



Cisco
Networkers 2011

May 19, Toronto, Canada

Knowledge
Is Power.
Learn. Share. Collaborate.



AnyConnect Secure Mobility

Presented by Tim Davidson



Cisco
Networkers 2011

May 19, Toronto, Canada

Knowledge
Is Power.
Learn. Share. Collaborate.



Agenda

- Solution Overview
- Deployment Scenarios
- Feature Highlights
- Q & A
- Wrap Up



Cisco
Networkers 2011

May 19, Toronto, Canada

Knowledge
Is Power.

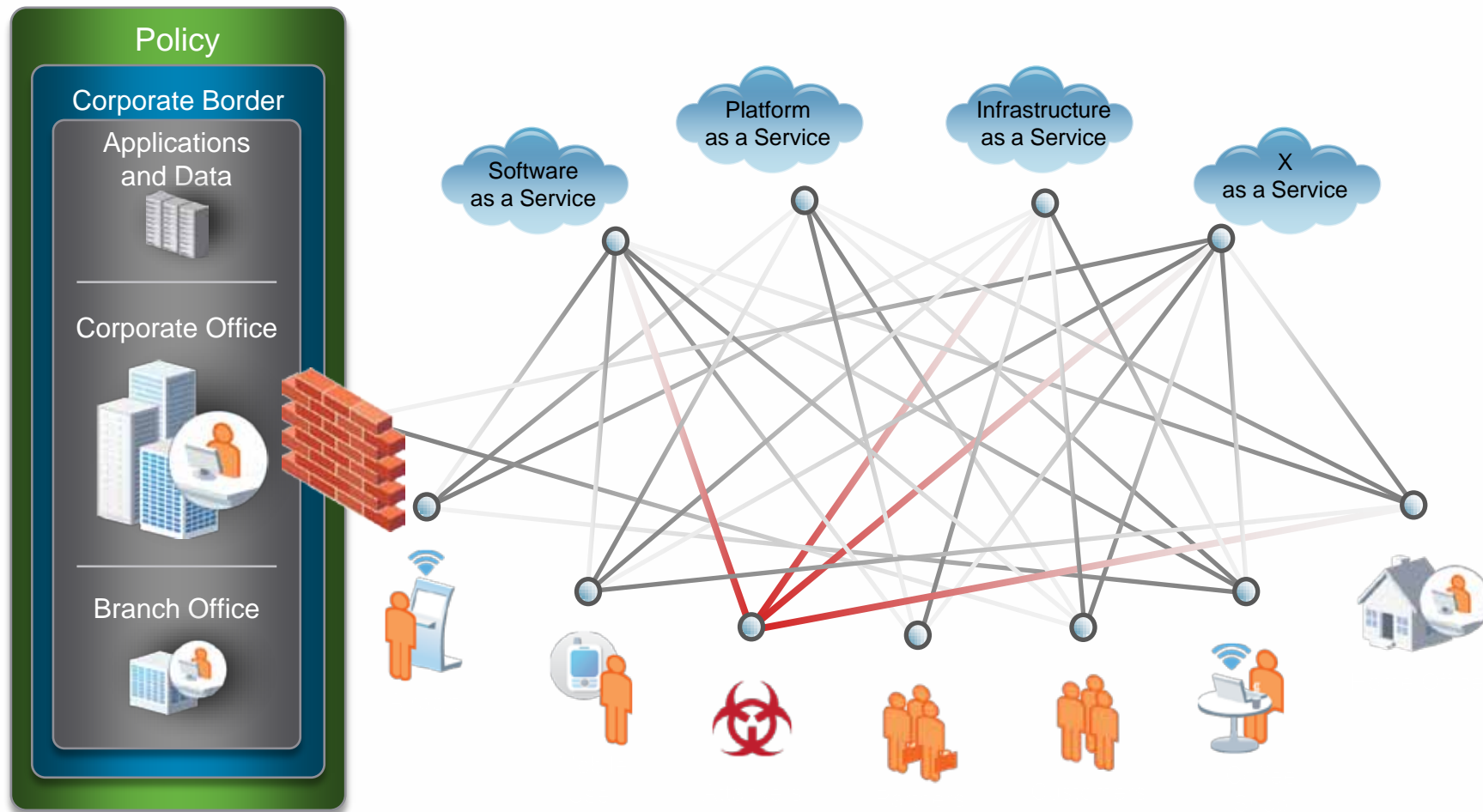
Learn. Share. Collaborate.



Solution Overview

Security in the Borderless World

Knowledge
Is Power.
Learn. Share. Collaborate.

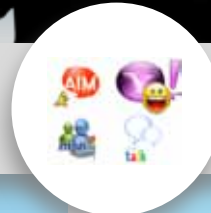


Personal Choice vs Corporate Policy

Knowledge
Is Power.
Learn. Share. Collaborate.



Personal



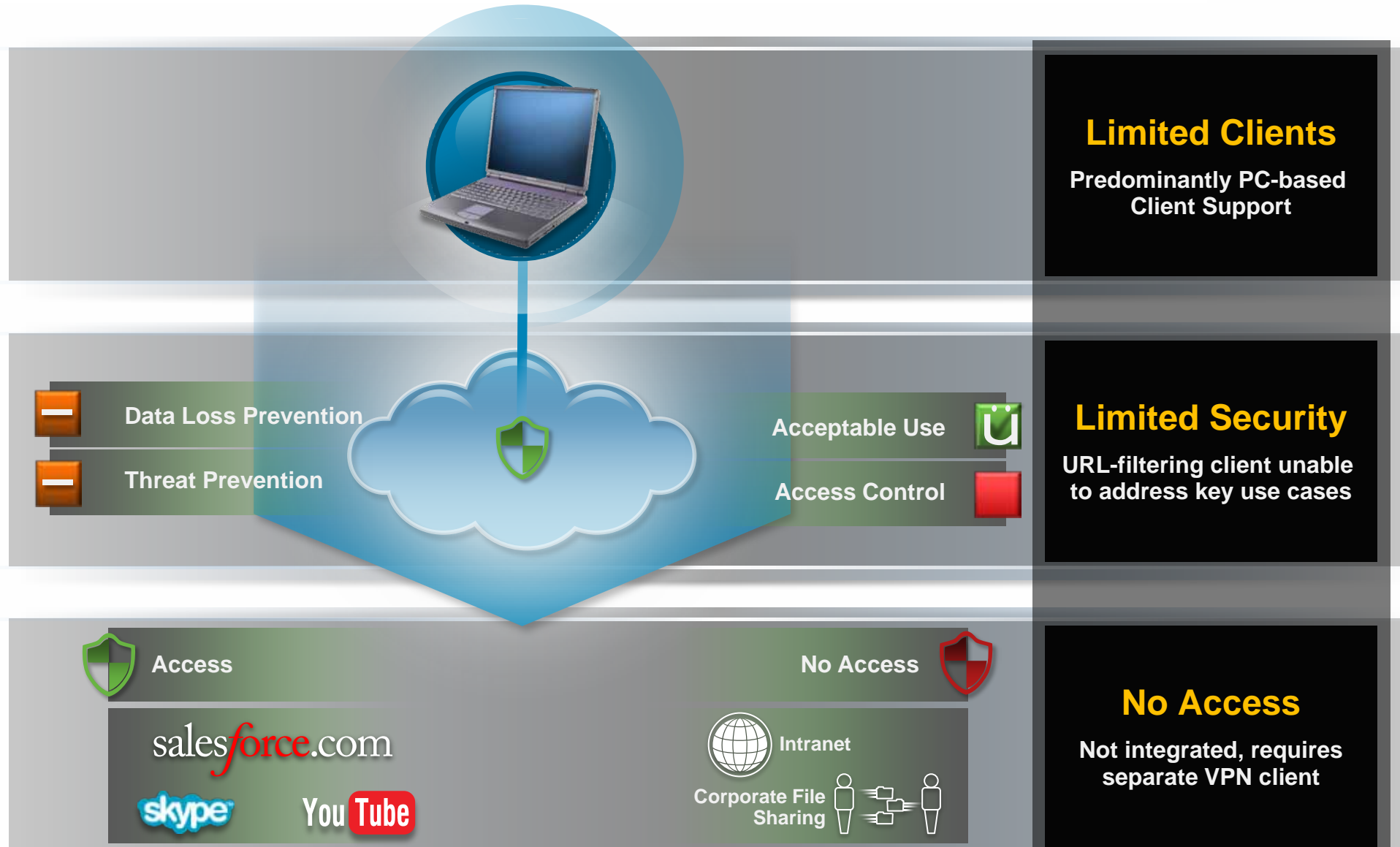
Business

Traditional Remote Access VPN



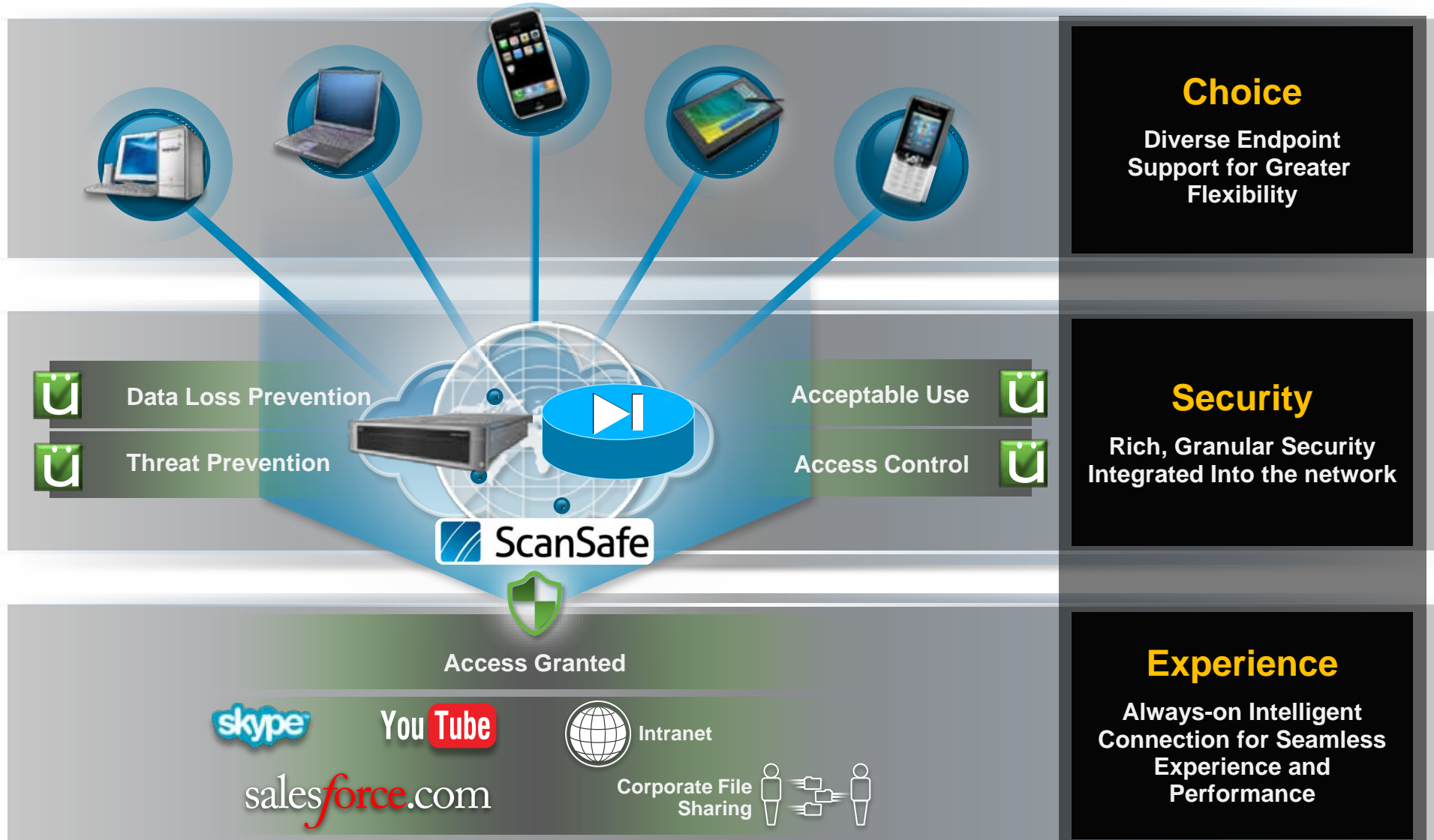
Traditional Mobile Web Security

Knowledge
Is Power.
Learn. Share. Collaborate.



Web Security with Next Generation Remote Access

Knowledge
Is Power.
Learn. Share. Collaborate.



AnyConnect Secure Mobility Client

Network and Security Follows User—It Just Works

Knowledge
Is Power.
Learn. Share. Collaborate.



Broad Mobile Support

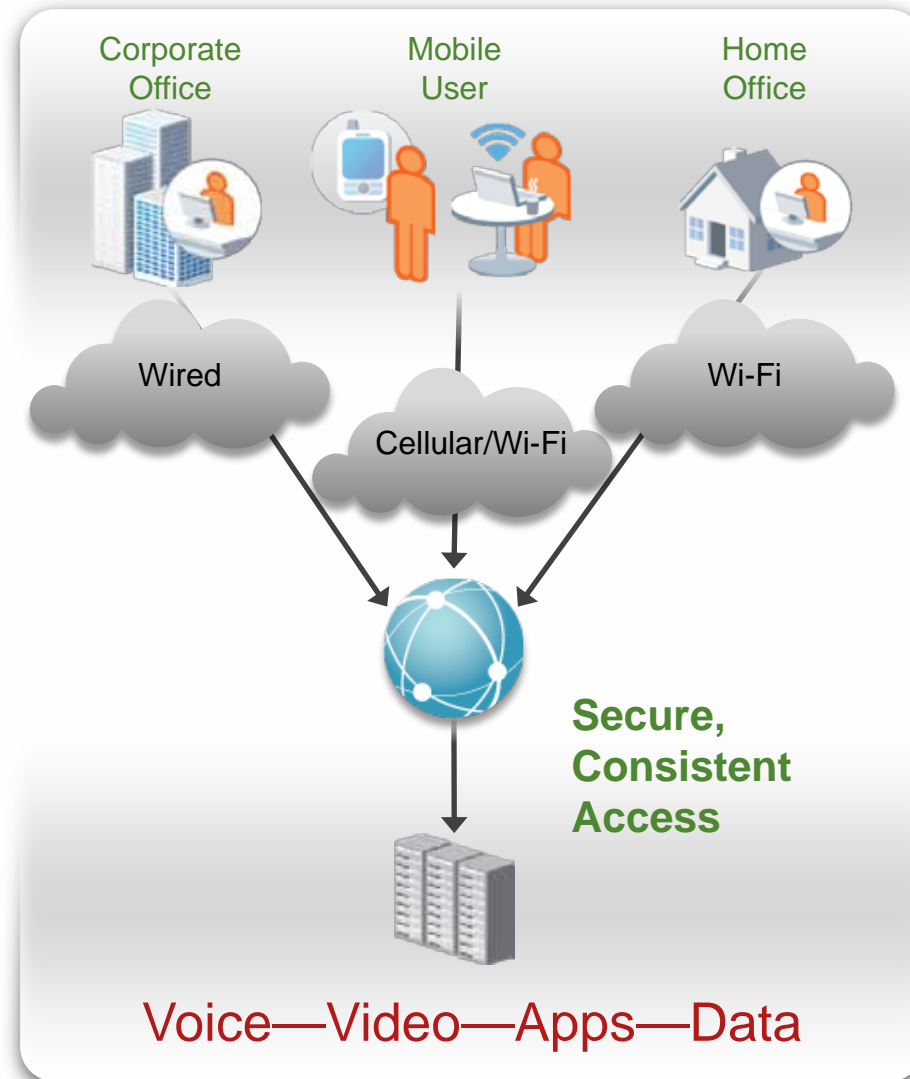
- § Fixed and semi-fixed platforms
- § Mobile platforms

Persistent Connectivity

- § Always-on connectivity
- § Optimal gateway selection
- § Automatic hotspot negotiation
- § Seamless connection hand-offs

Next-Gen Unified Security

- § User/device identity
- § Posture validation including Managed vs Un Managed Assets
- § Integrated web security for always-on security (hybrid)
- § Clientless and desktop virtualization



Enabling the New Borderless Organization

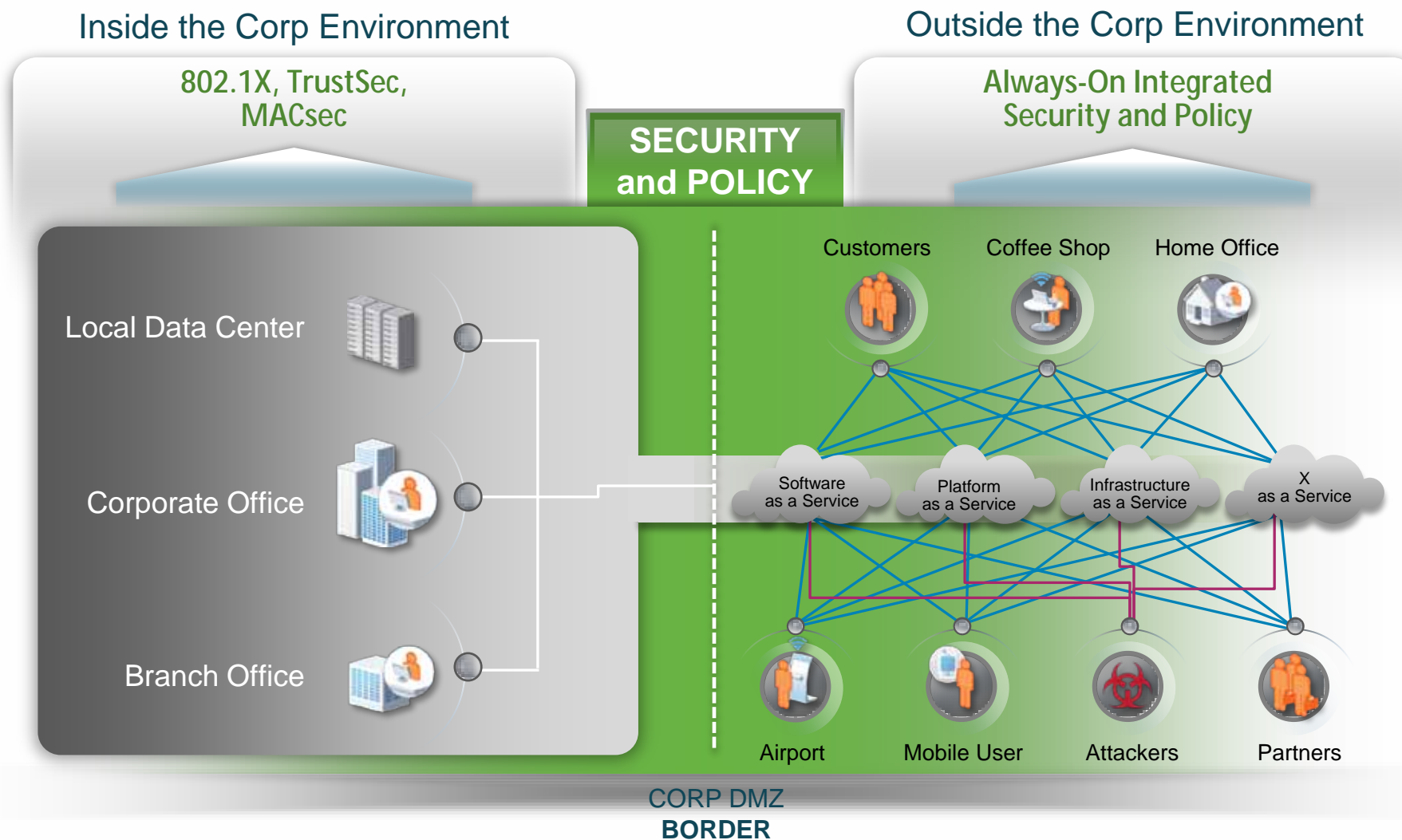
Knowledge
Is Power.
Learn. Share. Collaborate.



Securely, Reliably, Seamlessly

Secure Borderless Network Architecture Enabling Mobility, Extending Security

Knowledge
Is Power.
Learn. Share. Collaborate.





Cisco
Networkers 2011

May 19, Toronto, Canada

Knowledge
Is Power.

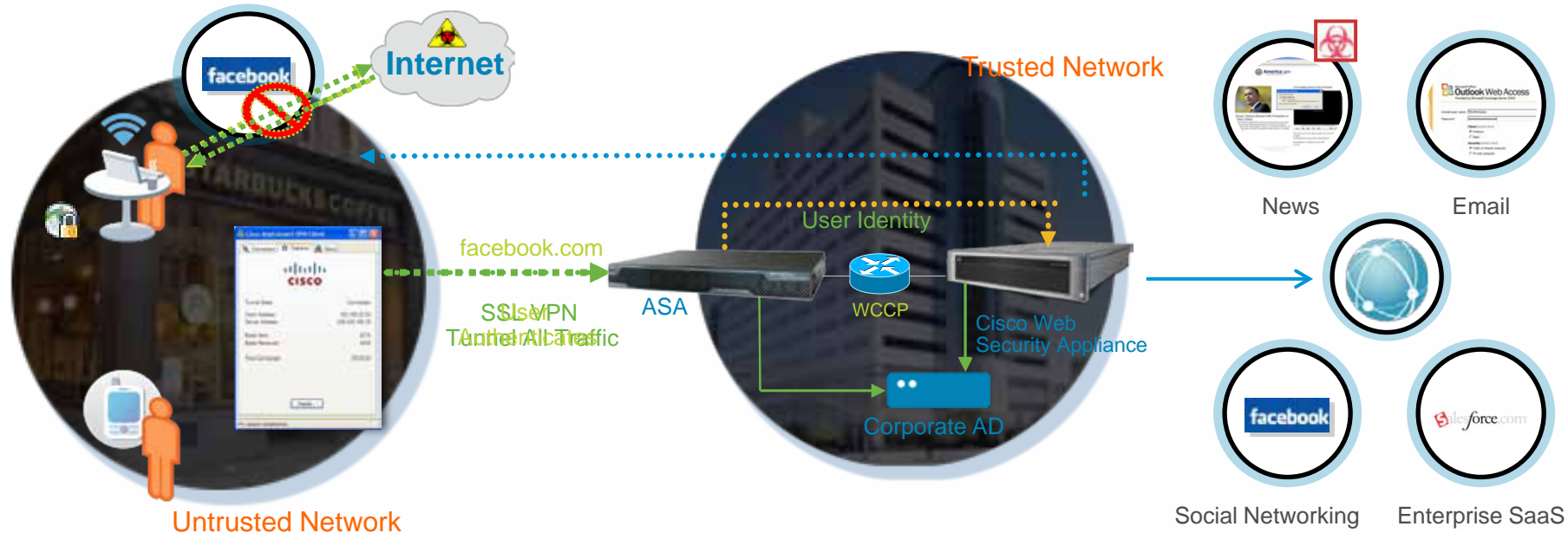
Learn. Share. Collaborate.



Deployment Scenarios

Cisco AnyConnect Secure Mobility with Web Security Appliance

Knowledge Is Power.
Learn. Share. Collaborate.



AnyConnect

- Always-on VPN (admin configurable)
- Optimal head end auto-detect
- Transparent auth (certificate)

ASA à WSA

- Authentication handoff (SSO)
- Identity and location aware policy enforcement
- Location-aware reporting

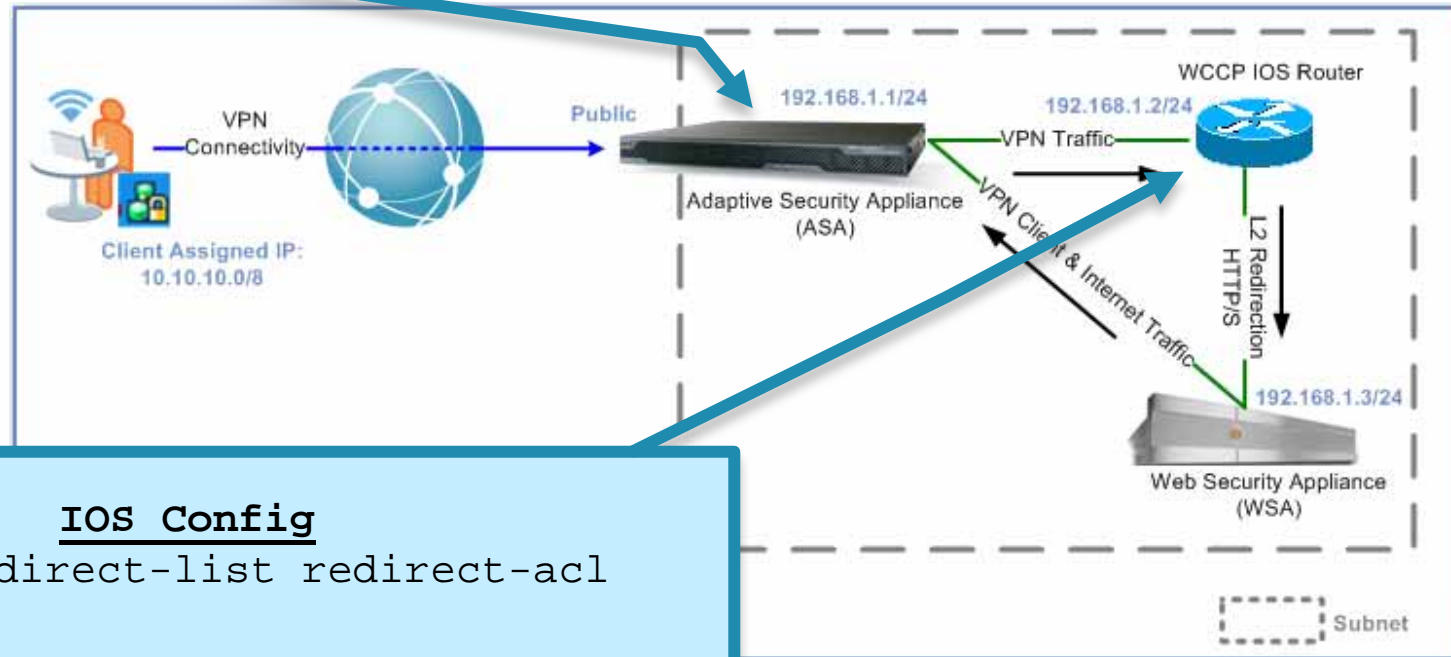
Transparent Redirection – Single ASA (WCCP on Router)

Knowledge
Is Power.
Learn. Share. Collaborate.



ASA Config

```
route inside 0.0.0.0 0.0.0.0 192.168.1.2 tunneled
route inside 10.10.10.0 255.0.0.0 192.168.1.2
```

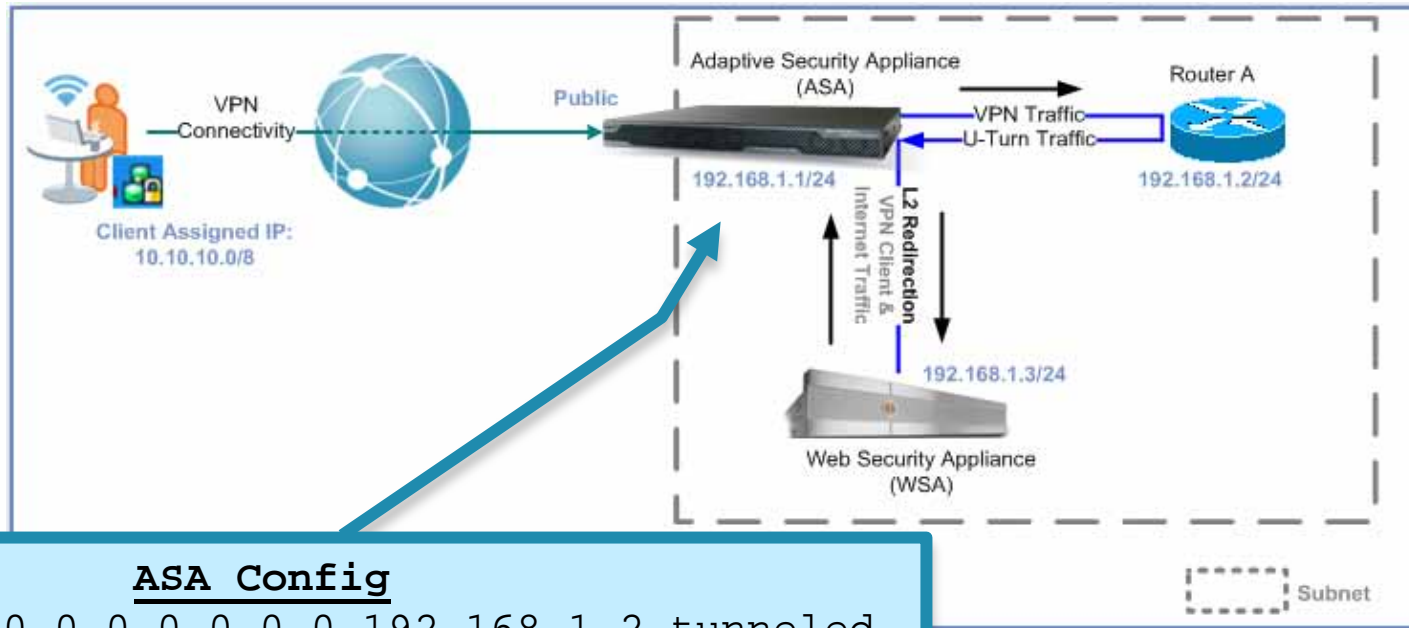


IOS Config

```
ip wccp 80 redirect-list redirect-acl
interface eth0
  ip wccp 80 redirect in
```

Transparent Redirection – Single ASA (WCCP on ASA)

Knowledge
Is Power.
Learn. Share. Collaborate.



ASA Config

```
route inside 0.0.0.0 0.0.0.0 192.168.1.2 tunneled  
route inside 10.10.10.0 255.0.0.0 192.168.1.2
```

```
wccp 80 redirect-list redirect-acl  
wccp interface inside 80 redirect in
```

Transparent Redirection (Alternate Egress)

Knowledge
Is Power.
Learn. Share. Collaborate.

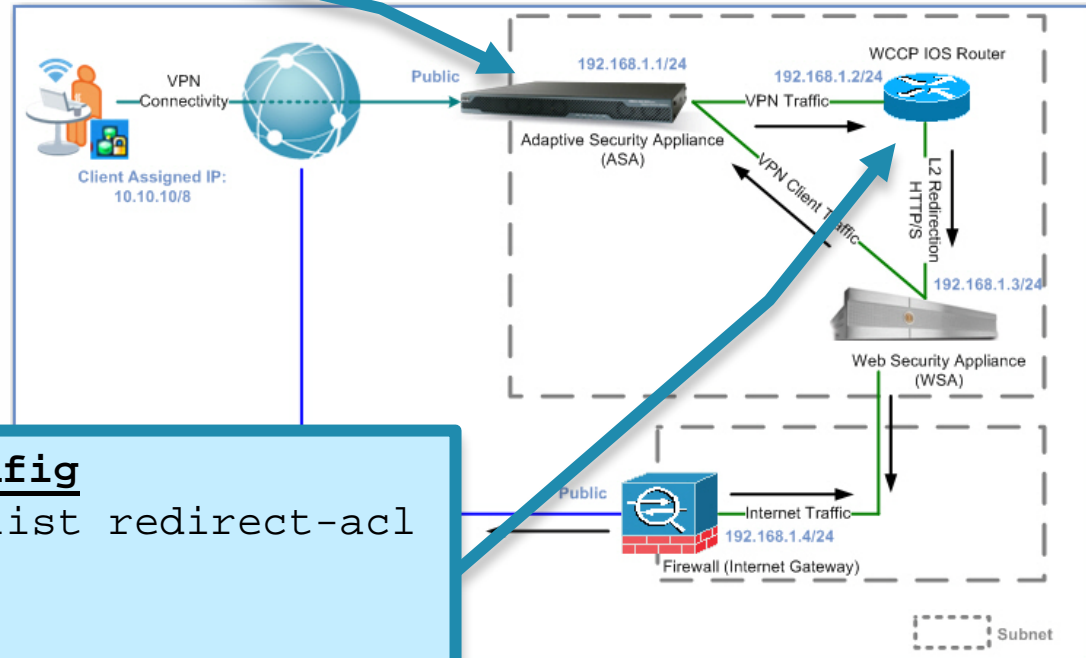


ASA-1 Config

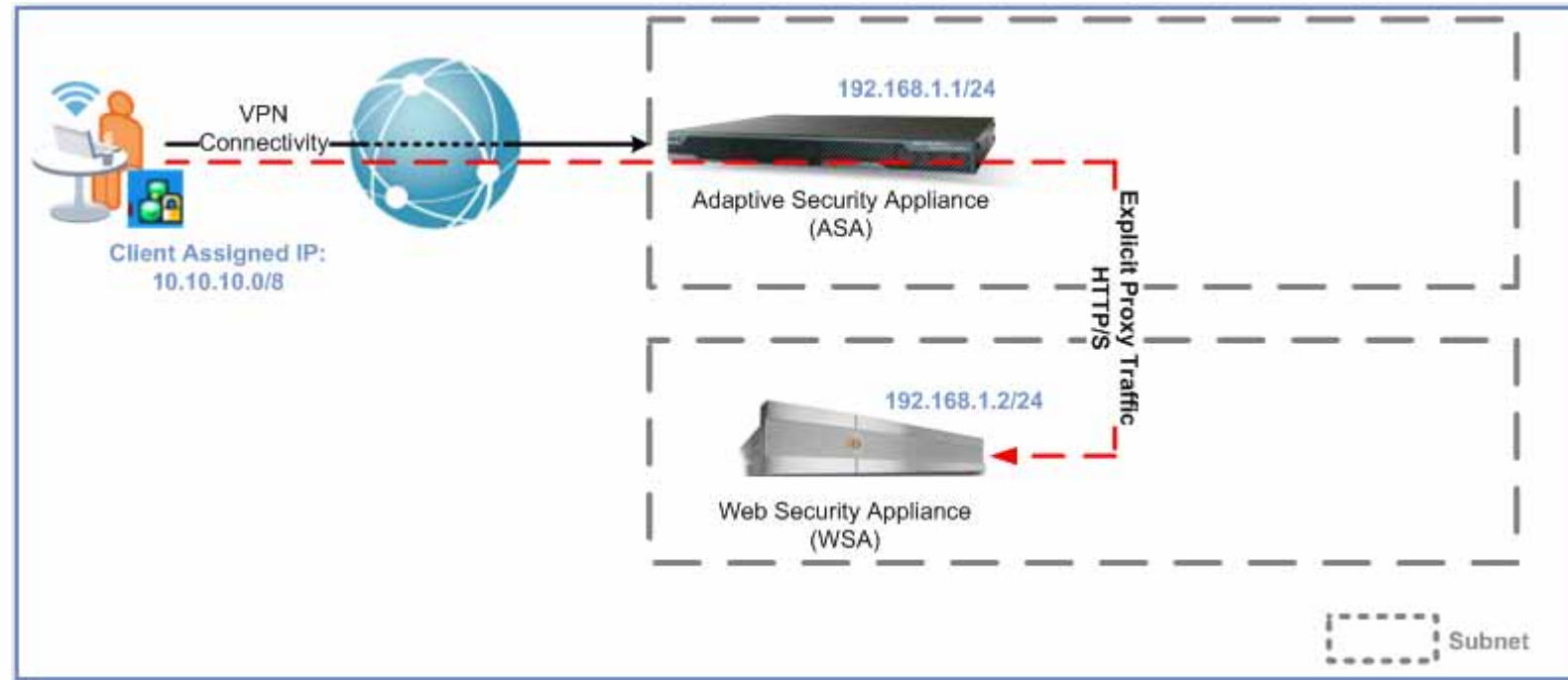
```
route inside 0.0.0.0 0.0.0.0 192.168.1.2 tunneled  
route inside 10.10.10.0 255.0.0.0 192.168.1.2
```

IOS Config

```
ip wccp 80 redirect-list redirect-acl  
  
interface eth0  
  ip wccp 80 redirect in
```



Explicit Proxy Redirection



Explicit Proxy Redirection

Knowledge
Is Power.
Learn. Share. Collaborate.



Edit Internal Group Policy: Secure Mobility

General
Servers
Advanced
Split Tunneling
Browser Proxy
SSL VPN Client
IPsec Client

Proxy Server Policy

Inherit

Do not modify client proxy settings

Do not use proxy

Select proxy server settings from the following

Auto detect proxy

Use proxy server settings given below

Use proxy auto configuration (PAC) given below

Proxy Server Settings

Server Address and Port: Inherit 192.168.1.2

Bypass server for local addresses: Inherit Yes No

Exception List
Enter the list of addresses that will not be accessed through a proxy server. This list corresponds to the Exceptions box in the Proxy Settings dialog box in Internet Explorer.

Exceptions: Inherit

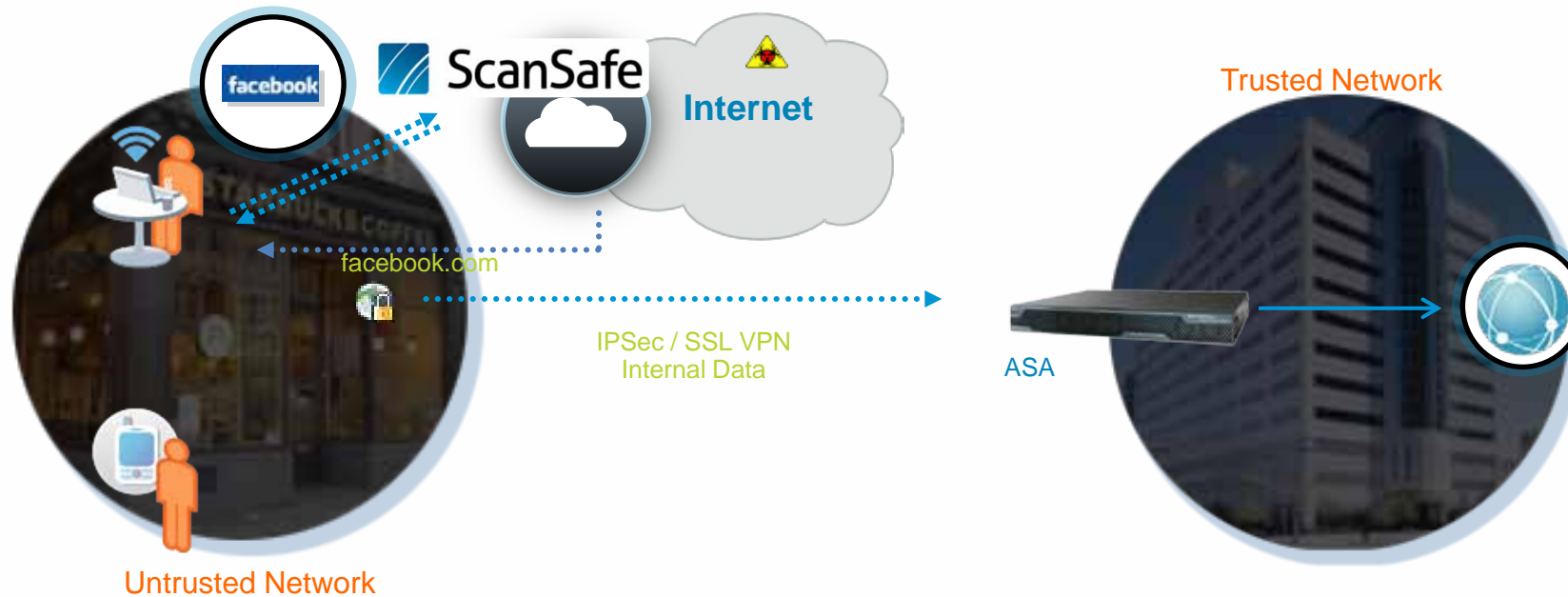
Proxy Auto Configuration (PAC)

Find: Next Previous

OK Cancel Help

Cisco AnyConnect Secure Mobility with Cloud Web Security

Knowledge
Is Power.
Learn. Share. Collaborate.



AnyConnect

- Always-on VPN (admin configurable)
- Optimal head end auto-detect
- Transparent auth (certificate)

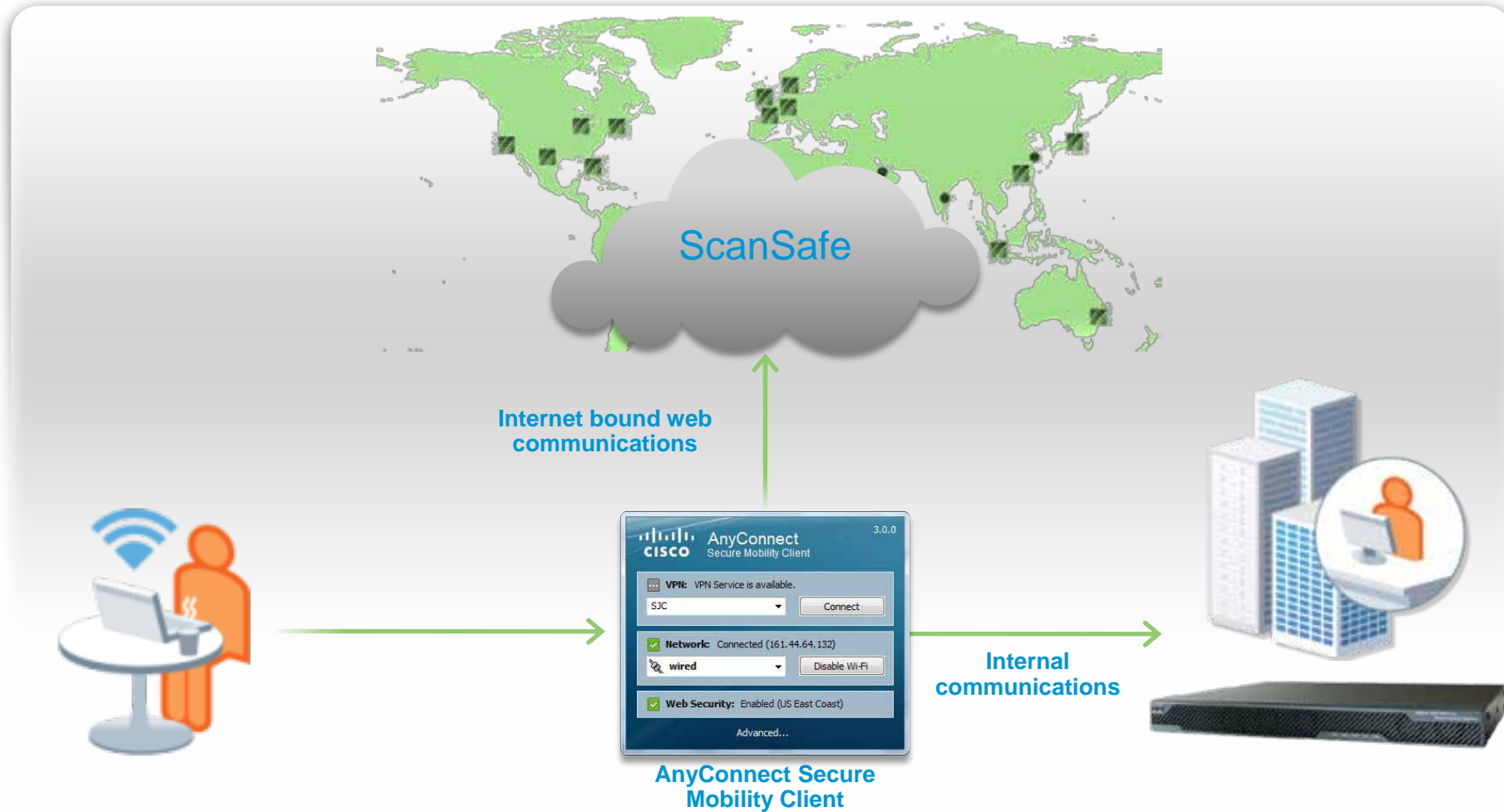
ScanSafe

- Web 2.0 Content Control
- Dynamic Web Classification
- Search Ahead
- Outbreak Intelligence

AnyConnect 3.0

Web Security with ScanSafe

Knowledge
Is Power.
Learn. Share. Collaborate.



AnyConnect 3.0

Web Security with ScanSafe



AnyConnect Client Profile Editor - ScanSafe

Profile: ScanSafe

Web Security

- Scanning Proxy
- Exceptions
- Preferences
- Authentication
- Advanced

Scanning Proxy

Updates to the Scanning Proxy list are now available.

Scanning Proxy	Host Name	Plain Port	SSL Port	Display/Hide
UK		8080	443	Display
Germany		8080	443	Display
France		8080	443	Display
Denmark		8080	443	Display
US West Coast		8080	443	Display
US East Coast		8080	443	Display
US Midwest		8080	443	Display
UK South		8080	443	Display

Update Proxies

Display

Hide

Display All

Default Scanning Proxy

US Midwest

Traffic Listen Port

Add

Delete

80
8080
3128

OK Cancel Help



Cisco
Networkers 2011

May 19, Toronto, Canada

Knowledge
Is Power.

Learn. Share. Collaborate.



Feature Highlights

Cisco AnyConnect Secure Mobility Features

Knowledge
Is Power.
Learn. Share. Collaborate.



AnyConnect

- § Trusted Network Detection
- § Session Persistence
- § Optimal Gateway Selection
- § Always-on VPN
- § Enhanced Device Support
- § IPSec IKEv2
- § Network Access Manager
- § Telemetry
- § SCEP Enrollment

ASA Firewall

- § AnyConnect Secure Mobility Head End Support
- § Optimized WSA Traffic handoff
- § Simplified Management
- § Enterprise firewall
- § Remote Access Head End
- § BotNet Filter

Web Security Appliance

- § Remote Specific Policy
- § Application Controls
- § SaaS Access Control
- § Multi-layer malware defense
- § URL filtering & Dynamic Categorization
- § Data Security
- § Application Visibility and Control

Cloud Web Security

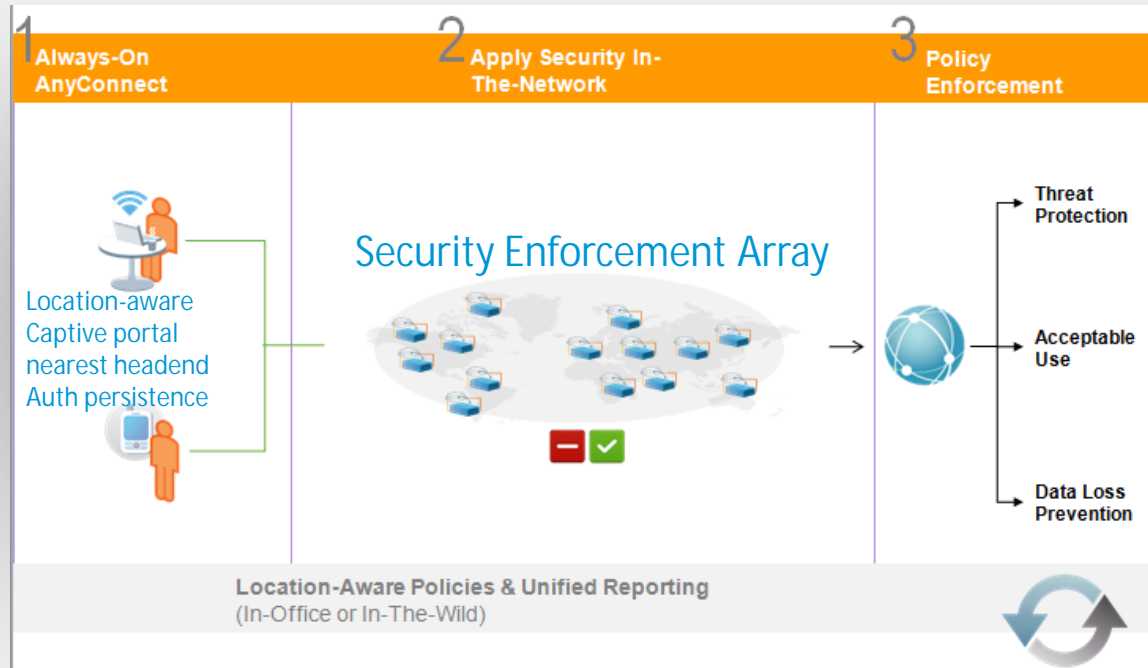
- § Web 2.0 Content Control
- § Dynamic Web Classification
- § HTTP/s Scanning
- § Search Ahead
- § Outbreak Intelligence
- § Real-Time Content Analysis

§ Acceptable Use / Control

§ Malware Defense

Cisco AnyConnect Secure Mobility Always On

Knowledge
Is Power.
Learn. Share. Collaborate.



Security Persistence with Always On VPN
(Fail Closed or Fail Open)

- Always On VPN extends the virtual perimeter to the endpoint
 - § Security Persistence and policy are administratively controlled
 - § If ASA head-end is unreachable,
 - § fail-open (direct network access)
 - or
 - § fail-close (no network access)

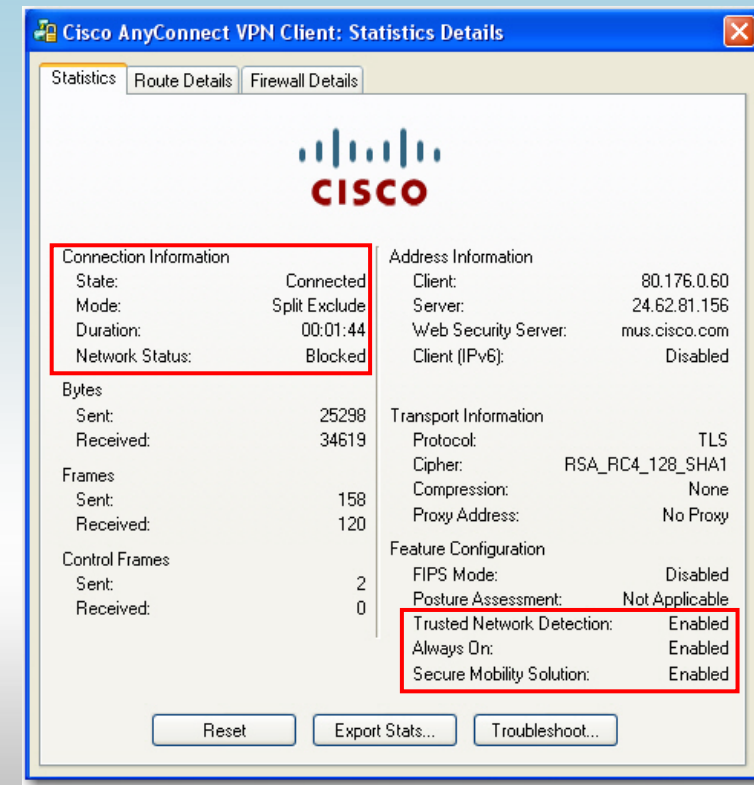
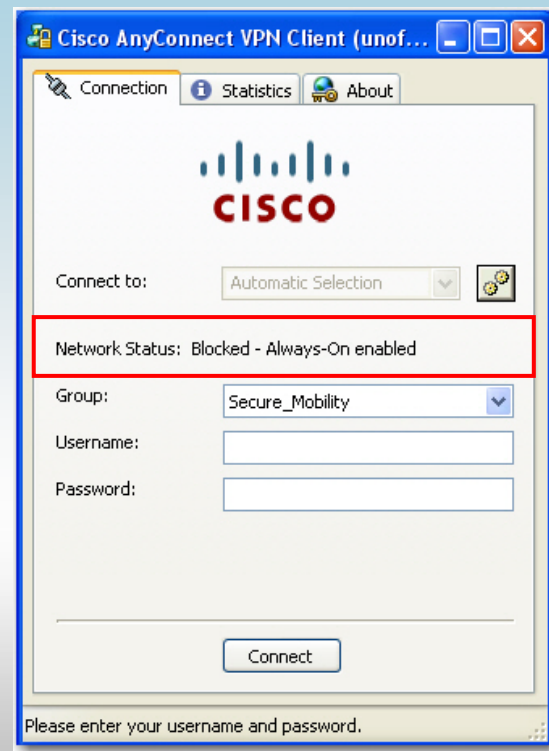
Cisco AnyConnect Secure Mobility Session Persistence

Knowledge
Is Power.
Learn. Share. Collaborate.



- § Always-On, Failed Closed
- § No Network Access Available
- § Manual URL Entry is not Allowed

§ Connection Status



AnyConnect Always-On ASDM Profile Configuration

Knowledge
Is Power.
Learn. Share. Collaborate.



Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile

Preferences

Auto Reconnect User Controllable
Auto ReconnectBehavior User Controllable
ReconnectAfterResume ▾

Preferences(Cont)

Enable Automatic Server Selection User Controllable
Suspension Time Threshold (hours) 4
Performance Improvement Threshold (%) 20

Automatic VPN Policy
Trusted Network Policy Disconnect ▾
Untrusted Network Policy Connect ▾
Trusted DNS Domains cisco.com
Trusted DNS Servers 90.176.0.1

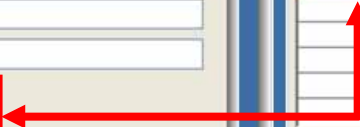
Always On
Connect Failure Policy Closed ▾

Allow Captive Portal Remediation
Remediation Timeout 5

Server List

Hostname	Host Address	User Group	Backup Server List	Automatic SCEP Host	CA URL
vpn.cisco.com			-- Inherited --		

Add Delete
Edit Details



Trusted Network Detection Intelligent Mobility

Knowledge
Is Power.
Learn. Share. Collaborate.



Trusted Network Detection



In Office



Out of Office

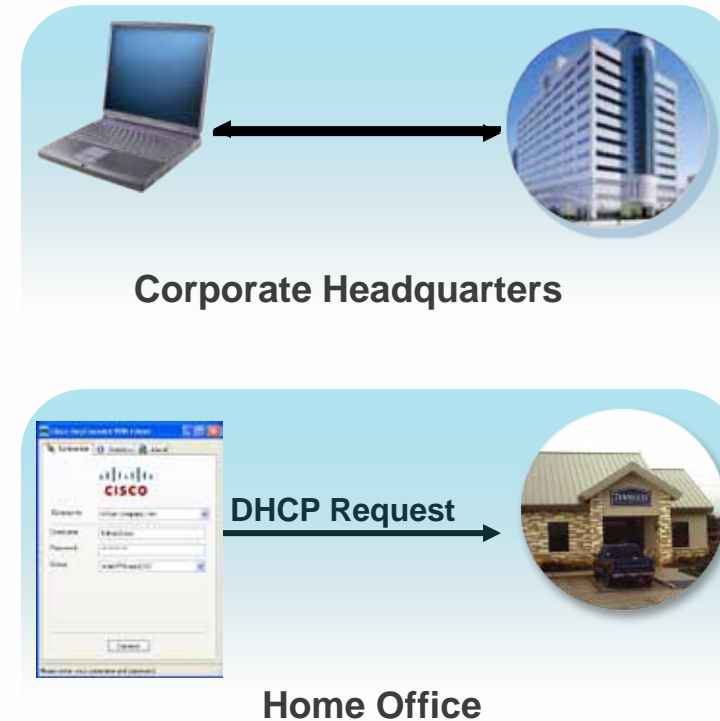
- § Automatically connects or disconnects under the following conditions:
 - § In Office
 - § Out of Office
- § Location determination made by Default Domain Name or DNS server IP
 - § Other checks likely in future
- § Certificate authentication for seamless reconnection
- § Administratively controlled policy
- § Windows XP, Vista, 7 & Mac OS X

Trusted Network Detection



Detects Trusted or Untrusted Network Infrastructures for Secure Connectivity

- § **Trusted Network Detection is Configurable VIA the AnyConnect Profile**
- § **Trusted Networks can be Defined as DNS Suffixes or DNS Server IP Addresses**
- § **DNS Suffixes and DNS Server IP Addresses must be defined on the Client Workstation Dynamically (DHCP)**
- § **If Both the Trusted DNS Suffix and DNS Server IP Address are Defined, the Entries will be ANDed to Determine the Trusted Network**



Trusted Network Detection

ASDM Profile Configuration

Knowledge
Is Power.
Learn. Share. Collaborate.



[Configuration](#) > [Remote Access VPN](#) > [Network \(Client\) Access](#) > [AnyConnect Client Profile](#)

Preferences

<input checked="" type="checkbox"/> Auto Reconnect	<input checked="" type="checkbox"/> User Controllable
Auto ReconnectBehavior	<input checked="" type="checkbox"/> User Controllable
<input type="text" value="ReconnectAfterResume"/> ▼	

Preferences(Cont)

<input checked="" type="checkbox"/> Enable Automatic Server Selection	<input checked="" type="checkbox"/> User Controllable
Suspension Time Threshold (hours)	<input type="text" value="4"/>
Performance Improvement Threshold (%)	<input type="text" value="20"/>
<input checked="" type="checkbox"/> Automatic VPN Policy	
Trusted Network Policy	<input type="text" value="Disconnect"/> ▼
Untrusted Network Policy	<input type="text" value="Connect"/> ▼
Trusted DNS Domains	<input type="text" value="cisco.com"/>
Trusted DNS Servers	<input type="text" value="90.176.0.1"/>
<input checked="" type="checkbox"/> Always On	
Connect Failure Policy	<input type="text" value="Closed"/> ▼
<input checked="" type="checkbox"/> Allow Captive Portal Remediation	
Remediation Timeout	<input type="text" value="5"/>

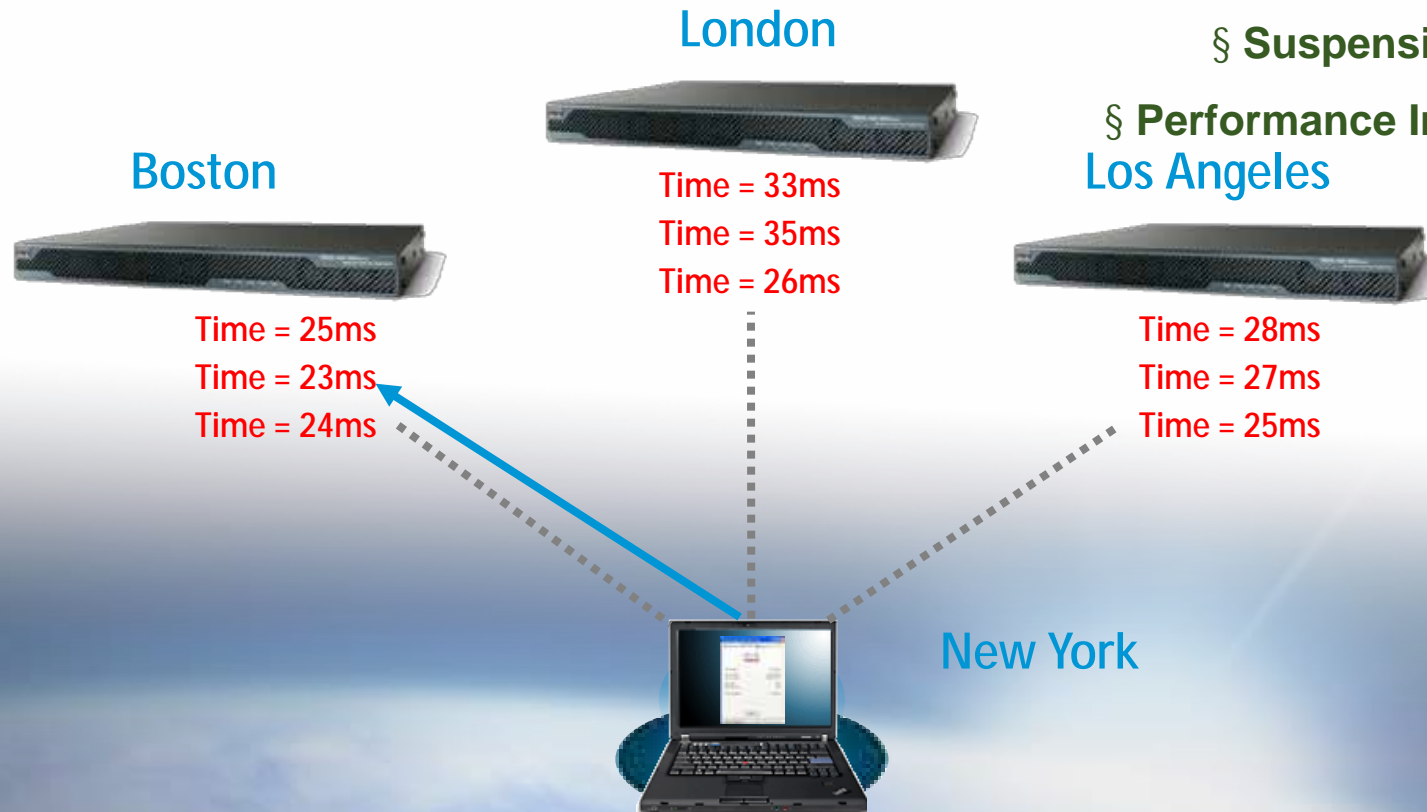
Optimal Gateway Selection



Feature Parameters:

§ Suspension Time Threshold (hours)

§ Performance Improvement Threshold (%)
Los Angeles



Optimal Gateway Selection

ASDM Profile Configuration

Knowledge
Is Power.
Learn. Share. Collaborate.



[Configuration](#) > [Remote Access VPN](#) > [Network \(Client\) Access](#) > [AnyConnect Client Profile](#)

Preferences

<input checked="" type="checkbox"/> Auto Reconnect	<input checked="" type="checkbox"/> User Controllable
Auto ReconnectBehavior	<input checked="" type="checkbox"/> User Controllable
ReconnectAfterResume	

Preferences(Cont)

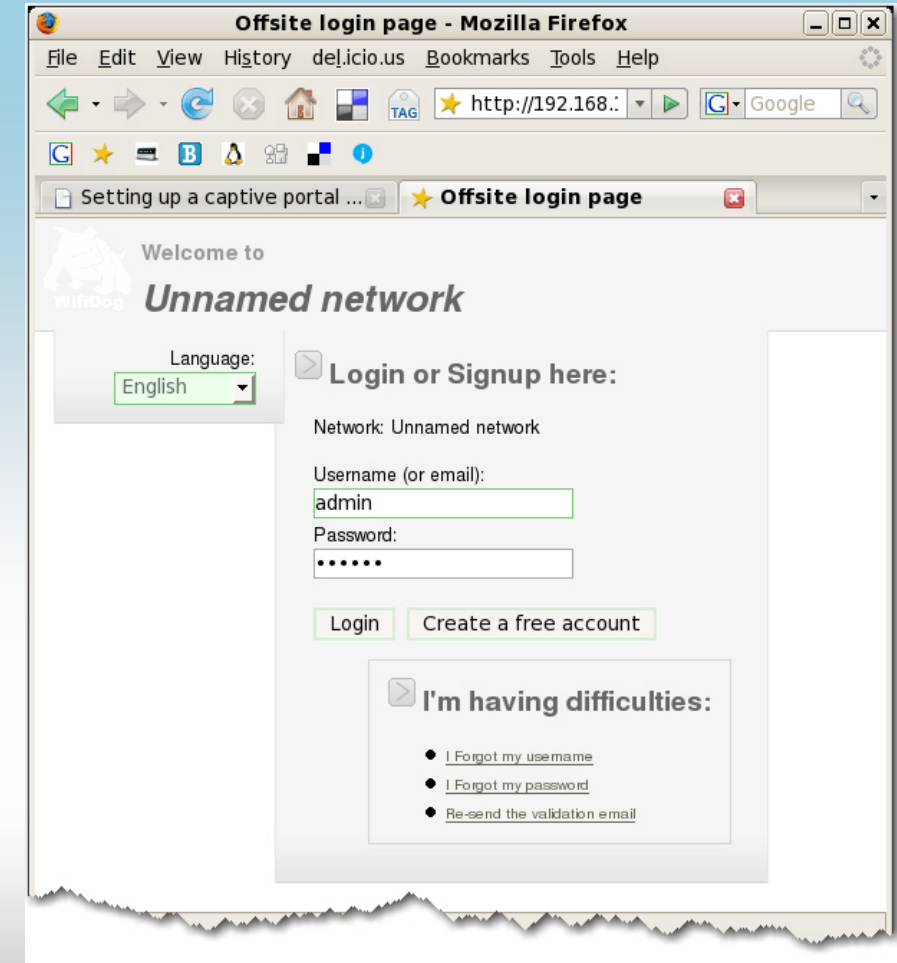
<input checked="" type="checkbox"/> Enable Automatic Server Selection	<input checked="" type="checkbox"/> User Controllable
Suspension Time Threshold (hours)	4
Performance Improvement Threshold (%)	20
<input checked="" type="checkbox"/> Automatic VPN Policy	
Trusted Network Policy	Disconnect
Untrusted Network Policy	Connect
Trusted DNS Domains	cisco.com
Trusted DNS Servers	90.176.0.1
<input checked="" type="checkbox"/> Always On	
Connect Failure Policy	Closed
<input checked="" type="checkbox"/> Allow Captive Portal Remediation	
Remediation Timeout	5

Captive Portal Detection

§ Always-On enforces VPN connectivity.

§ If AnyConnect fails to connect, its endpoint can fail closed, preventing network connectivity to and from the endpoint.

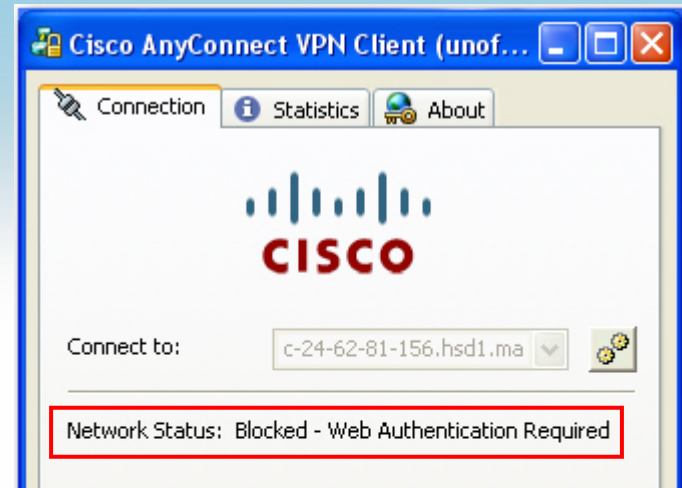
§ Always-On allows AnyConnect users to remediate their Captive Port prior to required VPN establishment.



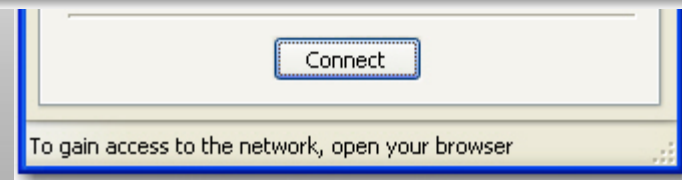
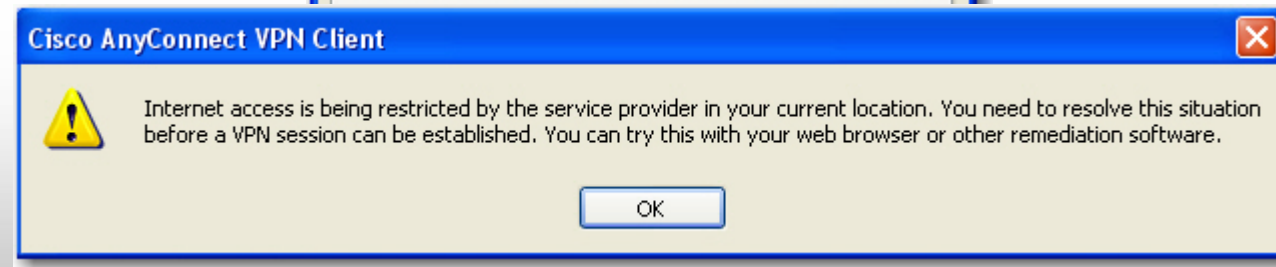
Captive Portal Detection

User Experience

Knowledge
Is Power.
Learn. Share. Collaborate.



§ Captive Portal Remediation Required



Captive Portal

ASDM Profile Configuration

Knowledge
Is Power.
Learn. Share. Collaborate.



[Configuration](#) > [Remote Access VPN](#) > [Network \(Client\) Access](#) > [AnyConnect Client Profile](#)

Preferences

<input checked="" type="checkbox"/> Auto Reconnect	<input checked="" type="checkbox"/> User Controllable
Auto Reconnect Behavior	<input checked="" type="checkbox"/> User Controllable
ReconnectAfterResume <input type="button" value="v"/>	

Preferences(Cont)

<input checked="" type="checkbox"/> Enable Automatic Server Selection	<input checked="" type="checkbox"/> User Controllable
Suspension Time Threshold (hours)	<input type="text" value="4"/>
Performance Improvement Threshold (%)	<input type="text" value="20"/>
<input checked="" type="checkbox"/> Automatic VPN Policy	
Trusted Network Policy	<input type="button" value="Disconnect"/> <input type="button" value="v"/>
Untrusted Network Policy	<input type="button" value="Connect"/> <input type="button" value="v"/>
Trusted DNS Domains	<input type="text" value="cisco.com"/>
Trusted DNS Servers	<input type="text" value="90.176.0.1"/>
<input checked="" type="checkbox"/> Always On	
Connect Failure Policy	<input type="button" value="Closed"/> <input type="button" value="v"/>
<input checked="" type="checkbox"/> Allow Captive Portal Remediation	
Remediation Timeout	<input type="text" value="5"/>

Session Persistence

Network Follows Users – It Just Works

Knowledge
Is Power.
Learn. Share. Collaborate.



Persistent
Connectivity

Auto-detect and connect
Transparent handoff
Session persistence

§ VPN session remains connected

§ While user migrates between networks (3G, WiFi, LAN, etc)

§ During loss of network connectivity

§ During system hibernation / standby

§ Administratively controlled policy

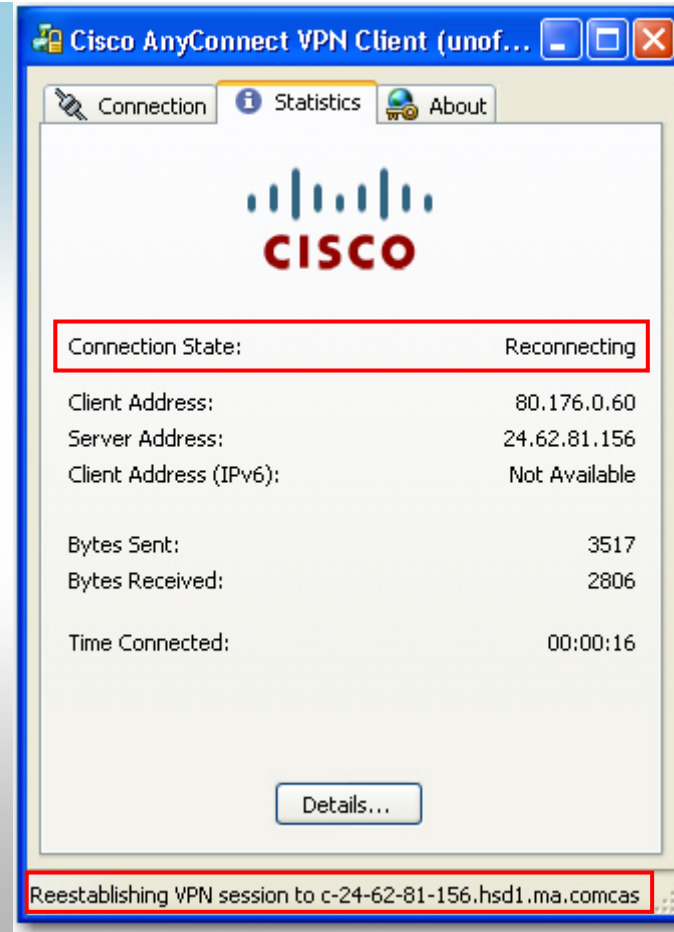
§ Compatible with all auth methods

User does not re-authenticate after hibernation/standby

Session Persistence

User Experience: User Indicator

Knowledge
Is Power.
Learn. Share. Collaborate.

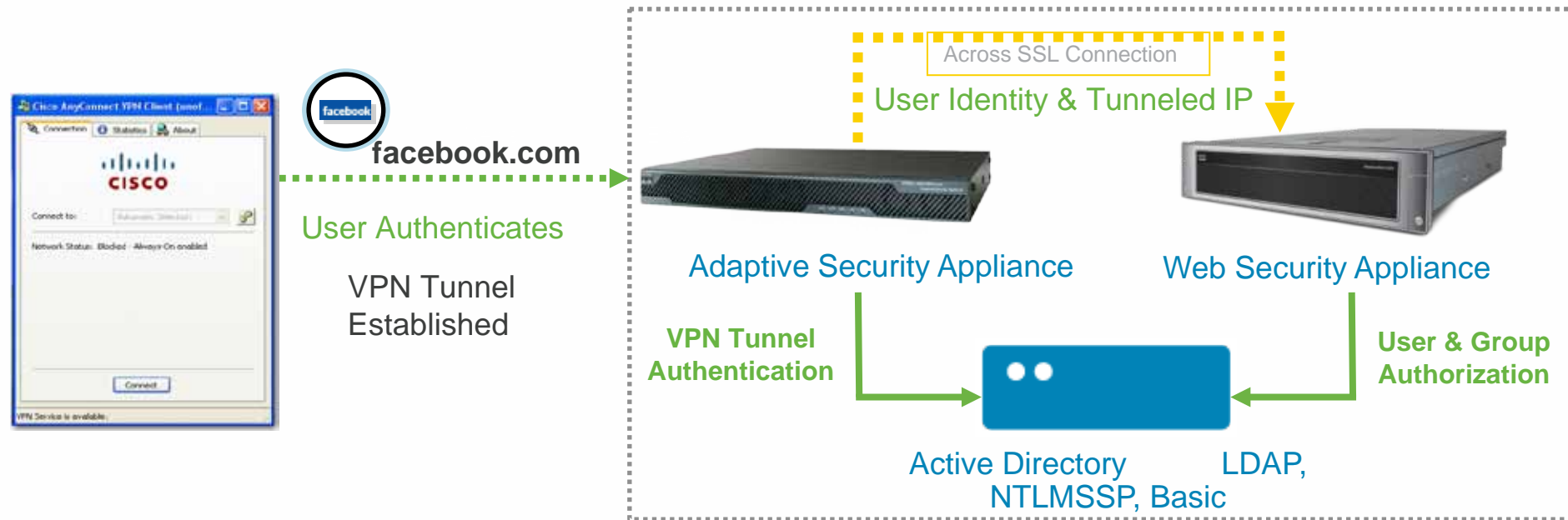


§ Connection State: Reconnecting

Cisco AnyConnect Secure Mobility

ASA-WSA Communication

Knowledge
Is Power.
Learn. Share. Collaborate.



ASA → WSA

1. AnyConnect Authenticates and Establishes a VPN Tunnel to the ASA
2. ASA Extracts Username from Certificate or AAA Server
3. ASA Forwards Username and Tunneled IP Address to the WSA
4. WSA Verifies Username and Group Membership against Active Directory
5. WSA Applies Policies based on Username or Group Membership

ASA > WSA Configuration

ASA to WSA Communication

Knowledge
Is Power.
Learn. Share. Collaborate.



- § ASA & WSA Communication Network
- § Enable Secure Mobility Solution
- § Services Port
- § WSA Access Password

Configuration > Remote Access VPN > Network (Client) Access > Secure Mobility Solution

Solution Access Control

Specify the addresses of the hosts/networks from where WSAs can communicate with this security appliance.

[+](#) Add [✎](#) Edit [🗑](#) Delete

Interface	IP Address	Mask
inside	10.10.10.250	255.255.255.255

Solution Setup

Enable Secure Mobility Solution

Service Port: ←

Change Password

WSA Access Password: ←

Confirm Password:

WSA > ASA Configuration

ASA to WSA Communication

Knowledge
Is Power.
Learn. Share. Collaborate.



- § Enable Secure Mobility Solution
- § Enable Cisco ASA Integration
- § ASA Hostname or IP Address & Service Port & Access Password

Monitor Web Security Manager Security Services Network System Administration

Mobile User Security Settings

When Mobile User Security is enabled, a policy can be created based on whether the user is physically in the corporate network or login through VPN.

Enable Mobile User Security

Define Remote Users by:

IP Range

(examples: 10.1.1.1, 10.1.1.0/24, 10.1.1.1-10)

Cisco ASA Integration

ASA Hostname or IP Address	Port	
<input type="text" value="172.20.11.11"/>	<input type="text" value="8081"/>	<input type="button" value="Add Row"/>
		<input type="button" value="Delete"/>

The values below will be applicable to all ASAs configured above.

ASA Access Password:

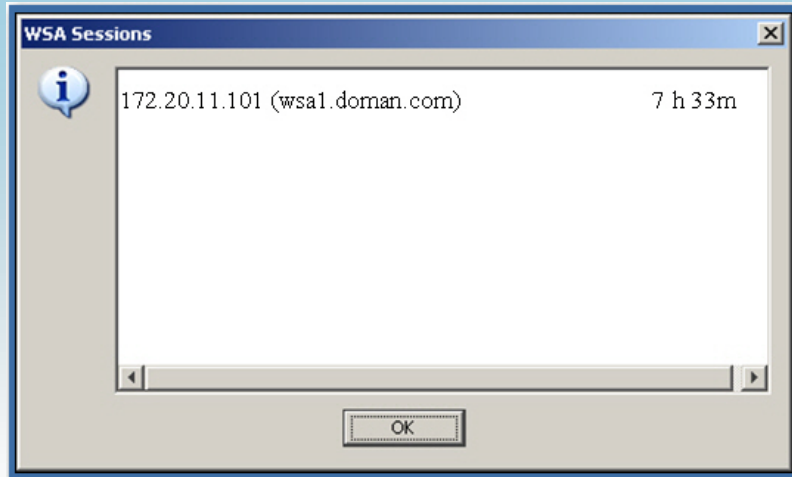
ASA > WSA Configuration

Communication Test

Knowledge
Is Power.
Learn. Share. Collaborate.



§ Verify ASA > WSA Communication



§ Verify WSA > ASA Communication

Start Test

Checking DNS resolution of ASA hostname(s)...
Success: Resolved '10.10.10.230' address: 10.10.10.230

Connecting and Running a test query on the ASA(s)...

Connecting and Running a test query on the ASA(s)...
Success: Connected and Authenticated with '10.10.10.230'
Success: Connected and Authenticated with '10.10.10.230'



Cisco
Networkers 2011

May 19, Toronto, Canada

Knowledge
Is Power.

Learn. Share. Collaborate.

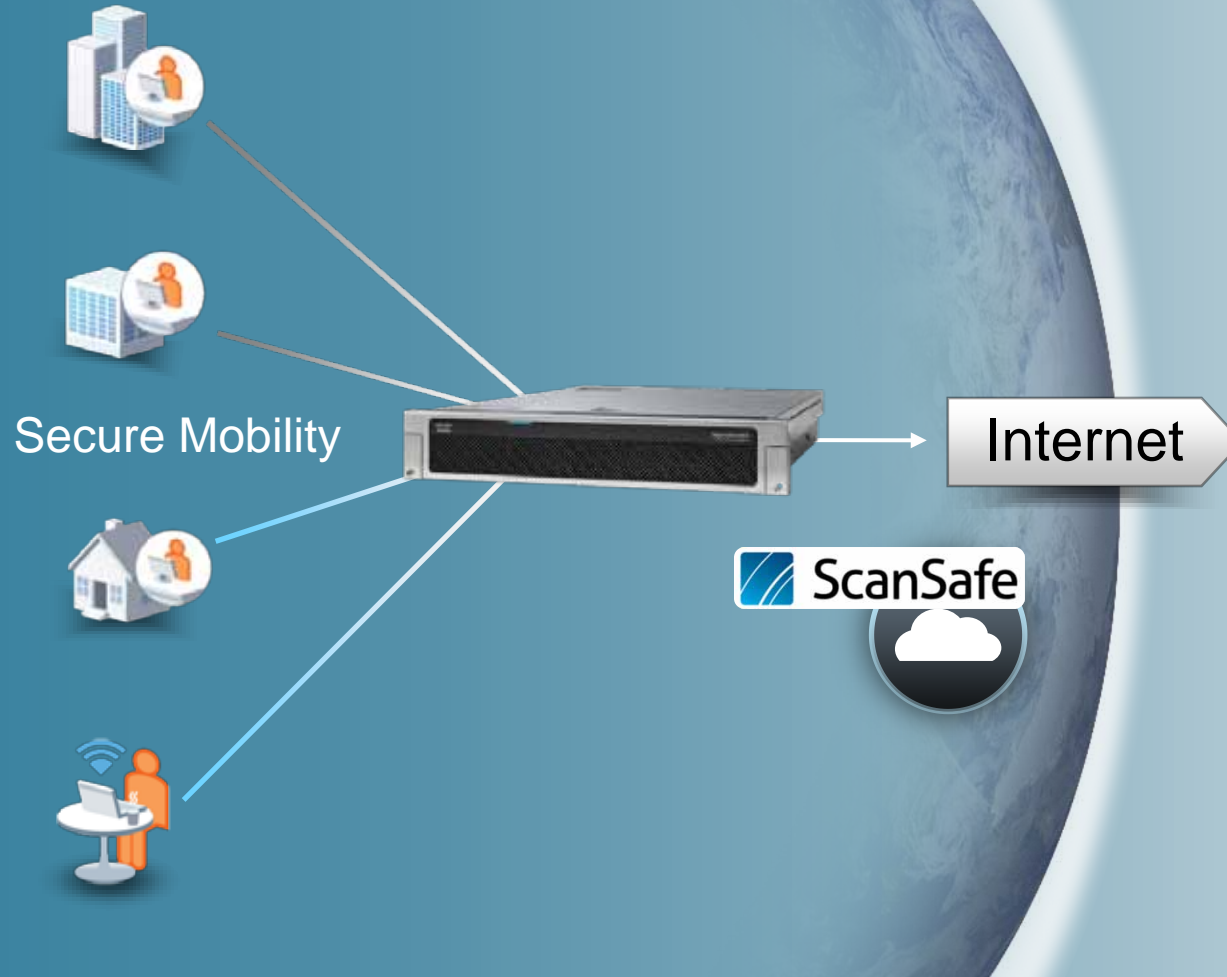


Policy Enforcement Control / Security

Cisco IronPort Web Security Appliance

Industry Leading Secure Web Gateway

Knowledge
Is Power.
Learn. Share. Collaborate.



Security



Malware
Defense



Data
Security

Control



Acceptable
Use Controls



SaaS Access
Controls

Centralized Management and Reporting



Cisco
Networkers 2011

May 19, Toronto, Canada

Knowledge
Is Power.

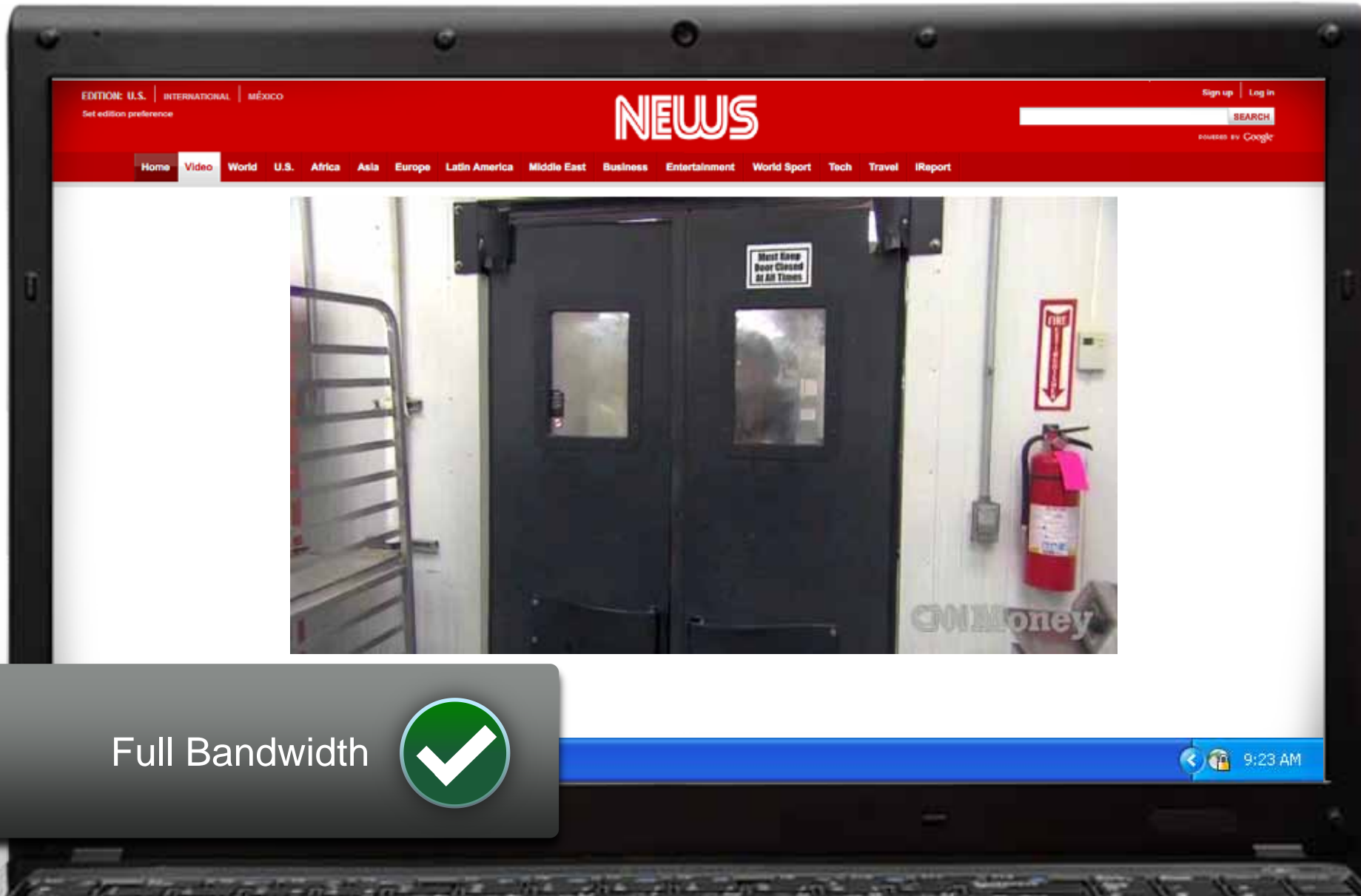
Learn. Share. Collaborate.



Controls in Action

Bandwidth Control: Corporate Approved

Knowledge
Is Power.
Learn. Share. Collaborate.



Full Bandwidth



Web Security Appliance Configuration

Allow Business Relevant Video

Knowledge
Is Power.
Learn. Share. Collaborate.



Access Policies

Policies

[Add Policy...](#)

Order	Group	Protocols and User Agents	URL Filtering	Applications
1	Allow Business Relevant Video Identity: All URL Categories: Infrastructure, News	(global policy)	Monitor: 2 Safe Search:	Block: 6

Applications Settings

[Browse Application Types](#)

To identify some applications, inspection of HTTPS content may be required. For best efficacy, enable the HTTP... enables decryption for application visibility and control (see Security Services > HTTPS Proxy).

Applications	Settings
	Edit all...
+ LinkedIn	5 Monitor Edit all...
+ Media	Bandwidth Limit: No Bandwidth Limit 11 Monitor Edit all...

Bandwidth Control: Restricted

Knowledge
Is Power.
Learn. Share. Collaborate.



Video **SHARE** Search Browse Upload

299 views 9:23 AM

Finance Legal Marketing

Web Security Appliance Configuration

Restrict Media

Knowledge
Is Power.
Learn. Share. Collaborate.



Access Policies

Policies

[Add Policy...](#)

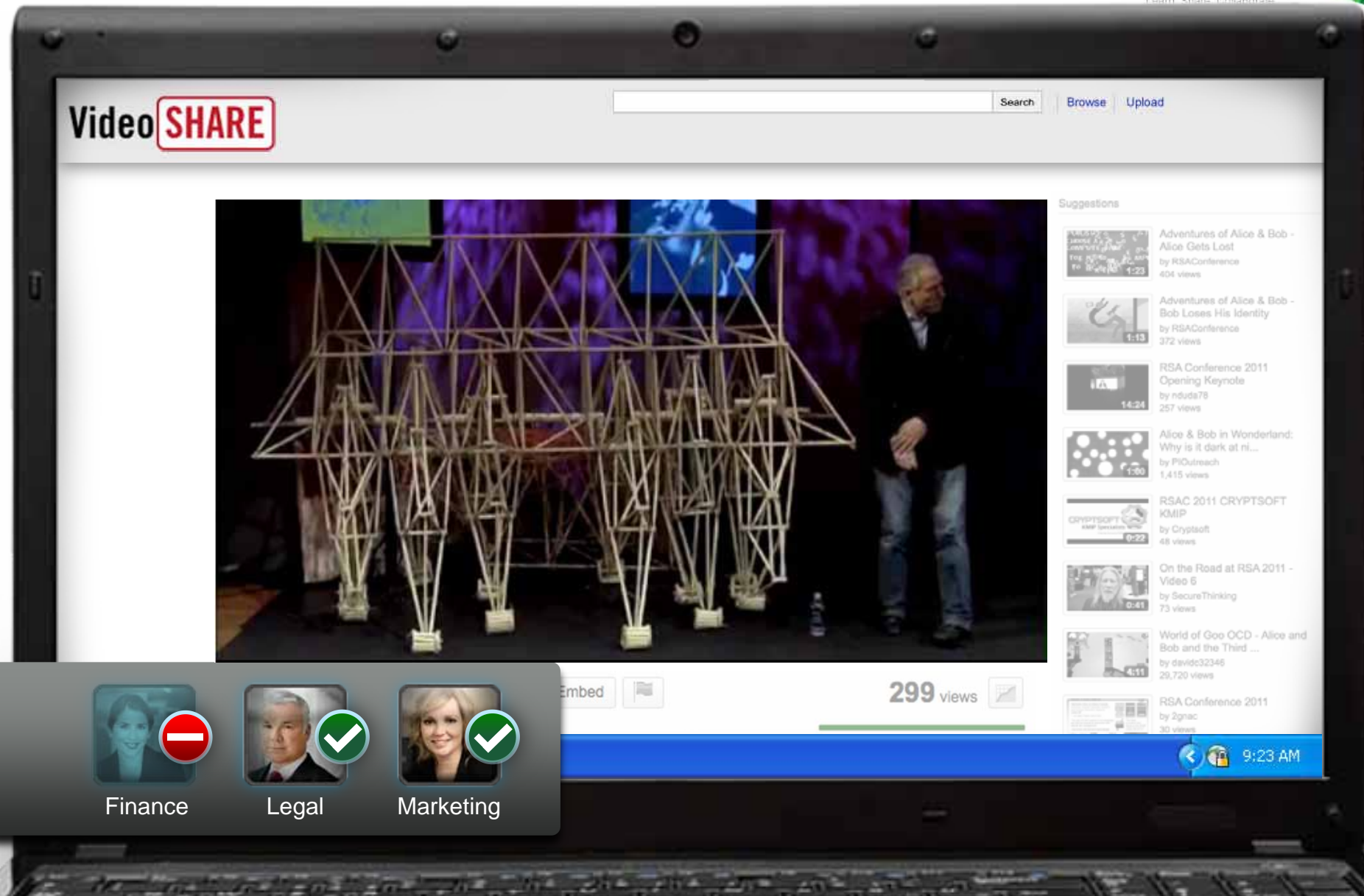
Order	Group	Protocols and User Agents	URL Filtering	Applications
	Global Policy Identity: All	No blocked items	Block: 10 Warn: 4 Monitor: 52 Safe Search: Block All Unsafe Site Content Ra	

Default Actions for Application Types

Application Types	Default Action for Type
Blogging	🟡 Monitor
Facebook	🟡 Monitor
Instant Messaging	🟡 Monitor
LinkedIn	🟡 Monitor
Media	🟡 Monitor Bandwidth Limit: 100 kbps
P2P / File Sharing	🟡 Monitor
Presentation / Conferencing	🟡 Monitor
Social Networking	🟡 Monitor

Bandwidth Control: Customized

Knowledge
Is Power.
Learn Share Collaborate

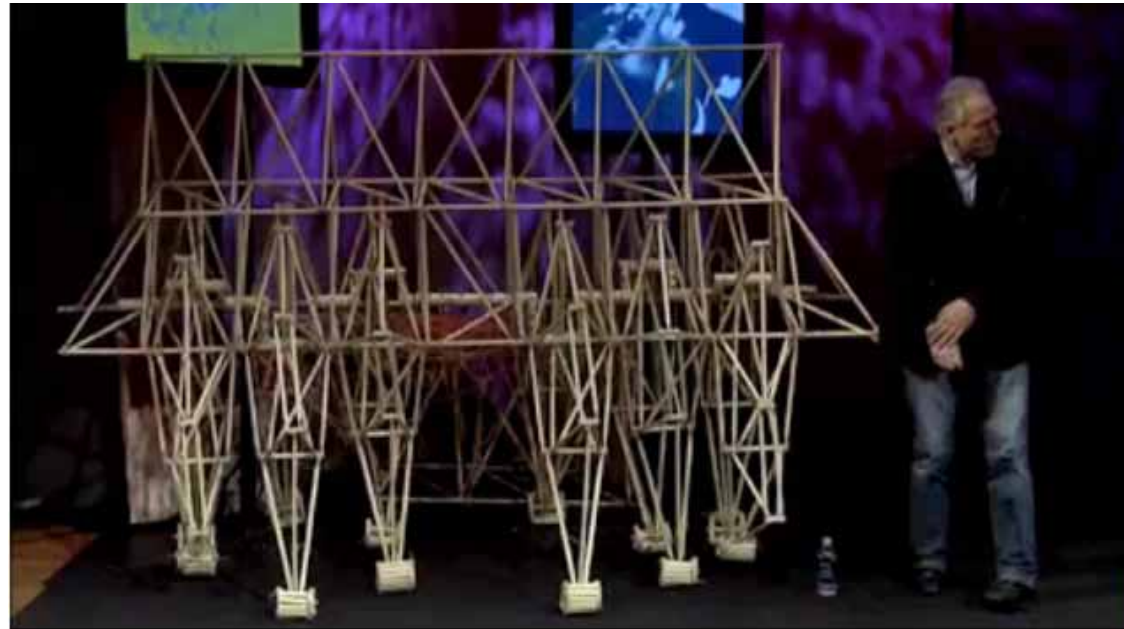


Video **SHARE**

Search

Browse

Upload



Suggestions



Adventures of Alice & Bob - Alice Gets Lost
by RSAConference
404 views



Adventures of Alice & Bob - Bob Loses His Identity
by RSAConference
372 views



RSA Conference 2011 Opening Keynote
by n8uda78
257 views



Alice & Bob in Wonderland: Why is it dark at ni...
by P10utreach
1,415 views



RSAC 2011 CRYPTOSOFT KMIP
by Cryptsoft
48 views



On the Road at RSA 2011 - Video 6
by SecureThinking
73 views



World of Goo OCD - Alice and Bob and the Third ...
by david32346
29,720 views



RSA Conference 2011
by 2gnac
30 views

Embed

299 views

9:23 AM



Finance



Legal



Marketing

Web Security Appliance Configuration

Override Restrictions

Knowledge
Is Power.
Learn. Share. Collaborate.



Access Policies

Policies				
Add Policy...				
Order	Group	Protocols and User Agents	URL Filtering	Applications
1	Marketing Policy Identity: All	(global policy)	(global policy)	Block: 6 Monitor: 41 (Bandwidth Limit: 11)

Identities and Users:

All Authenticated Users

Selected Groups and Users

Groups:
LAB-DEMO\Marketing

Users: No users entered

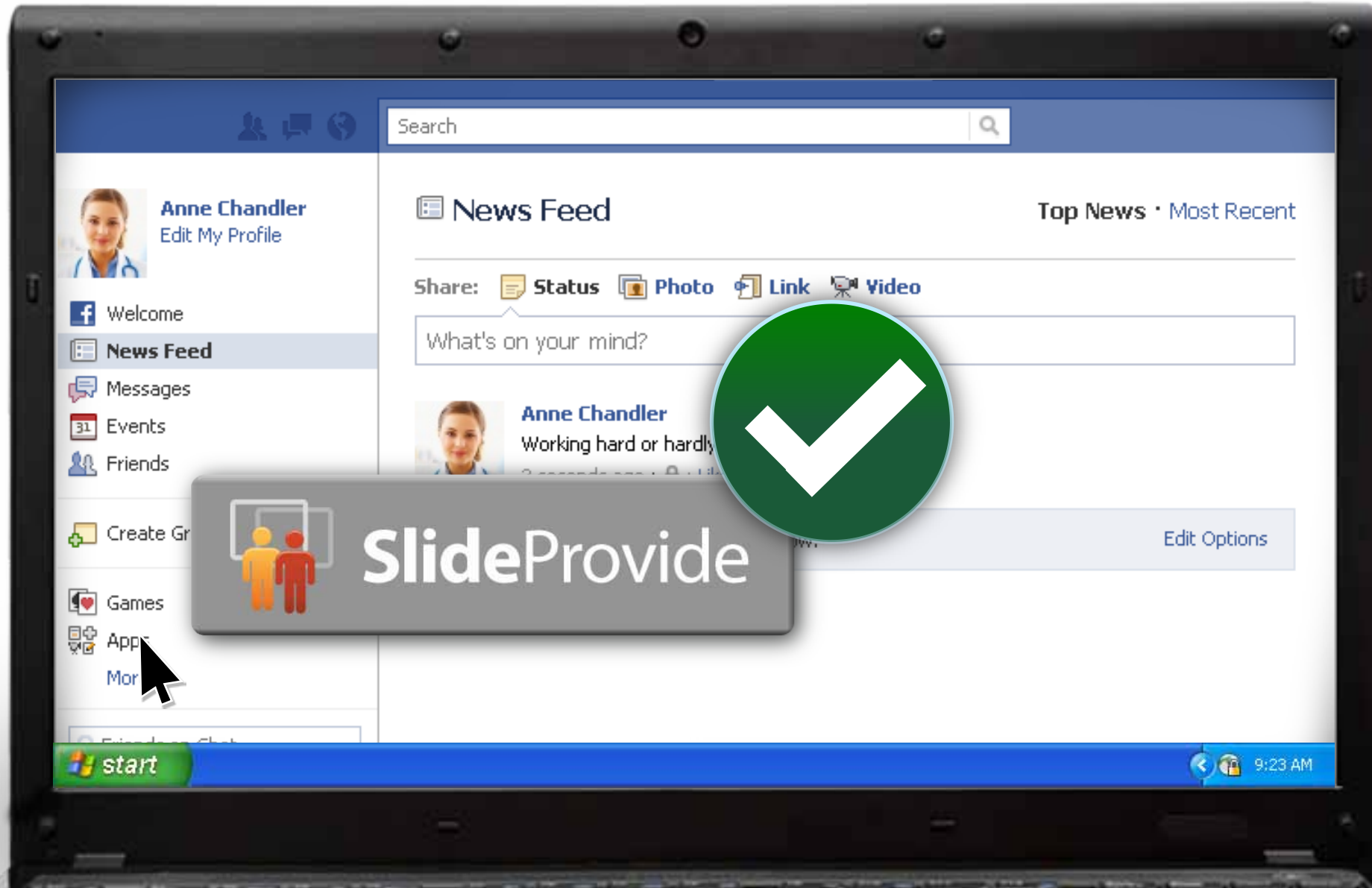
Applications Settings

Browse Application Types

To identify some applications, inspection of HTTPS content may be required. For best efficacy, enables decryption for application visibility and control (see Security Services > HTTPS Proxy).

Applications	
	Edit all...
<input type="checkbox"/> LinkedIn	5 Monitor Edit all...
<input type="checkbox"/> Media	Bandwidth Limit: No Bandwidth Limit 11 Monitor Edit all...

Facebook Controls



Facebook Controls

Knowledge
Is Power.
Learn. Share. Collaborate.



Web Security Appliance Configuration

Facebook Control

Knowledge
Is Power.
Learn. Share. Collaborate.



Access Policies

Policies

[Add Policy...](#)

Order	Group	Protocols and User Agents	URL Filtering	Applications
	Global Policy Identity: All	No blocked items	Block: 10 Warn: 4 Monitor: 52 Safe Search: Block All Unsafe Se Site Content Rating	

Edit Applications Settings

[Browse Application Types](#)

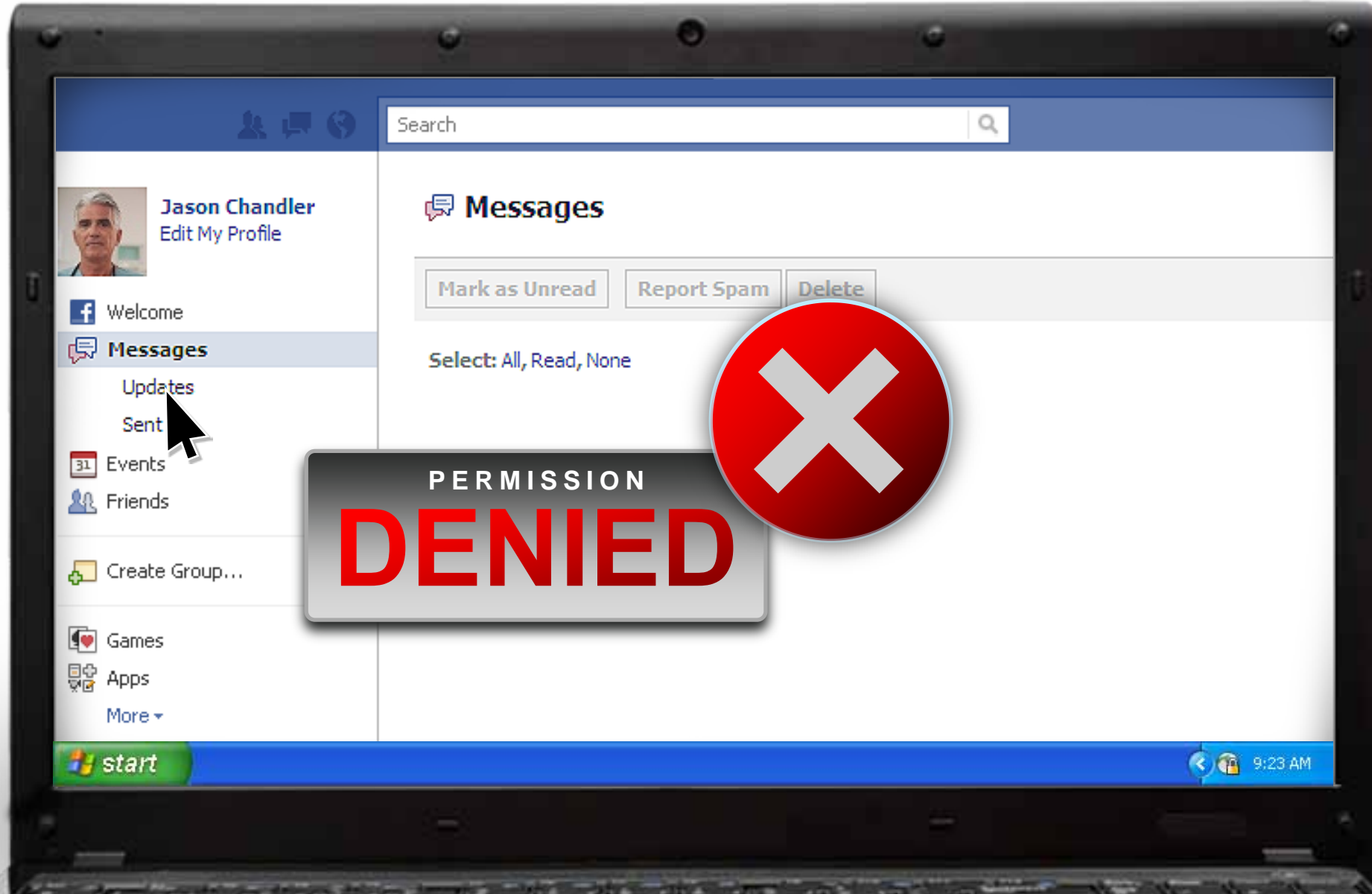
To identify some applications, inspection of HTTPS content may be required. For best efficacy, enable the HTTPS Proxy enables decryption for application visibility and control (see Security Services > HTTPS Proxy).

Applications	Settings
Facebook Applications: Business	Use Default for Type (Monitor)
Facebook Applications: Community	Use Default for Type (Monitor)
Facebook Applications: Education	Use Default for Type (Monitor)
Facebook Applications: Entertainment	Use Default for Type (Monitor)
Facebook Applications: Games	Block
Facebook Applications: Other	Use Default for Type (Monitor)
Facebook Applications: Sports	Block
Facebook Applications: Utilities	Use Default for Type (Monitor)
Facebook Chat	Use Default for Type (Monitor)
Facebook Events	Use Default for Type (Monitor)
Facebook General	Use Default for Type (Monitor)
Facebook Messages	Use Default for Type (Monitor)
Facebook Notes	Use Default for Type (Monitor)

Facebook Controls

May 19, Toronto, Canada

Knowledge
Is Power.
Learn. Share. Collaborate.



Web Security Appliance Configuration

Override Restrictions

Knowledge
Is Power.
Learn. Share. Collaborate.



Access Policies

Policies

Add Policy...

Order	Group	Protocols and User Agents	URL Filtering	Applications
1	Finance Policy Identity: All	(global policy)	Block: 11 Warn: 4 Monitor: 51 Safe Search:	Block: 8 Restrict: 1 Monitor: 33

Identities and Users: All Identities

- All Authenticated Users
- Selected Groups and Users

Groups:
LAB-DEMO\Finance

Applications

Facebook Applications: Utilities

Facebook Chat

Facebook Events

Facebook General

Facebook Messages

Facebook Notes

Facebook Photos

Facebook Places

Settings

Use Global (Monitor)

Block

Restrict: Block 2 behaviors

Restrict: Block 3 behaviors

Set action for application Facebook Messages

Use Global Setting (Monitor)

Monitor

Block Posting Text

Block

Cancel Apply

Restrict: Block 2 behaviors

Restrict: Block 3 behaviors

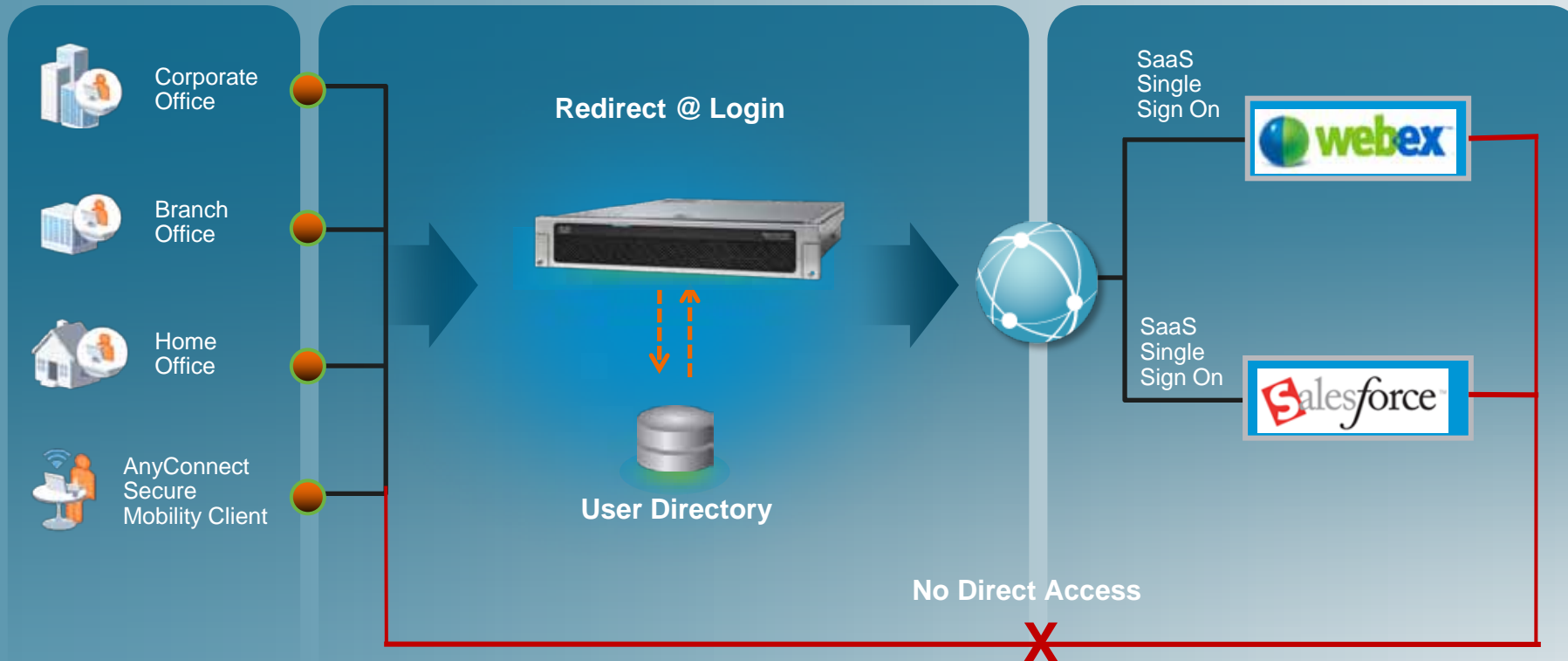
Restrict: Block 2 behaviors

Edit all...

Access Control

Regaining Visibility and Control Through Identity

Knowledge
Is Power.
Learn. Share. Collaborate.



Visibility | Centralized Enforcement | Single Source Revocation

SaaS Single Sign On

Knowledge
Is Power.
Learn. Share. Collaborate.



CRM Search

Home Chatter Getting Started Contacts **Accounts** Reports +

Create New...

Recent Items

No records to display

Recycle Bin

Quick Create

Account Name

Phone

Website

Save

Accounts Home

View: All Accounts

Recent Accounts

No recent records. Click Go or select New

Reports

Active Account

Accounts with

Account Histor

Partner Account

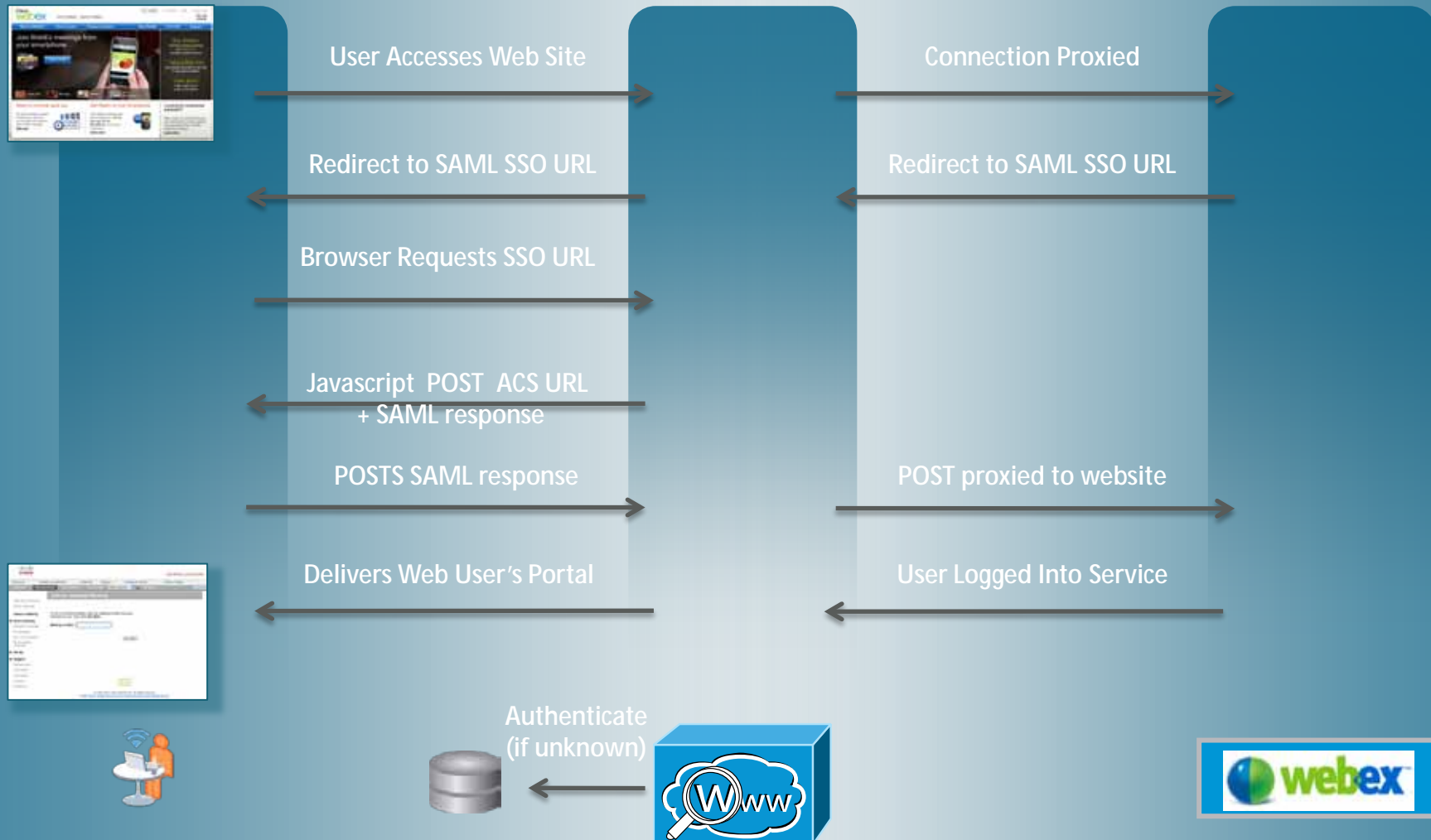
Go to Reports

Edit

Seamless Single Sign-on
No login needed



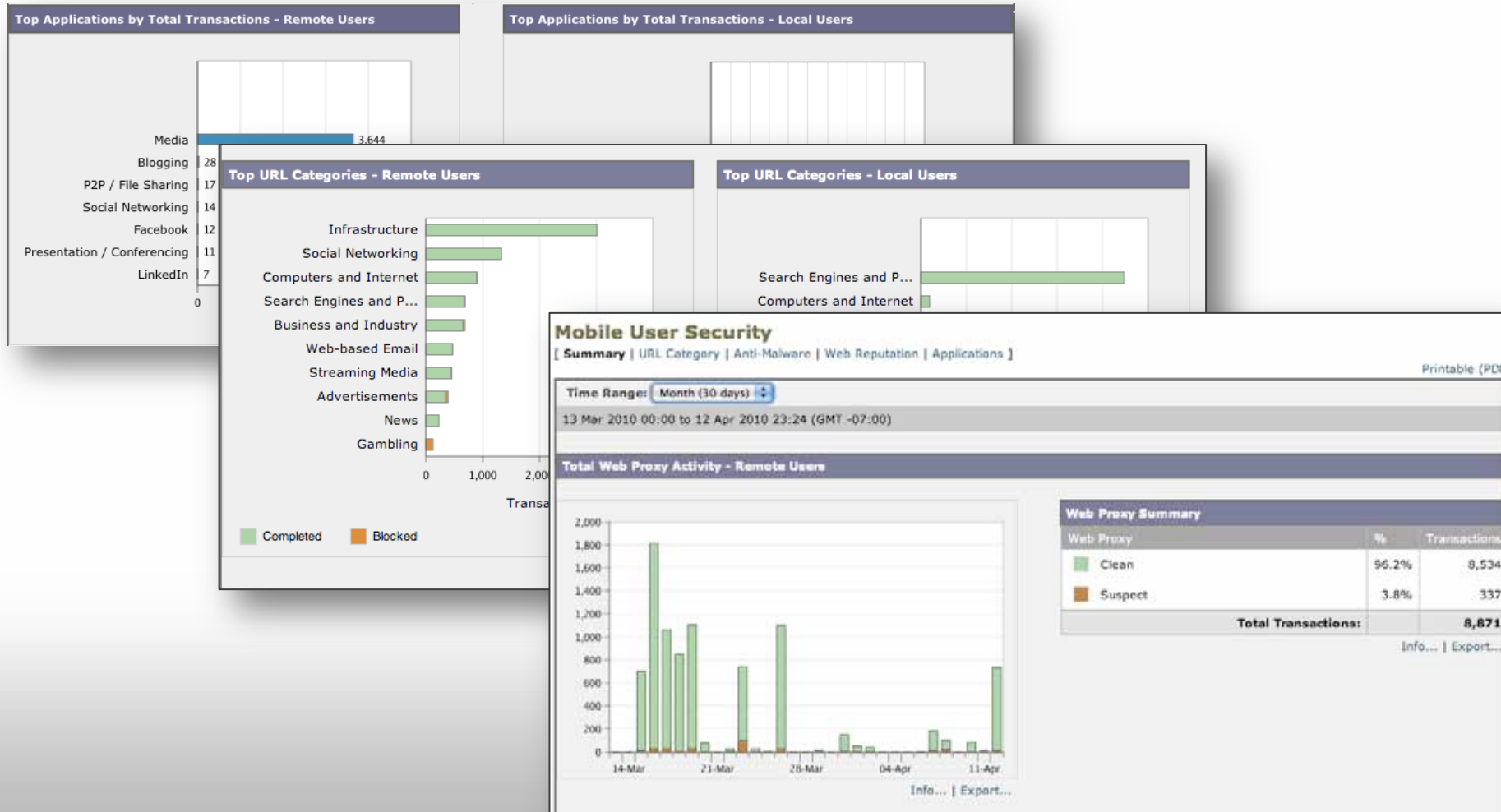
SaaS Single Sign-On



Secure Mobility Reporting

WSA Mobile User Reports

Knowledge
Is Power.
Learn. Share. Collaborate.



Secure Mobility Reporting

Simple investigative tool

Knowledge
Is Power.
Learn. Share. Collaborate.



Track User activity /
Search by IP ranges

Track a web site

Search

Available: 17 Aug 2009 21:44 to 28 Aug 2009 17:31 (GMT)

Time Range: Day

User / Client IP: (ex. jdoe or DOMAIN\jdoe)

Website: (ex. google.com)

Disposition: Allow Block Monitor Warn

Advanced Search transactions using advanced criteria

Clear Search

Printable Download

Items Displayed 50

« Previous | 1 | 2 | Next »

Time (GMT -05:00)	Transaction	Disposition	Bandwidth	User / Client IP
17 May 2010 11:05:13	http://www.ch-non-food.com/	Allow	21.5KB	173.37.9.25
17 May 2010 11:03:44	http://www.jobdig.com/	Allow	84.2KB	173.37.9.25
17 May 2010 11:02:21	http://m1.bzbattery.cn/up/up.htm	Block	2,151B	173.37.9.25
17 May 2010 11:01:43	http://www.oceanaresorts.com/default.asp	Allow	31.3KB	173.37.9.25
17 May 2010 11:00:53	http://www.booksamillion.com/	Allow	58.5KB	173.37.9.25
17 May 2010 11:00:01	http://www.reelviews.net/movies.php	Allow	72.6KB	173.37.9.25
17 May 2010 10:58:25	http://www.browserwelten.net/	Allow	158.1KB	173.37.9.25
17 May 2010 10:58:05	http://www.pathologyoutlines.com/	Allow	827B	173.37.9.25
17 May 2010 10:57:26	http://www.store.nodakoutdoors.com/	Allow	807.2KB	173.37.9.25
17 May 2010 10:57:00	http://www.cellularmagazine.it/include/common.js	Allow	80.7KB	173.37.9.25

- ü Know who is going to which web site
- ü Know who went to a specific web site
- ü And more...

Cisco AnyConnect Secure Mobility

Web Security with Next Generation Remote Access



✓ Data Loss Prevention

✓ Threat Prevention

Acceptable Use ✓

Access Control ✓

Access Granted



Choice

Diverse Endpoint Support for Greater Flexibility

Security

Rich, Granular Security Integrated into the network

Experience

Always-on Intelligent Connection for Seamless Experience and Performance



Cisco
Networkers 2011

May 19, Toronto, Canada

Knowledge
Is Power.

Learn. Share. Collaborate.



Questions



Cisco
Networkers 2011

May 19, Toronto, Canada

Knowledge
Is Power.

Learn. Share. Collaborate.



Final Thoughts

A pessimist sees the
difficulty in every
opportunity; an optimist
sees the opportunity in
every difficulty.

Winston Churchill



Thank you.

