Lippis Report

Research Note

## Lippis Report 168:

# Cisco Pulls All the Pieces of Its Network Security Program into One Architecture: SecureX

By Nicholas John Lippis III
President, Lippis Consulting

March, 2011

Cisco recently launched its SecureX architecture that extends perimeter-based network security to secure modern IT, recognizing the huge growth in mobile and cloud computing. SecureX is a multi-layer architecture built upon Cisco's AnyConnect client, its global footprint in real-time threat intelligence found in SIO (Security Intelligence Operation), Cisco TrustSec, including policy servers of NAC manager and server appliances, ASA firewall and the security enforcement features of its switches and routers. SecureX is an architecture to Cisco's network security products and service to work together in an effort to create deeper defenses and contain exploit infestation if, and when, they occur. Fundamental to SecureX is the concept of "context aware" policy across the enterprise, including remote endpoint devices, centralized policy creation with distributed security device and network enforcement. SecureX provides for innovation injection points through APIs (Application Programming Interfaces) for management and SIEM or Security Information and Event Management. In this Lippis Report Research Note, we explore SecureX with a focus on how context increases defenses and keeps IT assets safer.

SecureX offers something for everyone…such as a simpler, yet richer, management model for SecOps, deeper levels of security for users within and outside the corporate network, centralized policy creation that extends beyond the corporate firewall, and increased protections for users as they utilize mobile endpoints to access corporate and cloud-based applications.  IT business leaders should be pleased with better protections and compliance tools, especially as their vulnerabilities increase with mobile endpoints seeking network access growing.

SecureX is not just about extending security to mobile devices but to capturing contextual information in the use of policy creation. Contextual information includes user and device identity plus location, login time of day, plus which specific applications users attempt to access too, and this information is not only collected upon login but during their entire network connected session. Context aware policy allows IT leaders to use this information in the creation of policy with the end result of either allowing or denying access to IT resources, independent upon endpoint device and method of which access is attempted. And this context aware policy attribute of SecureX, over time, will be extend beyond normal data traffic streams to apply consistent unified policies to application, video or voice traffic also.

**The Future of Network Security: Cisco's SecureX Architecture**

PDF Get the White Paper

And while SecureX is security, in reality, it's bigger than just security, because security is a necessary integrated attribute to enable mobility, video, voice and web collaboration, etc. To create a secure IT environment, IT services need to interact with security services with minimum to no user intervention that steals productivity. In short, SecureX seeks to make Cisco security and network devices work better together through context aware policy so access and deny decisions are improved, and are built upon so that anomalistic behavior remediation is automated post access through traffic monitoring.

Use cases have changed dramatically since a new tier of computing has emerged, that being smartphones and tablets. For example, a laptop could be plugged into an iPhone, which is streaming video into the corporate network.  The network should be able to differentiate between data traffic, video traffic, phone traffic and even iPhone application traffic, then monitor all of those traffic types for behavior so if a Virtual Machine (VM) is launched on the laptop, the network recognizes this new entity and performs a new series of monitoring.  Security needs to be much smarter as the combinations and permutations of acceptable user behavior are fundamentally changing.

So where does this monitoring come from? Is it centralized, distributed, within appliances, in the cloud? The answer is all of the above. It's in the network infrastructure and highly distributed. The SIEM ecosystem plays a role, TrustSec provides monitoring as does SIO, ASA, IPS, etc. The network infrastructure itself is monitoring behavior that's outside of parameters/rules/policy that have been established for each network connection, and can take defined action when anomalistic behavior is identified. With monitoring and enforcement being so highly distributed, the chances of capturing anomalistic behavior increases significantly. Anomalistic behavior can occur anywhere, so depending upon where alerts are triggered, what type of traffic is involved, the kind of device being used, the location, the identity of the user, the time of day, etc., it's this contextual information that adds color to tripping anomalistic behavior and remediation options.

SecureX is much like Cisco's self-defending network concept, but with a global perspective and tools to extend contextual base security to the Cloud, virtualized environments and out to the growing mobile workforce. And this extension of security services is the biggest challenge with which IT business leaders struggle. IT leaders want to push context aware policy into their virtualized datacenters, their Cloud(s) and to mobile users, because it solves a large set of security problems. In fact, security concerns is one of the primary gating factors limiting enterprises from deploying these new innovative IT services that offer favorable business processes outcomes.

## Context Is Fundamental to Access Decisions

We already have perimeters and defenses within the enterprise, but IT has gone mobile, thanks to smartphones, iPads, tablets, etc. Also, applications are selectively moving into the Cloud as well. SecureX is a security architecture delivering control to SecOps and IT business leaders to extend their IT services to mobile workers, enabling them to embrace a new tier of computing and a new way of application delivery via the Cloud.

SecureX adds the concept of context aware policy to the principles of visibility and control as context provides insight into threats as employees are working outside of defined enterprise perimeters. The type of context that's important includes identity—such as who are you, where are you located, the device that you're using and can I trust the device—and what resources are you seeking to access. All of this contextual information needs to be considered when a firewall is determining network resources it will allow access to. In addition, contextual information may also instruct the network to enforce encryption on a session based on who you are and where you're trying to go.

## Policy Driven

To make contextual information work, a policy wrapper needs to surround context elements of personal identity, device identity, location, time of day and application access request. That is empowering the network to being able to create a uniform policy, such that the network is able to intelligently negotiate a variety of context options that are being considered when individuals attempt to access IT resources. This is the perfect job for a policy appliance.

To add context information to firewall decisions, Cisco is leveraging key pieces of its security product portfolio. For example, its TrustSec architecture provides access control plus encryption, which is the first and most critical piece of context information. Within access control, a device's security posture is assessed, the end user is identified, and their device is profiled, all of which is used to make an intelligent decision to grant or deny network access. In addition, the network can "tag" a user's data stream, so that as the stream transverses throughout the enterprise IT infrastructure, the network can enforce defined policy independent upon the stream's destination(s). For example, once the user has passed access control, should this user decide to search for a payroll server location, the network may recognize that he/she is not allowed access, thanks to defined policy, and the network can drop the requests and log the event. This set of sequences is a benefit of TrustSec.

## Access Control and Contextual Information

With trusted systems on the inside of an enterprise network providing enforcement through policy of mostly fixed endpoints, such as desktops and IP phones, the question on most IT business leaders' minds is how to extend these protections to the exponentially-growing mobile community and non-user network devices. IT leaders are confronted with an increasing number of both mobile endpoints and non-user endpoints, such as printers, video surveillance, wireless access points, etc., attempting to access their network and IT assets. To protect IT assets, IT leaders are seeking a process in which all devices connecting to the network, independent upon inside or outside the perimeter, are profiled to analyze device function and apply appropriate policy. For example, an IP camera may be identified during profiling and then a policy applied that allows IP cameras to transmit data, but not allowed to request data. In addition, during post access control, the network then monitors the IP camera to assure policy is applied while the IP camera is connected to the network.

This type of contextual information to build another level of defense is also extended to the virtualized data center environment. For example, once a virtual server comes online, policy can be applied to it, which is then communicated to the entire infrastructure. Policy may allow a virtual server to pass traffic between VMs on a select number of hypervisors. In addition, these VMs may also recognize that the new virtual server can do X and Y with these VMs but not Z. This level of control granularity enables SecOps to define virtual environment behavior in a meaningful way.

## The Network Can Be the Firewall

Clearly policy management is an integral component of SecureX. To define policy, Cisco offers the Cisco TrustSec solution, which can be deployed using the NAC Appliance or with a network-centric 802.1X strategy, combined with the Access Control Server. These solutions offer posture assessment, remediation and quarantine functionality. Device profiling for non-authenticating devices such as IP Cameras, printers, WLAN access points, etc., are placed on guest services with triple-A services. The aggregate of these features with the ability to create centralized policy that can be pushed out to the entire network infrastructure creates, in essence, a highly-distributed firewall. If a firewall's job is to allow or deny access to IT resources, then SecureX turns the entire network into a highly-distributed firewall, where every component of the network is now analyzing and processing traffic.

## Enforcement and Layers of Context

Context aware policy enforcement is performed with network infrastructure such as network switches, routing, firewalls, IPS, VPN, etc. There are layers of context: who are you, and should you be allowed to go to this website; or who are you, and what should I do with the types of email that you're creating, or the traffic you're generating based on who you are? It's a meta context environment that asks, "Who are you in a dynamic environment?" In this dynamic environment, a higher-level policy may ask, "When you're inside the network, there's one set of rules. But if you leave the network, policy moves and perhaps changes with you." For example, an exchange between two users may be allowed while both are inside the network. The network could allow certain content to pass between the users. But if one moves outside the network, then the network could stop some content from moving between them. Another example of enforcement due to anomalistic behavior could be a user logging in from within his/her New York network while another login request comes in from the same user located in Shanghai, China; the network needs to make a decision about which one of these users is authentic, and what action to take upon both users.

## Networking Is Much More than a Connectivity Service

Enforcement is performed in both security appliances and network infrastructure. This elevates the network beyond a connectivity service to a secure IT service where it provides visibility, context and control, thanks to SecureX. When a network utilizes 802.1X for access control, the network is not only providing connecting, but also enforcement, for example. A SecureX network is creating and analyzing policy tags, performing enforcement of policy, dynamically identifying new devices, monitoring traffic, communicating with policy server(s) and making decisions about which access rules to apply to a device.

## Protecting Mobile Users

The key architectural approach to SecureX is that the mobile device is equipped with a thin client, that being AnyConnect with the heavy processing burden of threat intelligence, mitigation and enforcement left in the Cloud or at the corporate head-end. Cisco's AnyConnect plays an important role in SecureX to protect mobile devices as it leverages a huge resource of threat intelligence. SIO collects and analyzes traffic of approximately 5 billion emails per day, 3 billion Web requests per day and 700,000 network sensors or IPS; expand that to include approximately 100 million endpoint devices that are equipped with an AnyConnect client, and SecureX provides the most comprehensive real-time threat intelligence telemetry and mitigation to endpoints.

All of these numbers can be boiled down through a few examples. Consider a user—with a laptop equipped with an AnyConnect client—is attempting to log into her/his corporate network. At the point of login, the network will identify the user, her/his role and which resource she/he is attempting to access. For example, Bill from finance is requesting access to the payroll server. Policy may be defined as Bill can only have access while he's inside the network perimeter, but not outside. Further, if Bill's inside the network perimeter, policy may dedicate that access to financial servers are encrypted via MACsec. No need for Bill to take any action, as a MACsec tunnel is established automatically as a matter of policy.

## Mobile Internet Browsing

Consider an AnyConnect iPhone mobile user browsing the Internet with Cisco's ScanSafe dynamically managing the Web interaction. With the endpoint's VPN connection terminated on an ASA firewall, behavior is monitored. If anomalistic behavior occurs, such as malware activity traversing terminated VPN connections, ASA, in conjunction with ScanSafe and SIO, can extract that information and analyze it. In the event that a virus is propagating on iPhone-based smartphones, SecOps can be notified with a message such as "This is a warning. There's something big happening on iPhone smartphones, and it's happening in this part of the world. SIO is analyzing this information, will create and distribute a signature fix shortly." This type of message can be pushed to all AnyConnect VPN terminating devices: "There's an iPhone virus coming on. SecOps is blocking it for the moment, and in the next few minutes, we'll distribute a signature to destroy this virus."

## A SecureX Ecosystem Is in the Works

There are two innovation inject points into SecureX to enable an ecosystem for management and SIEM. The management API offers an approach to a wider and consistent management view of network and security resources. SecOps often requested a super management platform where visibility and control is available from one tool. Unfortunately there is just too much information to display in one management window. But if multiple management tools/windows consulted the same policy data and shared this information, then a more consistent view of network assets can be obtained. An API to enable this type of information sharing would enable NetOps to manage its switched environment and be able to control not only switches, but also gain visibility in a security context of what policies have been applied to that switch. This concept can be extended to all network element management where they share policy information.

While not detailed in Cisco's SecureX architecture, Cisco did announce a new SIEM ecosystem last month as it placed CS-MARS in end-of-life. This SIEM ecosystem will contribute to the contextual element of SecureX. For example, there are a number of ecosystem partners in place providing sophisticated types of analysis as they deepen their interaction with Cisco's network infrastructure products. These partners collect and gather real-time alarm information and are correlative to global SIO. The combination of Cisco's SecureX and its SIEM ecosystem will be able to span threat intelligence from local machines to the global footprint of SIO, offering an expanse of security information that can be put to work to protect assets and mitigate threats once detected. These real-time local and global threat intelligence assets can also be interfaced with a policy engine to not only identify and control devices requesting network access, but to monitor behavior within and outside a corporate network.

The value benefit to a SIEM ecosystem and SIO feeding real-time global information to a policy server is best described through example. Should a device suddenly begin behaving anomalistically, the network can automatically identify the device and its closest switch, and take action, such as lock the device and redirect it to a remediation server. That is, SecureX will be able to perform infection containment and control, thanks to adding real-time local intelligence to the policy sever, thereby changing policy on the fly based upon contextual information.

SecureX is Cisco's latest attempt at integrating security deep into the network infrastructure as this infrastructure expands to mobile devices, cloud service providers and virtualized infrastructure. Its core component is context aware policy that is centrally administrated with enforcement highly distributed. SecureX is a modern security architecture for a new age of mobile and cloud computing.

## About Nick Lippis

Nicholas J. Lippis III is a world-renowned authority on advanced IP networks, communications and their benefits to business objectives. He is the publisher of the Lippis Report, a resource for network and IT business decision makers to which over 35,000 executive IT business leaders subscribe. Its Lippis Report podcasts have been downloaded over 160,000 times; i-Tunes reports that listeners also download the Wall Street Journal's Money Matters, Business Week's Climbing the Ladder, The Economist and The Harvard Business Review's IdeaCast. Mr. Lippis is currently working with clients to design their private and public virtualized data center cloud computing network architectures to reap maximum business value and outcome.

He has advised numerous Global 2000 firms on network architecture, design, implementation, vendor selection and budgeting, with clients including Barclays Bank, Eastman Kodak Company, Federal Deposit Insurance Corporation (FDIC), Hughes Aerospace, Liberty Mutual, Schering-Plough, Camp Dresser McKee, the state of Alaska, Microsoft, Kaiser Permanente, Sprint, Worldcom, Cigitel, Cisco Systems, Hewlett Packet, IBM, Avaya and many others. He works exclusively with CIOs and their direct reports. Mr. Lippis possesses a unique perspective of market forces and trends occurring within the computer networking industry derived from his experience with both supply and demand side clients.

Mr. Lippis received the prestigious Boston University College of Engineering Alumni award for advancing the profession. He has been named one of the top 40 most powerful and influential people in the networking industry by Network World. TechTarget an industry on-line publication has named him a network design guru while Network Computing Magazine has called him a star IT guru.

Mr. Lippis founded Strategic Networks Consulting, Inc., a well-respected and influential computer networking industry-consulting concern, which was purchased by Softbank/Ziff-Davis in 1996. He is a frequent keynote speaker at industry events and is widely quoted in the business and industry press. He serves on the Dean of Boston University's College of Engineering Board of Advisors as well as many start-up venture firm's advisory boards. He delivered the commencement speech to Boston University College of Engineering graduates in 2007. Mr. Lippis received his Bachelor of Science in Electrical Engineering and his Master of Science in Systems Engineering from Boston University. His Masters' thesis work included selected technical courses and advisors from Massachusetts Institute of Technology on optical communications and computing.