points where users and application attach users and application attach, increasing service deployment speed and agility, while reducing design complexity.
- **11x Faster Time to Service:** Since Fabric Connect only requires service changes at the edge of the network, it eliminates error-prone and time-consuming hop-by-hop configuration practices.
- **Enhanced Business Continuity:** The elimination of overlay protocols profoundly impacts network reconvergence times. Extreme Fabric Connect customers experience a vast improvement in average recovery times over conventional multi-protocol networks.
- **Flexible network topologies:** Extreme Fabric Connect works over any physical topology whether it is a ring, mesh, partial mesh or all of the above.

Inherent Network Security Through Secure Zones and Stealth Networking

Continued investment in digitization and IoT has huge implications on security — which continues to be the single biggest focus of CIOs across both state and municipal governments. As more devices connect to the network, the potential attack surface widens, and new security measures need to be considered.

One very effective means of securing the network is through network segmentation. According to Rob Joyce, former NSA official, "A well segmented network means that if a breach occurs, it can be contained. The difference between a contained and uncontained breach is the difference between an just an incident and a full-blown catastrophe." In the Smart City environment, the isolation and security of critical functions such as traffic control, smart grid applications, water management and more — is an absolute necessity.

Extreme Fabric Connect enables the creation of thousands of private virtual networks to protect and isolate these critical services. Each of these virtual service networks (VSNs) is completely isolated without any IP reachability in or out (unless specified). And as an added benefit, these secure virtual networks can be deployed quickly and without complexity at the network edges.

Some of the attributes of this capability include:

- **Breach containment and prevention of lateral movements** – The ability to create thousands of secure zones that can extend across the network infrastructure (from point of ingress to point of egress) offers the ability to isolate traffic by different service types, applications or IoT devices. In the event a breach occurs, the vulnerability remains isolated within that segment, preventing potentially catastrophic lateral movements.
- **Dark network topology enabled through stealth networking** – With Fabric Connect, secure zones are dynamically created with L2 Ethernet Switched Paths. These paths are therefore not vulnerable to L3/IP scanning/hacking techniques — ensuring that if breached - the end-to-end network topology is hidden.
- **Elimination of back door entry points** – With Fabric Connect, services extend and retract dynamically as corporate assets, IoT devices, and authorized users connect and disconnect. Network configuration profiles are removed from access edge switches and wireless access points as users/and devices disconnect from the network — reducing back door entry points and potential network vulnerabilities.

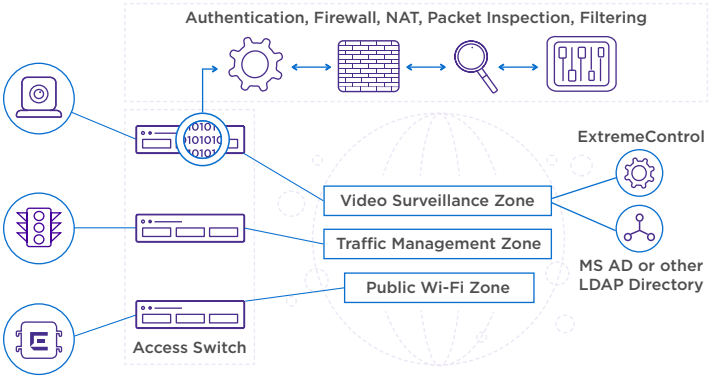

Figure 2: Segmented Zones for Smart City Functions

Scalable and High Performance Video Surveillance Deployed with Ease

Security and safety are direct influencers on the quality of living within the city and its surroundings. Video surveillance is a major contributor to this with many cities expanding its deployment.

Today, smarter IP cameras provide greater capabilities beyond generating and transmitting video, they can also communicate with centralized management systems delivering video analytics output, alarms, and metadata alongside the video stream. These smarter video surveillance systems need the right network infrastructure to ensure the scale, performance and quality of the video. Designed to simplify any video surveillance solution (IP, hybrid, unicast or multicast), Extreme Fabric Connect ensures that the network is ready to handle even the most complex city-wide video surveillance deployments.

Some specific attributes of this solution include:

- **Simplified deployment:** Fabric Connect eliminates network-wide provisioning practices common in today's IP-based surveillance networks. Provisioning is required on only the ports attached to cameras and monitoring stations/and receivers — with no need to provision any core switches in between. This not only reduces the risk of an outage due to human error during change but also allows the video surveillance network to be deployed faster and easier than ever before — with the ability to add, move and change cameras on the fly.
- **Real-time streaming:** Once the end points are provisioned, the network determines the shortest path from the sources (the cameras) to the destinations (monitoring stations) with optimized network path delivery, thus improving video delivery performance over traditional networked-based solution.
- **Better resiliency:** Extreme Fabric Connect eliminates gaps in video streams by delivering sub-second reconvergence resulting from network outages. Traditional IP network reconvergence can range anywhere from a few seconds to minutes based on topology, while Extreme Fabric Connect offers sub second recoveries for both unicast and multicast routing. Therefore, single link or nodal failures are completely transparent to the video surveillance application.
- **Supports massive numbers of cameras:** The ability to support tens of thousands of unicast/and multicast streams, with very limited impact on switch processing is advantageous for Extreme Fabric Connect customers. This differentiated ability delivers both implementation and operational cost efficiency compared with traditional unicast/multicast networked solutions

High-Performance Wireless that is Simple to Deploy and Manage

According to IDC, public Wi-Fi is the most widely deployed Smart City use case and it is a great starting point in connecting citizens, businesses and visitors. However, Wi-Fi is also critical in enabling many other smart city applications such as public safety, IP Video, traffic and parking controls, air quality and many others.

Extreme offers powerful 'best fit' Wi-Fi offerings that deliver superior quality of experience to mobile users and that can adapt to the diverse wireless requirements and environments typical in any Smart City deployment.

Key capabilities include:

- **Single pane of glass management** for wired and wireless environments that can be deployed on-premises or virtually in a public/or private cloud environment.
- **Common fabric-based architecture** that supports the ubiquitous deployment of secure network segments across wired and wireless as well as the dynamic auto-attachment of users/and IoT devices into the assigned fabric-based service or secure segment.
- **Investment Protection –** With consistent wireless hardware, management and services across public, private and hybrid cloud, Smart Cities can adapt their deployment model — gradually evolving from on premise to cloud — without needing to change their access points.
- **Pervasive Intelligence –** Extreme provides the intelligence Smart Cities need to better engage mobile users and drive both business and operational transformation. Delivering pervasive APIs, the data insights and contextual information needed to personalize engagement can be enabled. By augmenting machine intelligence with human intelligence, Extreme modernizes operational environments shifting the focus from 'Managing the Network' to 'Managing City Services'.
- **Supports multiple IoT wireless technologies -** Many of Extreme's APs include integrated BLE/802.15.4 radios to enable on-boarding and securing of BLE and Thread enabled IoT devices. In fact, Extreme is currently the only Enterprise WLAN vendor to support the Thread Networking Specification for Smart Building/and Smart City IoT implementations.

Visibility, Control, and Security for IoT Devices

In a Smart City implementation, the network must be capable of connecting the broad range of IoT devices and users, however, it must be very selective in doing so. Authorized IoT devices should be expeditiously and effortlessly on-boarded, while unauthorized devices must be prevented from gaining access to the network. The best way to implement this is with policies that define which devices, users, and apps can access the network resources — with this policy implemented consistently across the network.

ExtremeControl applies granular controls over endpoints that are requesting on-boarding to the network. ExtremeControl matches endpoints with attributes, such as user, time, location, vulnerability, or access type, to create an all-encompassing contextual identity. Role-based identities follow a user or IoT device, no matter from where or how it is connected to the network. Compromised devices are quickly identified and quarantined from the network.

In addition, isolation of groups of IoT devices performing a specific function or role is supported by assigning each of these functions their own secure segment. This not only protects the rest of the network and applications from that particular group of devices, it also enables much better visbility and control over the traffic within that specific segment. ExtremeControl working in conjunction with Fabric Connect automatically identifies, classifies and onboards the IoT device, applies policies, then provisions an end-to-end secure segment (L2 or L3) from the point of ingress to the point of egress. As an added benefit, full network service automation and dynamic secure attachment of wired and wireless IoT devices is delivered — dramatically reducing provisioning at the edge of the network.

Finally, to enhance security of IoT devices (specifically aging wired IoT devices), Extreme Defender for IoT controls IoT device network access by applying and enforcing device profiles, and isolating IoT into secure zones. It works with Extreme Fabric Connect to create secure zones that can be deployed quickly and easily at the network edge, or can work over third party networks isolating groups of devices in IPSec tunnels.

Centralized Management, Visibility, and Control

In the Smart City environment, centralized management, visibility, and control is critical to ensuring that the network delivers the desired efficiency and cost reduction objectives. Extreme Management Center provides a true 360 degree view of the wired and wireless network, users, devices and applications with context and scale through integrated management, analytics, and policy. It is designed to provide granular insights, visibility and automated control across the network — from the wired and wireless edge all the way to the data center in order to steamline and simplify network operations.

Extreme Management Center consists of the following components:

- **ExtremeControl:** As mentioned in the section above, locates, authenticates and applies targeted policies to users and devices as they connect to the network

through a single integrated user interface.

- **ExtremeAnalytics:** Speeds up troubleshooting by separating network from application performance so you can quickly identify root-causes. It monitors shadow IT, identifies and reports malicious or unwanted applications, and assesses security compliance.
- **ExtremeManagement:** Offers a single pane of glass for the entire wired and wireless network — data center to edge. Zero-touch provisioning automates complex provisioning, reducing time to service and reducing error.
- **Information Governance Engine:** Analyzes and assesses network configurations to help determine HIPAA, PCI and GDPR compliance readiness across the wired and wireless network.

Summary

Extreme Networks is helping cities across the globe digitally transform so that they can achieve their desired environmental, social and financial outcomes. We understand that the right network infrastructure is paramount in facilitating this transformation and that it assist in increasing efficiency, improving service and reducing costs. Extreme Network's Secure Automated Smart City Architecture achieves these objectives, helping local governments do more with less.

For more information on how Extreme Networks can help, please contact your local representative or visit www.extremenetworks.com.

Extreme™
Customer-Driven Networking

http://www.extremenetworks.com/contact