Miercom

The leading edge in networking information

Business Decision Series

Cisco Catalyst 3650
Test Results and Business Outcomes

CISCO

February 2015

Miercom
www.miercom.com

Making Business Dollars … and Sense

It's the difference between raw data, and information. The ***Miercom Business Decision Series*** combines the results of our hands-on testing, with insight on how particular features can positively impact the business bottom line. This report details some of the clear business advantages that the Cisco Catalyst 3650 Series delivers.

The Cisco Catalyst 3650 is an enterprise access switch – ideal for branch-office deployments. Models in this versatile switch series deliver a spectrum of capabilities:

- Up to 48 switch ports (10/100/1000BaseT); up to four integral 10GE uplinks.
- Power-over-Ethernet (PoE) and PoE+ support.
- Integral wireless support and wireless controller.
- License feature sets for L2 and full L3 – IPv4, IPv6.
- Stacking of multiple switches, which then act as a single logical switch.
- Plus a gamut of management, security and ease-of-use features.

Miercom engineers validated these features and then collaborated with Cisco in ascertaining how they yield tangible business benefits to users. These benefits – business outcomes, if you will – are detailed in this report, grouped into three areas:

1. **Securing your business**. Cisco includes with each switch: integral Wireshark packet-capture and analysis, Flexible NetFlow, and optionally, Lancope's StealthWatch. It is a powerful combination for detecting security threats and protecting your business.

2. **Simplicity**. Cisco has well-integrated wired and wireless access, our engineers found. Defining policies – such as for QoS or security – is done once for both wired and wireless environments, and users can readily access and switch between the two.

3. **Enhancing business continuity**. The high availability features that Cisco has built into the Catalyst 3650 Series – redundant power supplies, and active/standby switch control significantly enhance business continuity.

In this report we've detailed some of the more apparent business benefits that the Cisco Catalyst 3650 delivers, but by no means all. We think this approach offers an interesting and worthwhile perspective, answering the question: When you buy a new, leading-edge network system like the Cisco Catalyst 3650, what does it buy ***you***?

Robert Smithers
CEO
Miercom

Securing your Business
Are your being scanned?

Why this matters?

Hackers invariably first run scans – scanning programs, which systematically probe every host in your network – to find openings and vulnerabilities for subsequent attacks.

Even if the hacker plans a "zero-day" attack – that is, a new attack with no known 'footprint' or 'signature' – the traffic pattern of a scan is identifiable.

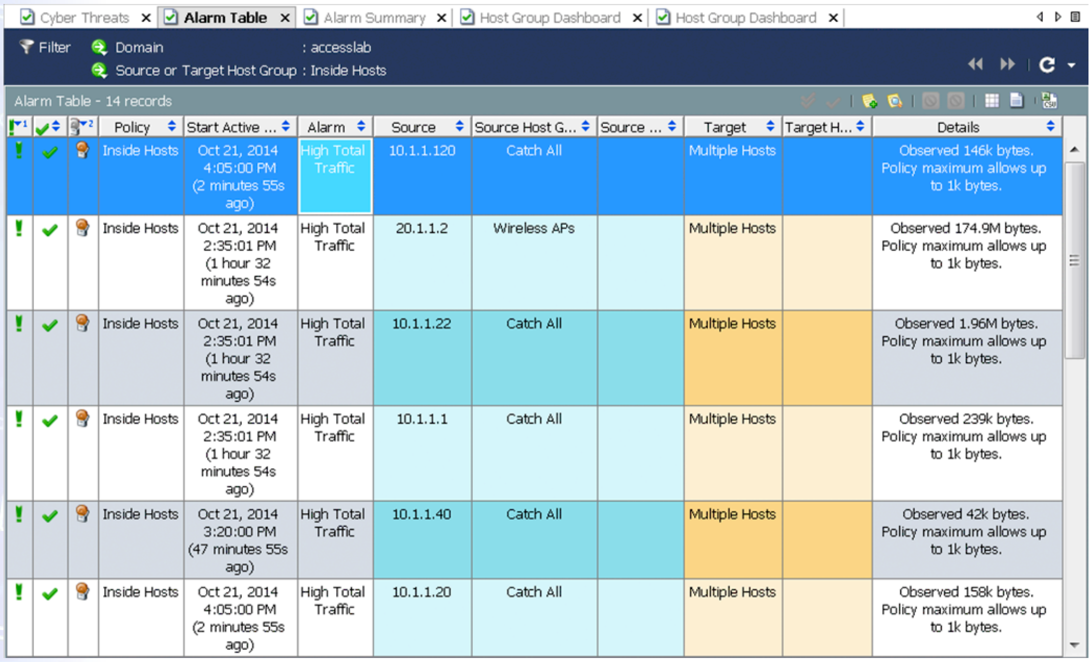
Business Outcome

Improved security for better protection of sensitive business data from theft.

With tools available to the Catalyst 3650 user, notably **Cisco Flexible NetFlow** and **StealthWatch** – a program from Lancope – possibly malicious intrusion patterns can be identified, and a warning issued.

Staying Alert

The alarm table of the StealthWatch management console is shown. The data pattern of possible hacker scans is identified in minutes and shown as an orange alert, changing to red if it repeats. The source IP address is shown, along with details of the suspected attack.



Domain : accesslab
Source or Target Host Group : Inside Hosts

Alarm Table - 14 records

	✓		Policy	Start Active ...	Alarm	Source	Source Host G...	Source ...	Target	Target H...	Details
!	✓	●	Inside Hosts	Oct 21, 2014 4:05:00 PM (2 minutes 55s ago)	High Total Traffic	10.1.1.120	Catch All		Multiple Hosts		Observed 146k bytes. Policy maximum allows up to 1k bytes.
!	✓	●	Inside Hosts	Oct 21, 2014 2:35:01 PM (1 hour 32 minutes 54s ago)	High Total Traffic	20.1.1.2	Wireless APs		Multiple Hosts		Observed 174.9M bytes. Policy maximum allows up to 1k bytes.
!	✓	●	Inside Hosts	Oct 21, 2014 2:35:01 PM (1 hour 32 minutes 54s ago)	High Total Traffic	10.1.1.22	Catch All		Multiple Hosts		Observed 1.96M bytes. Policy maximum allows up to 1k bytes.
!	✓	●	Inside Hosts	Oct 21, 2014 2:35:01 PM (1 hour 32 minutes 54s ago)	High Total Traffic	10.1.1.1	Catch All		Multiple Hosts		Observed 239k bytes. Policy maximum allows up to 1k bytes.
!	✓	●	Inside Hosts	Oct 21, 2014 3:20:00 PM (47 minutes 55s ago)	High Total Traffic	10.1.1.40	Catch All		Multiple Hosts		Observed 42k bytes. Policy maximum allows up to 1k bytes.
!	✓	●	Inside Hosts	Oct 21, 2014 4:05:00 PM (2 minutes 55s ago)	High Total Traffic	10.1.1.20	Catch All		Multiple Hosts		Observed 158k bytes. Policy maximum allows up to 1k bytes.

Source: Miercom, February 2015

'Problem' flows were defined to **Flexible NetFlow**, which runs on and can monitor all traffic through the switch. NetFlow captures statistics of such flows and forwards them to StealthWatch which is running on a VM server. StealthWatch looks for 'scanning' activity – in this case a lot of traffic from one IP source address to many others, aimed at a range of IP addresses and, on spotting one, generates an alarm.

On a Linux host, the engineers launched "nmap," a scanning program, which proceeded to scan all active hosts within the user's subnet, simulating an "eavesdrop" of the network.

The testers monitored the Lancope StealthWatch console. In a few minutes, the console showed a "cyber-attack" alarm, initially in orange and then turning red. Besides clearly showing the source of the scanning traffic, StealthWatch also issued email and text alerts.

Securing your Business

Can you protect against Denial-of-Service attack?

Why this matters?

A Denial-of-Service, or DoS, attack is one of the most common hacker attacks, and among the most disruptive. The attacker launches an overload of traffic that can overwhelm, isolate or even crash a target host or network device.

Identifying the source and type of attack are key to remediating the attack.

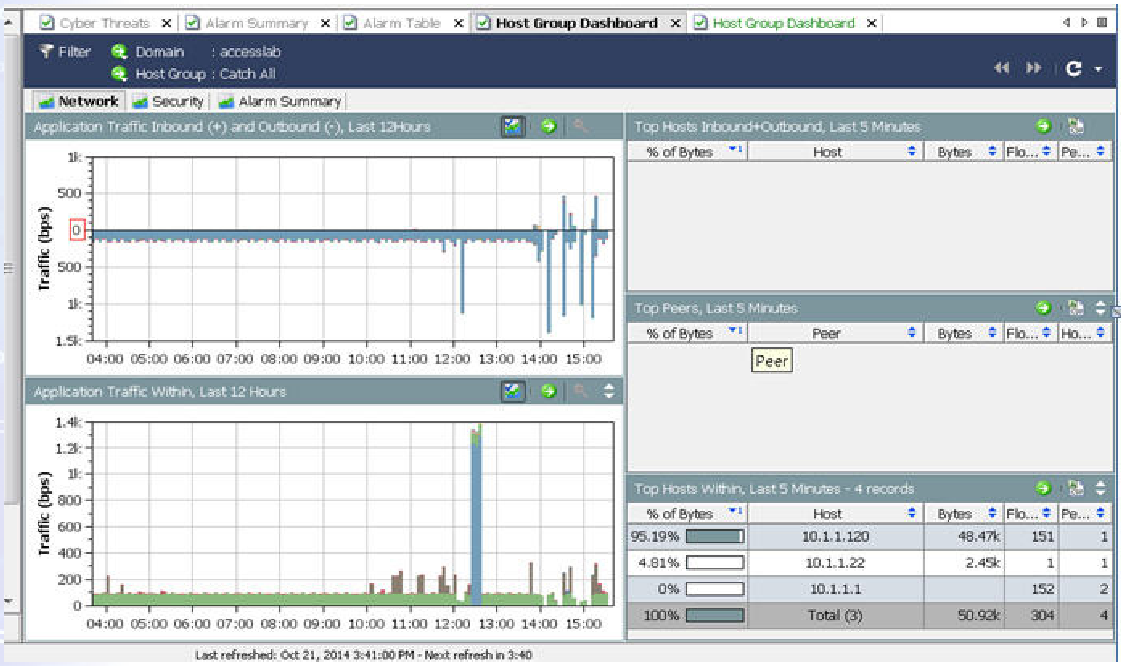
Business Outcome

Improved protection of IT resources and business data from disruptive attack.

Tools available to Catalyst 3650 users – including **Cisco Flexible NetFlow**, **Wireshark** and **StealthWatch** –readily identify a likely DoS attack and the source. The user can drill down and confirm the nature of the attack, and then apply corrective action.

Who's Attacking?

Using data provided by Cisco Flexible NetFlow, this StealthWatch graph shows a spike, where 95 percent of all inbound traffic is coming from the same source – the footprint of a possible DoS attack. The source is identified and, with Wireshark, packets are decoded and the attack is verified.



Domain : accesslab
Host Group : Catch All

Application Traffic Inbound (+) and Outbound (-), Last 12Hours

Application Traffic Within, Last 12 Hours

Top Hosts Inbound+Outbound, Last 5 Minutes

% of Bytes	Host	Bytes	Flo...	Pe...

Top Peers, Last 5 Minutes

% of Bytes	Peer	Bytes	Flo...	Ho...

Top Hosts Within, Last 5 Minutes - 4 records

% of Bytes	Host	Bytes	Flo...	Pe...
95.19%	10.1.1.120	48.47k	151	1
4.81%	10.1.1.22	2.45k	1	1
0%	10.1.1.1		152	2
100%	Total (3)	50.92k	304	4

Last refreshed: Oct 21, 2014 3:41:00 PM - Next refresh in 3:40

Source: Miercom, February 2015

We used **Flexible NetFlow on Catalyst 3650**, which enables monitoring all traffic through the switch, to define problem flows – in this case an overwhelming amount of data from a single source. NetFlow captures such flows and forwards them to StealthWatch. **StealthWatch** looks for patterns where a large percentage of inbound traffic comes from one source and, spotting one, generates an alarm.

On a Linux host out on the simulated Internet, the testers launched an"hping2" SYN flood, simulating a DoS attack. The Flexible NetFlow was set to look for and capture flows where a disproportionate amount of inbound traffic came from a single source, and forward them to StealthWatch for analysis.

The testers monitored the StealthWatch alarm table and traffic watch display. In a few minutes, the console showed a "cyberattack" alarm. Besides clearly showing the source of the DoS-attack traffic, StealthWatch also issued email and text alerts.

Securing your Business

Can you identify malicious traffic?

Why this matters?

The 'baseline' traffic on a network is fairly consistent and predictable under 'normal' conditions-in terms of the number of communicating nodes, the applications, the protocols and traffic levels.

Being alerted when unusual traffic volumes or patterns occur is a crucial first step in detecting and averting a possible attack.

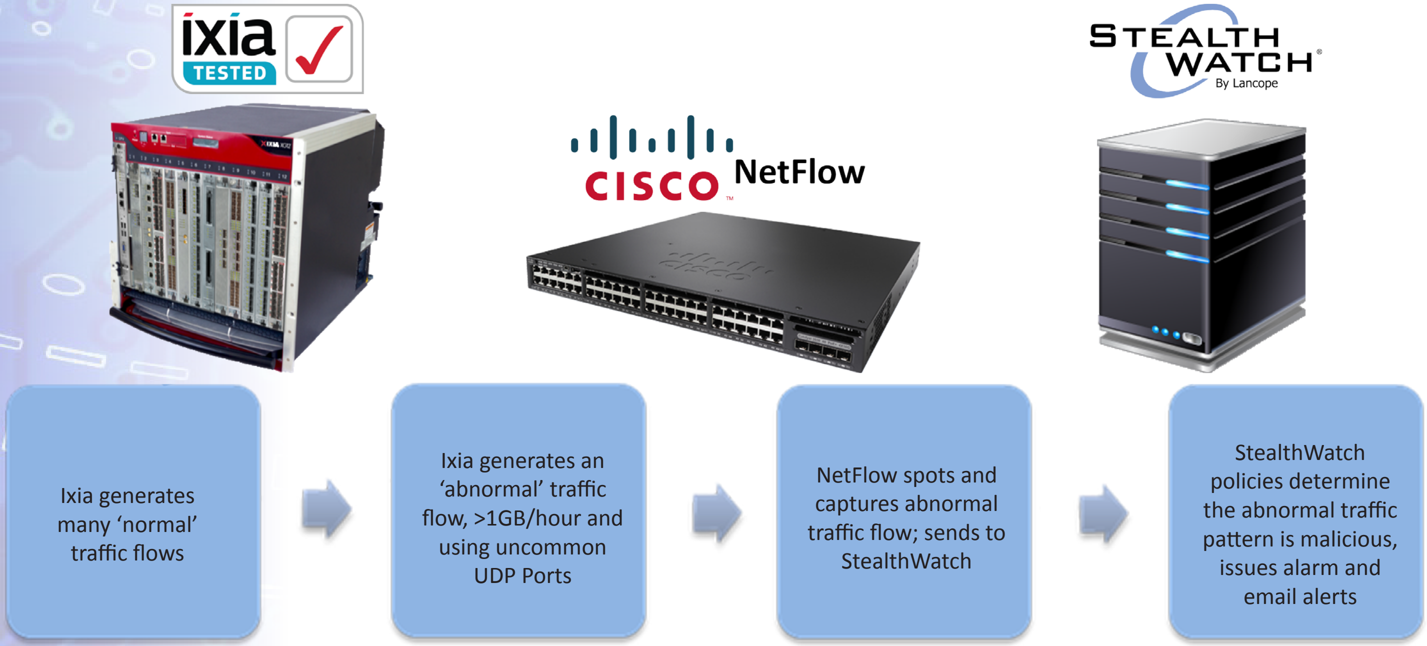
Business Outcome

Improved protection of business data by detecting and analyzing unusual and suspicious network activity.

Cisco Flexible NetFlow an integral capability within the Cisco Catalyst 3650 can be enabled to collect the statistics of the traffic that is abnormal and forward it to **StealthWatch** for further analysis and, if appropriate, alarm response.

Abnormal is suspect

In this test case, Cisco Flexible NetFlow was set to look for and capture abnormal traffic flows, defined in this case as exceeding a traffic volume of 1 Gigabyte per hour and using unusual UDP ports. An abnormal flow is spotted on StealthWatch with the data that is being collected by Flexible NetFlow.



Ixia generates many 'normal' traffic flows

Ixia generates an 'abnormal' traffic flow, >1GB/hour and using uncommon UDP Ports

NetFlow spots and captures abnormal traffic flow; sends to StealthWatch

StealthWatch policies determine the abnormal traffic pattern is malicious, issues alarm and email alerts

Source: Miercom, February 2015

The Ixia test tool was configured to issue five "conventional" traffic flows, with traffic loads under 1GB per hour using common UDP ports such as for Web browsing and FTP file transfer. **Cisco Flexible NetFlow**, which can monitor all traffic through the switch, was set to look for high volume flows and traffic using uncommon and suspicious UDP ports.

Ixia then generated an "abnormal" flow, using uncommon UDP ports and generating traffic over 1GB/Hour. The data exported by NetFlow to StealthWatch helped determine the abnormal traffic pattern. StealthWatch analyzed the uncommon flow, determined it was suspicious, and generated an alarm. In addition to identifying the source of suspicious traffic, StealthWatch also issued email and text alerts as soon as the attack was detected.

Securing you Business

Is someone stealing your data?

Why this matters?

Some call it “Data Exfiltration” – the looting of a company’s data, whether it’s customer lists, secure credit-card records, or proprietary design or product files.

This can be perpetrated by a cable connected client but also, increasingly, via wireless access. The ability to spot excessive download of data files, over wireless or wired connections, can help safeguard data.

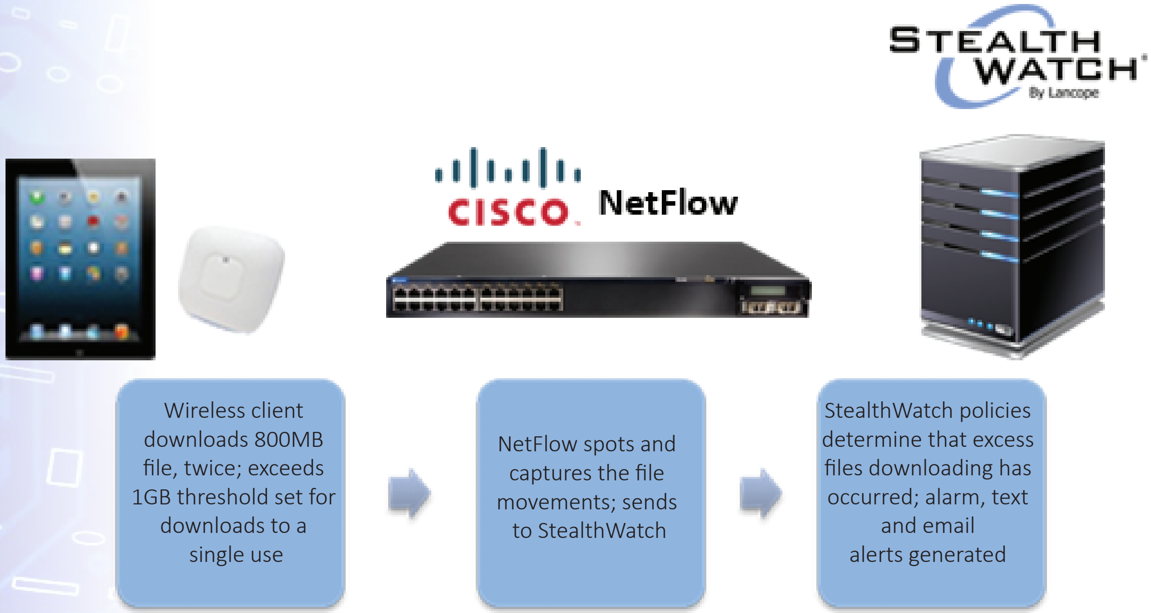
Business Outcome

Improved protection of business data by spotting large data downloads over the network, including via wireless.

Cisco Flexible NetFlow, an integral capability within the Cisco Catalyst 3650, can be enabled to collect the statistics of the traffic that is abnormal and forward it to **StealthWatch** for analysis, detection and, if appropriate, alarm response.

Proactively Monitor Traffic

Flexible NetFlow was set to look for and capture excessive file downloads, in this case exceeding 1 GB, to a single user. An iPad client downloads individual files under 1 GB, but the total exceeds the 1GB threshold. The traffic is captured and passed on to StealthWatch, which raises an alarm.



Wireless client downloads 800MB file, twice; exceeds 1GB threshold set for downloads to a single use

NetFlow spots and captures the file movements; sends to StealthWatch

StealthWatch policies determine that excess files downloading has occurred; alarm, text and email alerts generated

Source: Miercom, February 2015

Cisco Flexible NetFlow, which runs on and can monitor all traffic through the switch, was configured to look for sizable file downloads, capture any such flows and forward them to a VM server running **StealthWatch**.

An iPad client downloaded a large file (800 MB) from a data repository server. There was no response. Then the same iPad client downloaded another large file (again, 800 MB) from the server. Both file downloads were captured by Flexible NetFlow and forwarded to StealthWatch.

StealthWatch examined the flows, which exceeded the policy settings and thresholds – a single user had downloaded more than 1 GB of files – and raised an alarm. Besides showing the source of the downloads, StealthWatch also issued the alarm via email and text alerts.

Simplicity

Simplified troubleshooting through remote diagnosis

Why this matters?

Protocol analyzers, for packet capture and deep packet inspection, are key to diagnosing network problems. These devices often require on-premise use by network administrators.

The ability to remotely access this function means a problem or threat can be diagnosed faster, without having to travel to the remote site where the switch resides.

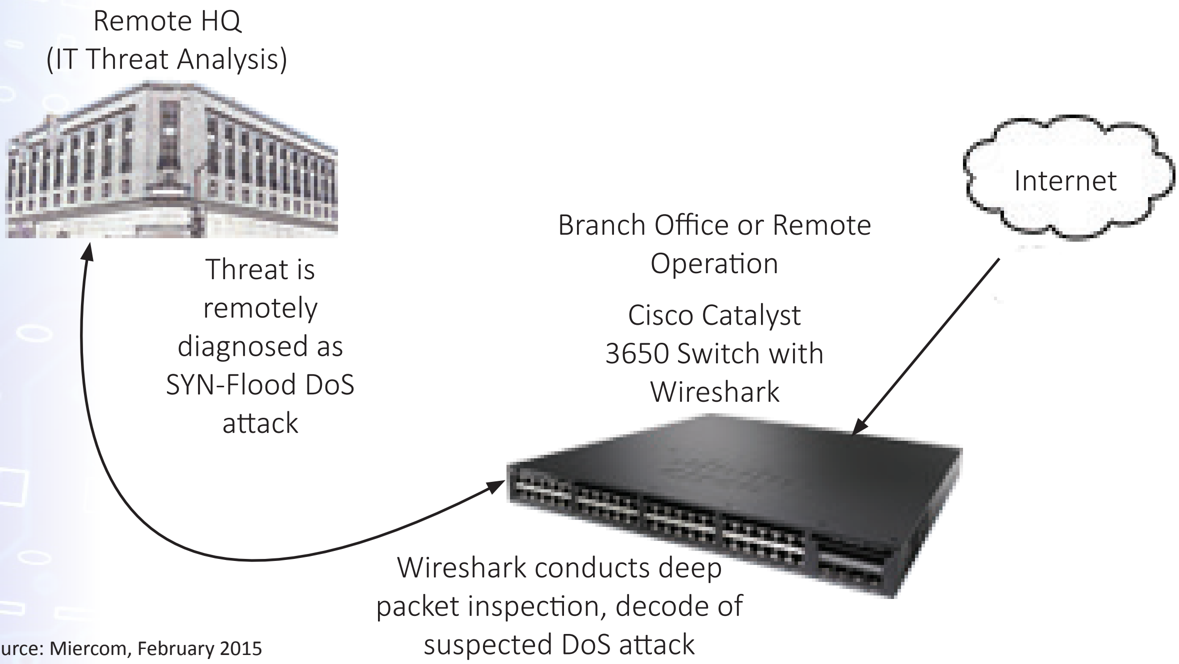
Business Outcome

Better response time at lower cost for troubleshooting network problems, including security threats.

Wireshark, a world-class protocol analyzer, is embedded in the Cisco Catalyst 3650. A network tech can remotely start a Wireshark monitoring session and collect packets, for fast, cost-effective troubleshooting.

Remote Diagnosis

The Wireshark embedded in the Cisco Catalyst 3650 enables deep packet inspection remotely over the network. In this test case, the Wireshark decodes captured packets from a SYN denial-of-service attack, allowing the remote technician to verify the attack and issue remediation commands.


Remote HQ
(IT Threat Analysis)
Internet
Branch Office or Remote Operation
Cisco Catalyst 3650 Switch with Wireshark
Threat is remotely diagnosed as SYN-Flood DoS attack
Wireshark conducts deep packet inspection, decode of suspected DoS attack

Source: Miercom, February 2015

From a Linux host, an “Hping2” SYN attack was launched against a server, which traversed the Cisco Catalyst 3650 switch. **Wireshark** was enabled on the switch and filters were set up to capture ten seconds of traffic.

The raw packets were captured and saved to local flash memory. The same packets could also have been exported to an external PC for further analysis.

The network diagnostician remotely troubleshoots and verifies by examining the packets’ payload that a SYN DoS attack is underway. The tech ascertains the source address, the target server, and the exact ports that the attack is targeting. Armed with this information remediation actions can be launched.

Simplicity

Consistent wired and wireless policy setting

Why this matters?

Setting security policies –who can access which services – and Quality-of-Service parameters, such as bandwidth restrictions, are complex enough on a wired network. Then add wireless to the mix.

The solution: a single, straightforward central point for defining security and QoS restrictions, which applies them consistently across wired and wireless networks.

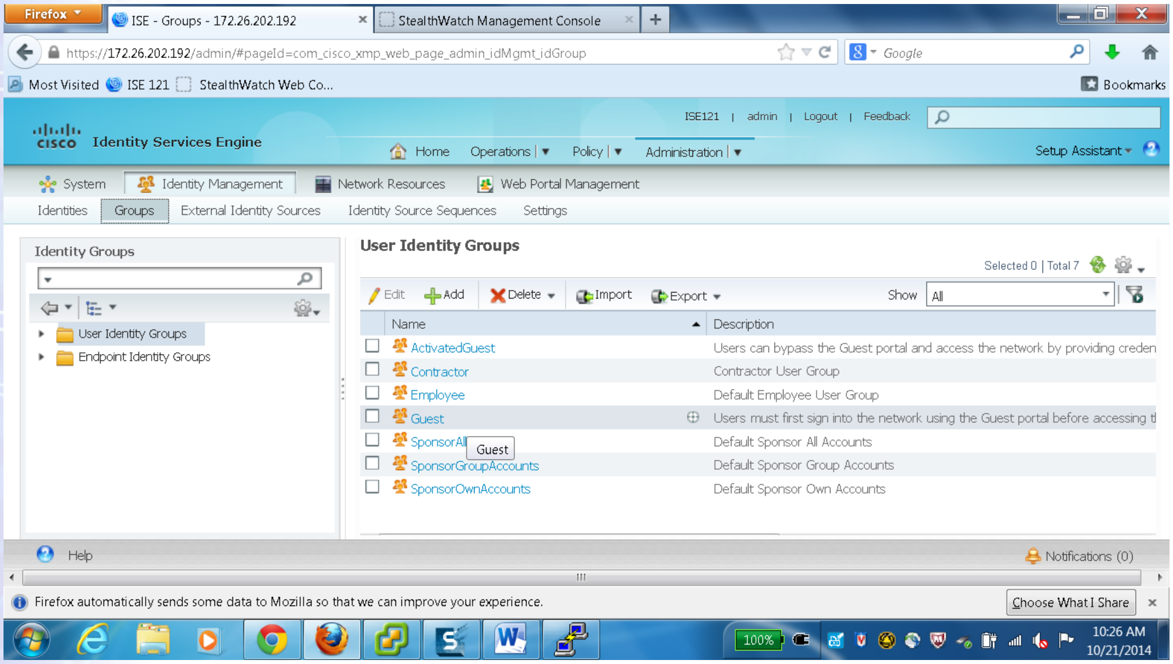
Business Outcome

Agility through simplicity; Cisco's Identity Services Engine (ISE) provides a central point for defining security and QoS policies, and enforcement across both wired and wireless networks.

The Catalyst 3650 with integrated wireless and ISE allow fast and easy application of bandwidth and access restrictions –for both wired and wireless network environments.

Centralized Policy Setting

The interface for defining groups for security and QoS restrictions is shown. In this test we applied different settings to an employee (employee group) and to a contractor (contractor group), and verified their proper and consistent application across wired and wireless networks.



User Identity Groups

	Name	Description
□	ActivatedGuest	Users can bypass the Guest portal and access the network by providing creden
□	Contractor	Contractor User Group
□	Employee	Default Employee User Group
□	Guest	Users must first sign into the network using the Guest portal before accessing t
□	SponsorAll	Default Sponsor All Accounts
□	SponsorGroupAccounts	Default Sponsor Group Accounts
□	SponsorOwnAccounts	Default Sponsor Own Accounts

Firefox automatically sends some data to Mozilla so that we can improve your experience.

Source: Miercom, February 2015

We defined two sample users, an employee and a contractor, via the Cisco Identity Services Engine (ISE). The employee was given access to all services and Websites, including FTP, with no bandwidth limitations. The contractor was denied access to websites but granted FTP upload ability, with a lower, constrained bandwidth (500 kbps). The process took just a few minutes. At the time of client login, the Catalyst 3650 downloads the policies from ISE and applies them to the user groups.

The policies for each user's connectivity and access were tested, via both wired laptops (MacBooks) and wireless iPads. In each case, and even switching between wired and wireless, the employee was able to accomplish each task with no restrictions and no bandwidth limits. We confirmed that the contractor could not access Websites. We also confirmed via the switch CLI the reduced bandwidth allotted for the contractor's FTP transfer, which took noticeably longer.

Simplicity

Simplify Apple Bonjour services across VLANS

Why this matters?

Mobility and seamless connectivity are being pursued in many enterprise organizations. Yet some features of networking, like VLANs, can frustrate connectivity as users and devices change locations.

A feature that keeps track of service and user associations can enable quick and dynamic re-connection as users move about.

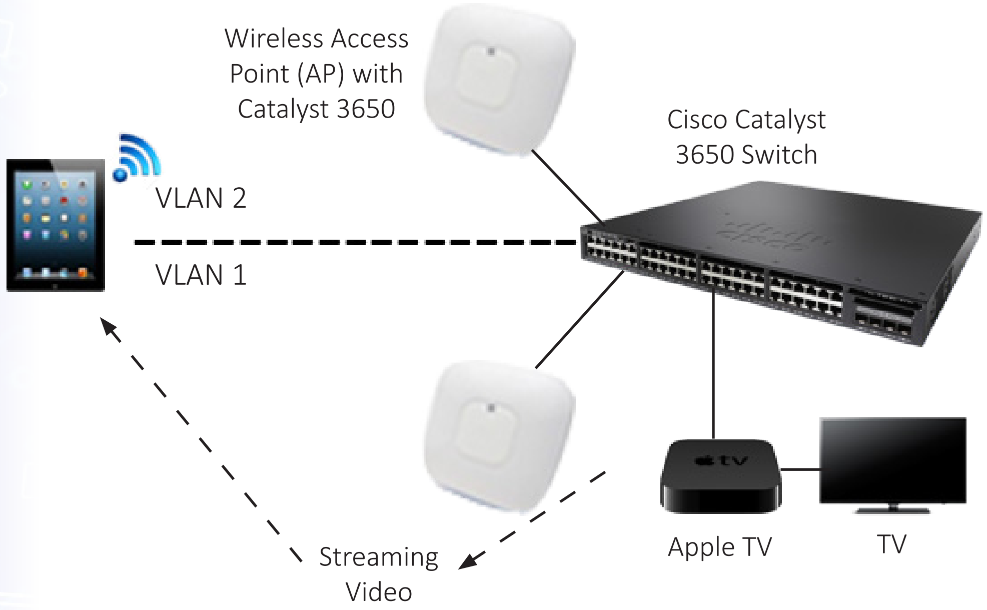
Business Outcome

Improved mobility and user experience through seamless access to applications and services.

The Service Discovery Gateway (SDG) feature of the Catalyst 3650 can reflect services from one VLAN to another. This facilitates BYOD (bring your own device) rollout, including 'zeroconf' (no configuration required) protocols, such as Apple Bonjour.

Connected Mobility

As mobile devices change locations and connect via a different VLAN, service connectivity is invariably lost. In this test case an iPad views streaming video from an Apple TV. When moved to a different VLAN the video connection is lost, unless the Service Discovery Gateway feature is enabled.


Wireless Access Point (AP) with Catalyst 3650
Cisco Catalyst 3650 Switch
VLAN 2
VLAN 1
Streaming Video
Apple TV
TV

Source: Miercom, February 2015

An Apple TV and an iPad are connected in the same VLAN. Both devices run "zeroconf" (no configuration required) service – called Bonjour for Apple devices – using mDNS and therefore are visible to each other. The iPad is then moved to and reconnected via a different VLAN.

Since zeroconf works only on the same local VLAN/IP subnet, the iPad loses its streaming video connection with the Apple TV. The Service Discovery Gateway (SDG) feature of the Catalyst 3650 reflects services from one VLAN to another. After enabling SDG, the same iPad moving between VLANs seamlessly retains the same streaming video connection.

Any zeroconf supporting device (i.e. printers, cameras, routers) can benefit from the SDG feature, which can enable enterprises to more readily deploy BYOD in their networks.

Enhancing Business Continuity

Fast and stateful failover in a stack

Why this matters?

Network components can fail. But well designed equipment and systems can mitigate a failure allowing communications and business operations to continue.

A network switch in a branch office plays a critical role, and products with configurations that support varying degrees of fault tolerance should be considered.

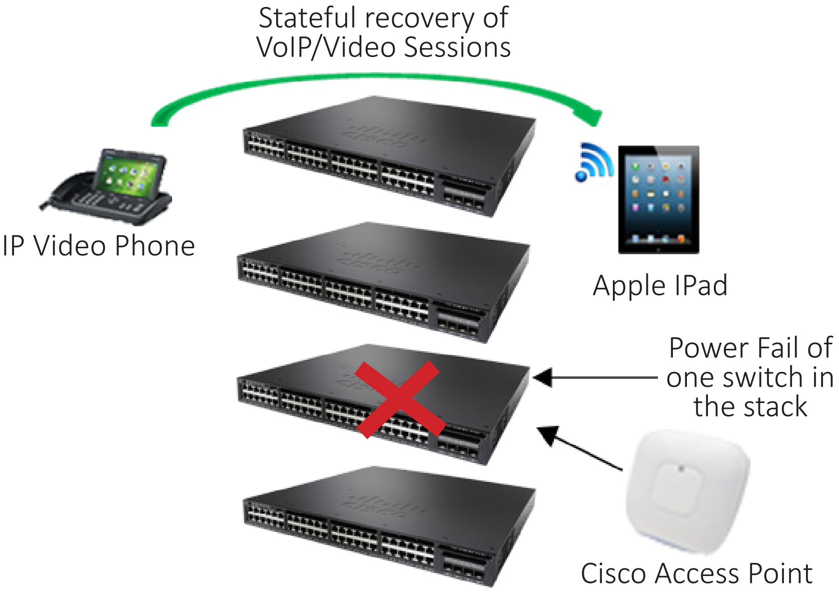
Business Outcome

Network and business continuity, even if a key IT infrastructure component fails. The ability of a multi-switch stack to survive a failure is built in.

Since business operations continue, replacing a failed switch can be done on a scheduled basis. A maintenance crew doesn't have to be dispatched immediately to a remote branch.

Stateful Switchover

A Catalyst 3650 stack will automatically configure for a stateful switchover if one switch in the stack should fail. In this test case, a Jabber call between an iPad and an IP video phone continues unaffected by the 200-millisecond failover. There is not even a noticeable glitch during the video session.


Stateful recovery of VoIP/Video Sessions
IP Video Phone
Apple IPad
Power Fail of one switch in the stack
Cisco Access Point

Source: Miercom, February 2015

Four Catalyst 3650 switches are configured in a stack. Each has full NSF/SSO (Non Stop Forwarding, Stateful Switch-Over) support. When the stack boots up, the active and standby switch roles are assigned automatically. What's more, the state of all connections is dynamically retained in both the active and standby switches.

A Jabber video call is then established between an IP videophone endpoint and an iPad. We then power-cycle the active switch to simulate a failure. The fail-over time is very brief, only about 200 milliseconds.

The result: The video call is sustained with no interruption and no glitch during the video session is observed.

About this Miercom Testing

This testing and report was sponsored by Cisco Systems. The data was verified completely and independently by Miercom's own lab-test engineers.

Miercom has published hundreds of network-product-comparison analyses in leading trade periodicals and other publications. Miercom's reputation as the leading, independent product test center is undisputed.

Private test services available from Miercom include competitive product analyses, as well as individual product evaluations. Miercom features comprehensive certification and test programs including: Certified Interoperable, Certified Reliable, Certified Secure and Certified Green. Products may also be evaluated under the Performance Verified program, the industry's most thorough and trusted assessment for product usability and performance.

Use of This Report

Every effort was made to ensure the accuracy of the data contained in this report but errors and/or oversights can occur. The information documented in this report may also rely on various test tools, the accuracy of which is beyond our control. Furthermore, the document relies on representations by vendors that were reasonably verified by Miercom but beyond our control to verify to 100 percent certainty.

This document is provided "as is," by Miercom and gives no warranty, representation or undertaking, whether express or implied, and accepts no legal responsibility, whether direct or indirect, for the accuracy, completeness, usefulness or suitability of any information contained in this report.

No part of any document may be reproduced, in whole or in part, without the specific written permission of Miercom or Cisco Systems. All trademarks used in the document are owned by their respective owners. You, the reader, agree not to use any trademark in or as the whole or part of your own document in connection with any activities, products or services which are not ours, or in a manner which may be confusing, misleading or deceptive or in a manner that disparages Miercom or our information, projects or developments.