cisco

Bezpečný přístup na základě identity

Jiří Tesař CSE Security, CCIE #14558 jitesar@cisco.com

Program

- Problematika přístupu do sítě
- Bezpečnost postavená na identitě uživatele
- Jak na BYODy ?
- Nastavení mobilních platforem a řízení přístupu do sítě
- Vzdálené VPN přístupy
- Kontextová bezpečnost

cisco

Problematika bezpečných přístupů do sítě

Network Admission Control



AUTHENTICATE

users and devices to the network

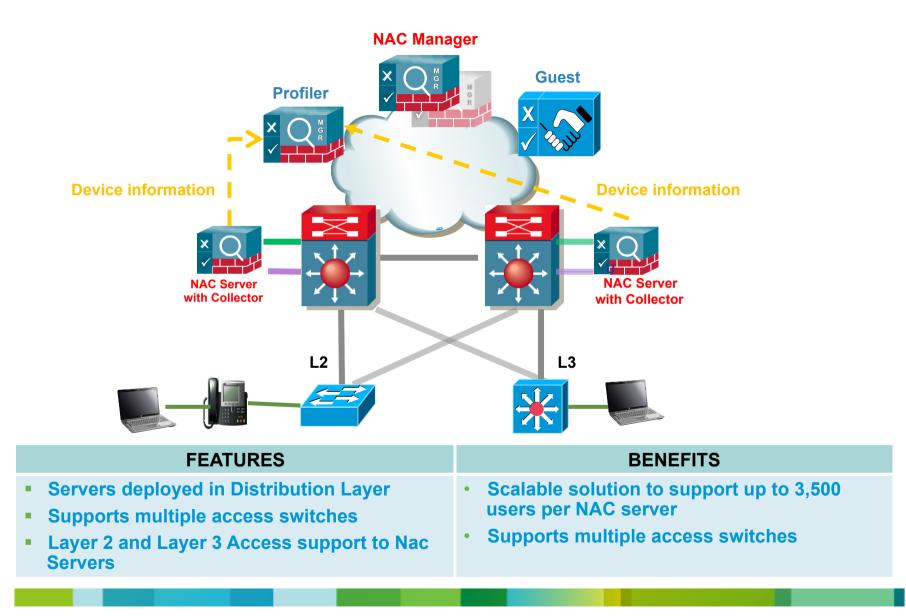


Differentiated Access role based access control

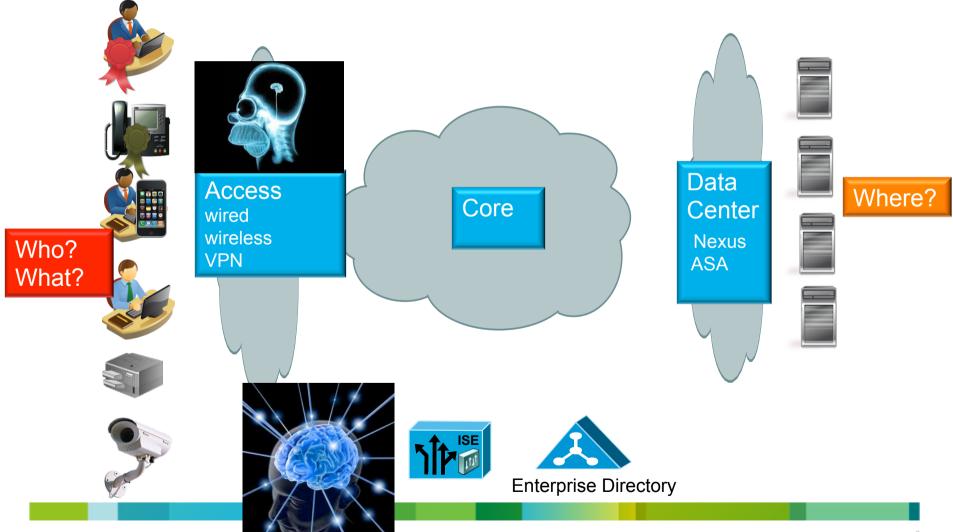


Audit and Report who is on my network

a) NAC – Centralized Deployment

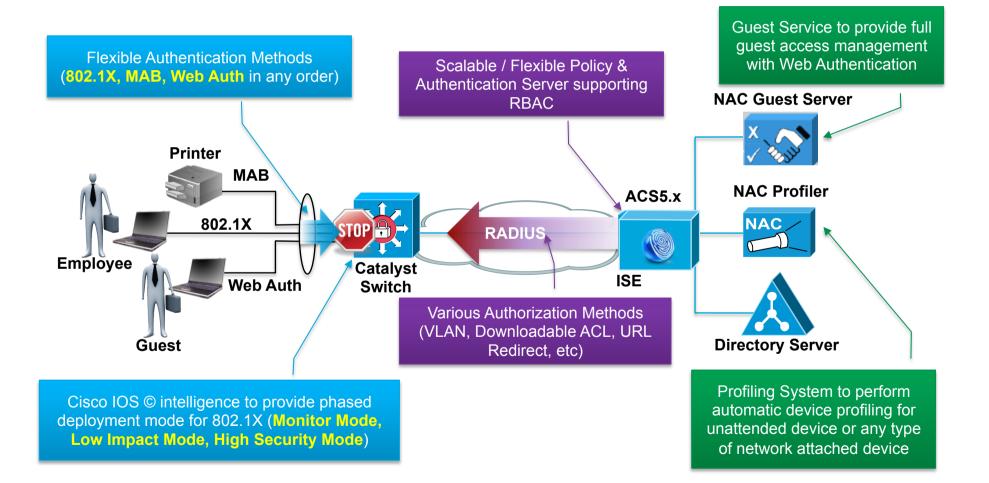


b) Adding Intelligence to the Network



2011 Cisco and/or its affiliates. All rights reserved.

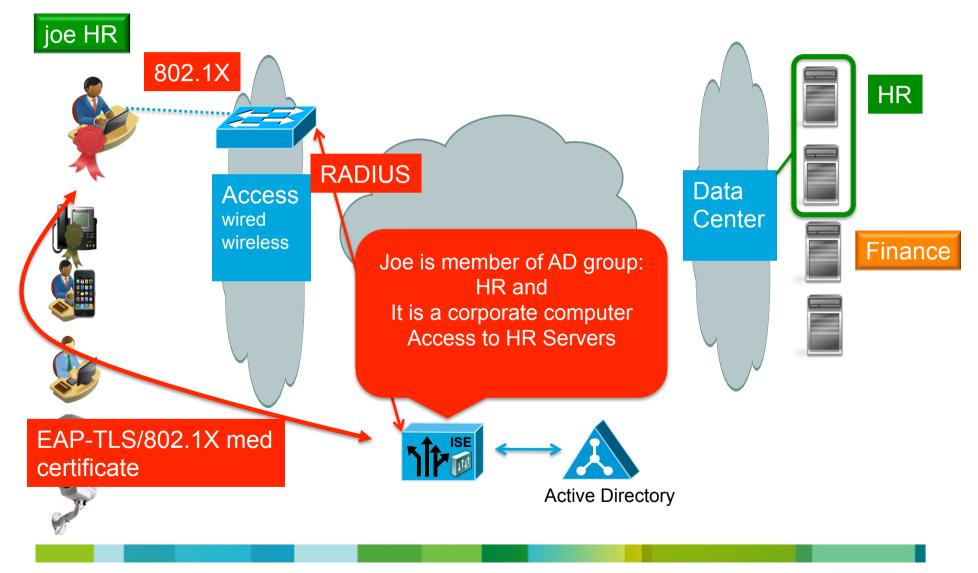
Identity Solution Specifics



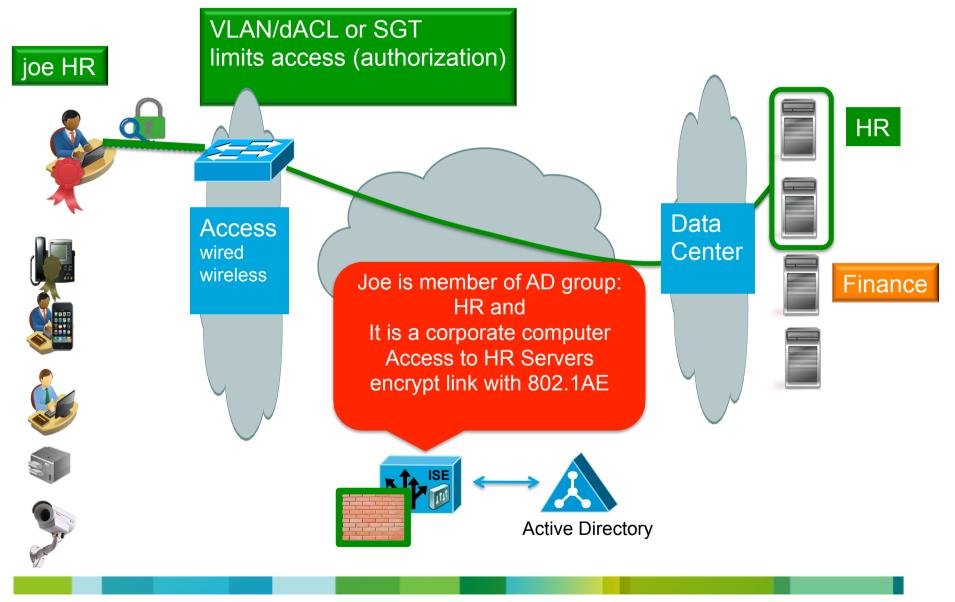
cisco

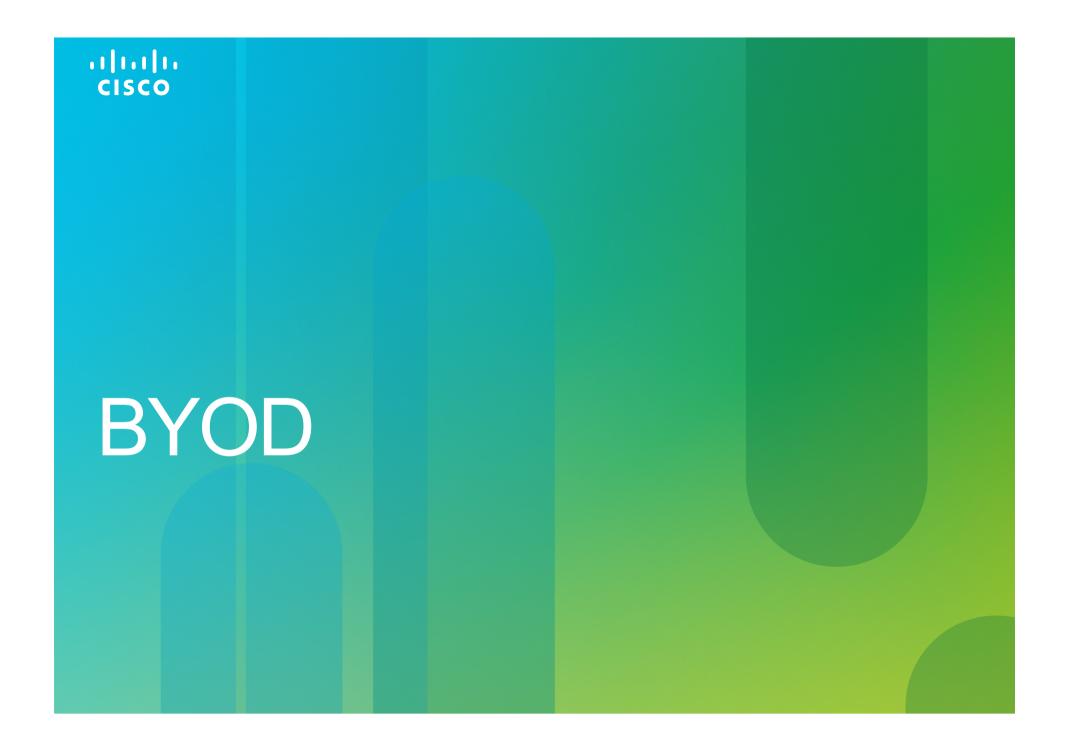
Základní řízení přístupu podle identity

Mapping user's group to security role



Mapping user's group to security role

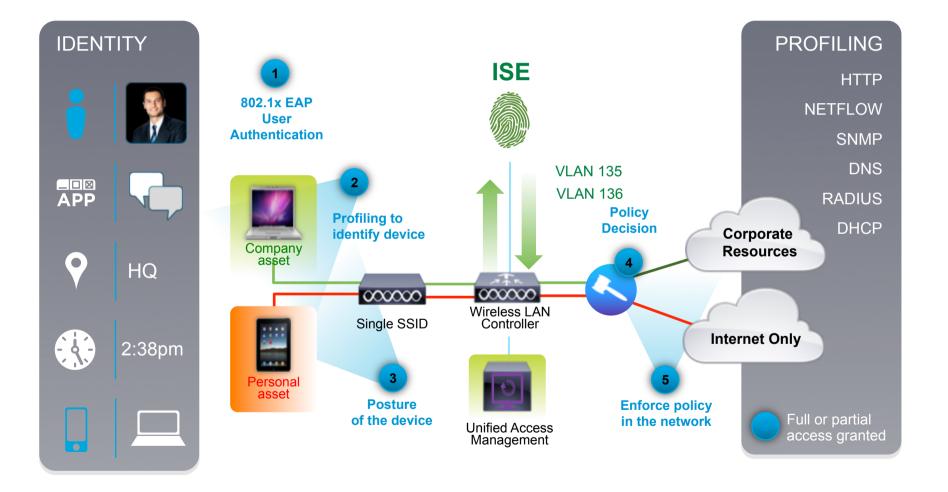




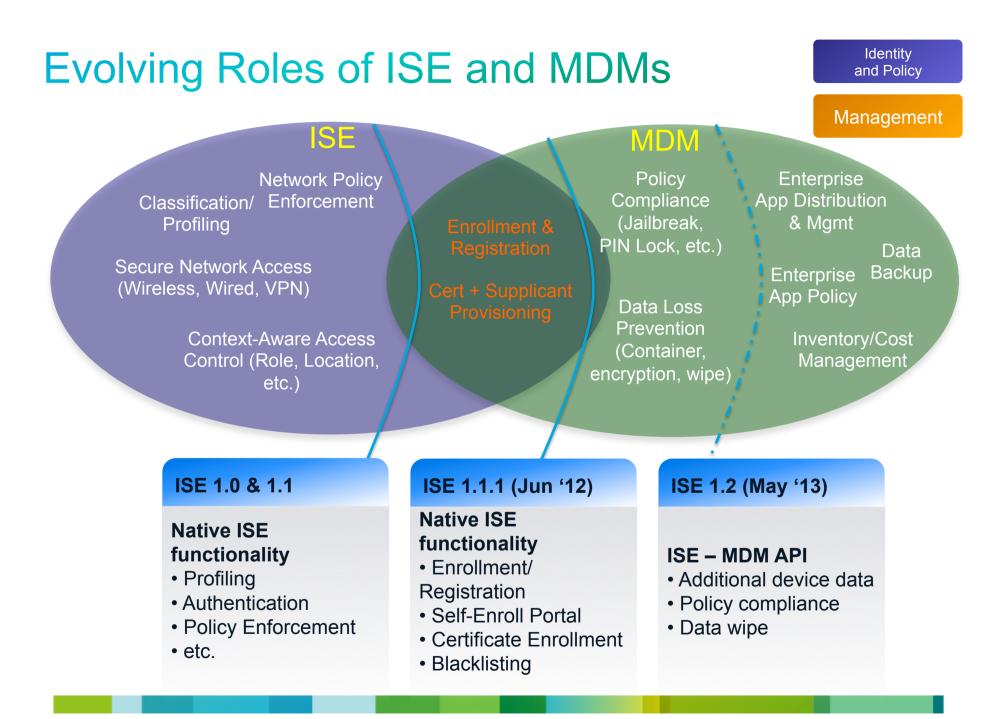
Identity and Policy

Example of BYOD Enforcing Different Policies for Corporate and Personal Devices

Unified Infrastructure



Identity **ISE: Powerful, Flexible Solution** and Policy Unified No other solution brings all the context together Infrastructure **Device Type** Location Authorization Policy At A Glance Custom User Posture **Access Method** Time First Matched Rule Applies Standard Status Rule Name Identity Groups Other Conditions Permissions Enabled Profiled Cisco IP Phones Cisco-IP-Phone Cisco IP Phones Enabled Game Console Game Console Game Console-Registered demo.local:ExternalGWups EQUALS demo.local/Users/Domain Enabled Computers AND San Jose Al Domain Computer CERTIFICATE:Subject Alternative Name AD Login Anv MATCHES .*(demo.local)\$ / Radius:User-Name MATCHES ^(host/).* Enabled Employee-Wired Any Employee Wired AND Postume Compliant Employee Employee_Wireless AND Posture Compliant AN LDAP1:badPwdCour Enabled Workstation Employee Wireless Employee-Wireless MATCHES [0-5] Enabled Employee Wireless ANE Posture_Compliant ANE North_America Employee-iPAD Apple-iPad Employee iPAD Android OR AppleiPad OR Apple-Enabled Contractor-iPAD Contrator Wireless AND Posture_Compliant AND North_America Contractor iPAD iPhone OR AppleiPod OR BlackBerry Business Hours AND DEVICE:Device Type EQUALS All Device Enabled Guest Guest-Wired Guest Types#Wired AND Posture Compliant Business Hours AND DEVICE: Device Type EQUALS All Device Enabled Guest-Wireless Guest Wireless Guest Types#Wireless AND Posture Compliant Disabled Default-Posture Anv CWA_Posture_Remediation Enabled Default Central_Web_Auth Any



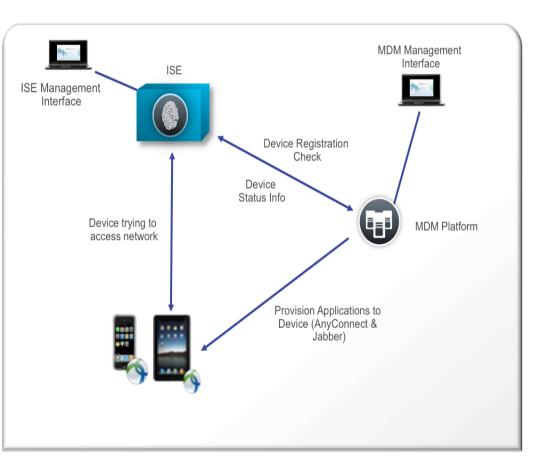
ISE 1.2 & MDM Integration - Scope

High Level Goals of Integration

- On-prem MDM Device Registration
 - Non registered clients redirected to MDM registration page
- Restricted Access
 - Non compliant clients will be given restricted access based on MDM posture state
- Augment Endpoint Data
 - Update data from endpoint which cannot be gathered by profiling
- Ability to Initiate Device Action from ISE
 - Device stolen -> need to wipe data on client









Attributes from MDM

- With the API, we can query on: General Compliant or ! Compliant (Macro level) -or-
 - Disk encryption is one
 - Pin lock
 - Jail broken
- Bulk re-check against the MDM every 4 hours.
 - But we are not using the cached data in the AuthZ
 - If result of Bulk Re-check shows that a device is no longer compliant – we will send a CoA to terminate session.
 - Works same with all 4 vendors.

	Q
∉ • ≣ •	∰ .
DeviceRegisterStatus	
DeviceCompliantStatus	
DiskEncryptionStatus	
PinLockStatus	
JailBrokenStatus	
Manufacturer	
Model	
L IMEI	
SerialNumber	
OsVersion	
PhoneNumber	

MDM Integration

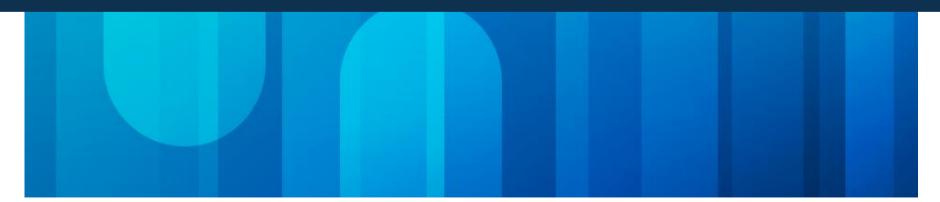
 Ability for administrator and user in ISE to issue remote actions on the device through the MDM server (eg: remote wiping the device)

MyDevices Portal	Endpoints	
Endpoints Directory in ISE	✓ Edit ♣Add X Delete ♣Impor	t 👻 🕞 Export 👻 🎼 MDM Actions 👻
	Endpoint Profile Android Android Android Android	▲ MAC Full Wipe F4:6 Corporate Wipe PIN Lock 00:23:76:95:86:93
CISCO My Devices Portal	Android Welcome employee1@ise.local (<u>Sign Out</u>)	00:18:A4:06:71:4E
Add a New Device To add a device, enter the Device ID a	and description and click Submit.	EditReinstate
Edit Reinstate Lost? Delete Full Wipe Corporate Wipe PIN Lock Select Device ID Description O CC:CC:12:34:15:CC	State	 Lost? Delete Full Wipe Corporate Wipe PIN Lock
		Cisco Public 17



Provisioning

Onboarding & Provisioning Demo



© 20isto iExpond/or its affiliates. All rights reserved.

© 2011 Cisco and/or its affiliates. All rights reserved.

ıılıılıı cısco

VPN Access

AnyConnect



© 2010 Cisco and/or its affiliates. All rights reserved.

Mobile Host Scan ("MDM Lite")

Additional access authorization capabilities based on endpoint Premium license requirement ASA 8.4.2+, 8.2.5+ Android 2.4.x, Apple iOS 2.5.x Desktop post 3.1

Description: Selection Criteria Define the AAA and endpoint at the logical expression text. User has ANY of the followin AAA Attribute Advanced	Add Endpoint Attribute Endpoint Attribute Type: AnyConnect Client Version: Version: Platform: Platform Version: Version: Platform Version: Version: Platform Version: Version: Version: Platform 4G Version Version	ACL Priority: 0 e AAA attribute criteria Advanced option to specify Add Edit Delete Logical Op. ③
Access/Authorization Policy Att Configure access/authorizati group-policy hierarchy. The are not specified in DAP). Action Network ACL Filter Action: O Continue		system and the archy attributes (those that AnyConnect

AnyConnect Attribute	DAP Attribute Name	DAP Attribute Type	DAP Logical Operations
Client Version	endpoint.anyconnect.clientversion	version	EQ, NE, GT, GE, LT, LE
Platform	endpoint.anyconnect.platform	string	EQ, NE
Platform Version	endpoint.anyconnect.platformversion	version	EQ, NE, GT, GE, LT, LE
Device Type	endpoint.anyconnect.devicetype	string	EQ, NE
Device UniqueID	endpoint.anyconnect.deviceuniqueid	caseless	EQ, NE

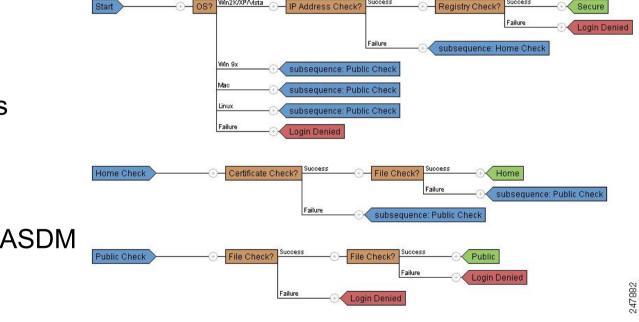
Hostscan

Yes, we can check health of client's PC

Identify the OS, antivirus, antispyware, and firewall software installed on the host - > coming from CSD, but it is not the replacement

Mn2K/XP/Msta

- ASA: prelogin policy that evaluates :
 - OS,
 - IP address,
 - registry entries,
 - Local certificates
 - filenames.
- Configurable from ASDM



ScanSafe & AnyConnect Integration

	I Manage filters	a filter 📪 Create a filter
	Filter nar	me: Denied 💌
Select the categories to be	included in the filter "Deni	ied"
Inbound Filters Alcohol Art / Museums Categories Banking Domains/URLs Content Types		Anonymous Auctions / C Building / Re Chat Chat Computer G Doi: 10.100 Computer C
3.0.0403 Secure Mobility Client VPN: VPN Service is available. SJC-FT Connect	Web Images Videos M Google Everything Videos News Images	aps News Shopping Gmail more ▼ beer About 117,000,000 results (0.18 seconds) Brands for beer: Bud Light Budweiser Heineken Corona Sam Adams Seer is the world's most widely consumed and probably the oldest of alcoholic beverages; it the third most popular drink overall, after water and tea en.wikipedia.org/wiki/Beer - Cached - Similar
Network: Connected (172.16.83.128) Wired Disable Wi-Fi	♥ Maps➡ Blogs▼ More	GermanyBeer and breweries by regionBelgiumIndiaCzech RepublicKenyaBeer styleMorocco
Web Security: Enabled (Germany) Advanced	Any time Latest Past month	More results from wikipedia.org » SeerAdvocate - Respect Beer. Beer community dedicated to supporting and promoting beer through education and appreciation. Learn more about craft beer, find a brewpub, brewery, bar,
Search Desktop 🖉 🖓 🖉 🖉 4:50 PM	All results Related searches Wonder wheel Timeline More search tools	 beeradvocate.com/ - Cached - Similar Realbeer.com: What Part Of Beer Don't You Understand? 2 Everything you could ever want to know about beer, brewpubs, microbreweries, homebrewir and the beer industry. We have over 150000 pages about beer, www.realbeer.com/ - Cached - Similar Samuel Adams® - Take Pride In Your Beer 2
Cisco Expo © 2011 Ci	Something different	With over 30 styles of beer, Samuel Adams® has been brewing quality beer since 1984 and

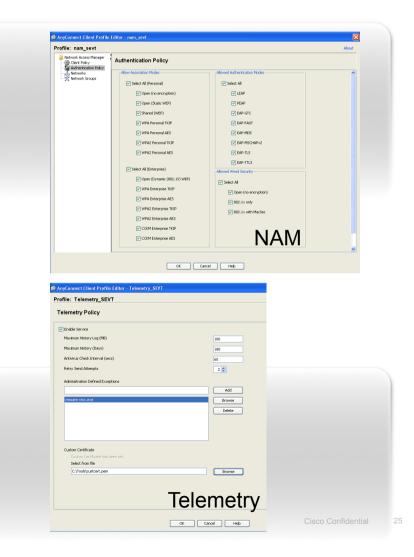
ng quality With over 50 styles of beer, ball

AnyConnect 3.0 Deployment – Profile Editors

Profile Editors integrated in ASDM 6.4

Profile: MUS_Profile	
Preferences (Part 1)	
Bobus Dress Genfrice hadrog Genfrice hadrog Genfrice hadrog Genfrice hadrog Genfrice hadrog Genfrice hadrog Sever List	V Lee Connelles V Lee Connelles Le Connelles Le Connelles Le Connelles Le Connelles Le Connelles
Windows VRV Establishment AllowRemoteUsers	V Lizer Controllable

Series Advanced Series Series	Web Security	Scanning Pro:	ху					
Image: Arrive and the second secon	- 🞯 Preferences - 🏰 Authentication	Scanning Proxy list i	s currently up-to-date.					
Image 00054130 000 443 Disky Image Image 00054130 000 443 Disky Image Image Image 00054130 000 443 Disky Image Image<	-	Scanning Proxy	Host Name		SSL Port	Display/Hide		Display
Trafic Liter Ford							^	
Demain 103541516 000 443 004/ Verte Coart 2232417 000 443 004/ Verte Coart 2232417 000 443 004/ Verte Coart 20232417 000 443 004/ Verte Coart 100 443 004/ Verte Coart 10								Hide
Id Wer Code 1/2/17/41/19 1/0000 143 1/04/97 Id Merice Code 1/2/17/16/22 1/0000 143 1/04/97 Id Merice 1/1/16/02/2 1/0000 1/04/97 1/04/97 Id Merice 1/1/16/02/2 1/0000 1/04/97 1/04/97 Id Merice 1/1/16/02/2 1/0000 1/04/97 1/04/97 Id Merice 1/1/16/02/2 1/04/97 1/04/97 1/04/97 Id Merice 1/1/16/97 1/1/16/97 1/1/16/97 1/1/16/97 Id Merice								Circles 41
bistar coat: 00.254.129 0000 443 0049 00 bistar 2000 443 000 443 0049 00 bistar 2000 443 000 443 0049 00 bistar 2000 00 bi								Usplay Al
It is Noted by the second seco								
Veb Security								
Visit and the second se								
Web Web Security		US South	72.37.249.43	anan	443	Display	×	
		Traffic Listen Port		×	We Se	eb curit	y	



NG Encryption with ASA 9.0

- AES-GCM/GMAC support (128-, 192-, and 256-bit keys) IKEv2 payload encryption and authentication ESP packet encryption and authentication
- SHA-2 (Phase 3a) support (256-, 384-, and 512-bit hashes)
 ESP packet authentication
- ECDH support (groups 19, 20, and 21)
 IKEv2 key exchange
 IKEv2 PFS
- ECDSA support (256-, 384-, and 521-bit elliptic curves)
 - IKEv2 user authentication PKI certificate enrollment PKI certificate generation and verification



ıılıılı cısco

Identity Based Security @Infrastructure

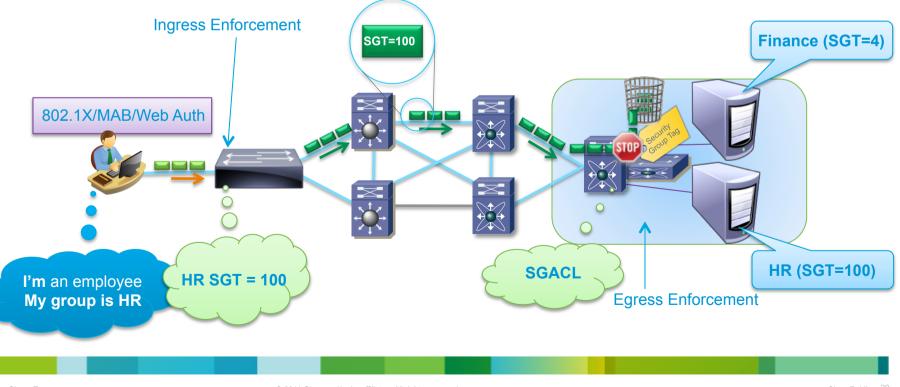
Identity Based Security on FW

	Enabled	Source	User	Destination	Service	Action
🥵 i	inside (5 inco	ming rules)				
1	1	🌍 any	ASATEST\\John_chambers	📑 block	🖙 http	😢 Deny
2	1	🌍 any	ASATEST\\John_chambers	🏟 any	🖙 http	🖌 Permit
3	1	🌍 any	🚨 none	🏟 any	<u>⊥</u> ₽> ip	🖌 Permit
4	1	🌍 any		🏟 any	<u>⊥</u> ₽> ip	😢 Deny
5	V	🏟 any	👃 LOCAL (mvassigh	FreeMailer	<u>tœ</u> ≻ smtp	🖌 Permit
🦻 i	inside IPv6 (1	l implicit incoming rule)		[Farran ell		
1		🏈 any		A A GMX ure ne	<u>IP</u> ip	🖌 Permit

Security Group Based Access Control

• SGA allows customers:

- Provides topology independent policy
- Flexible and scalable policy based on user role
- Centralized Policy Management for Dynamic policy provisioning
- Egress filtering results to reduce TCAM impact



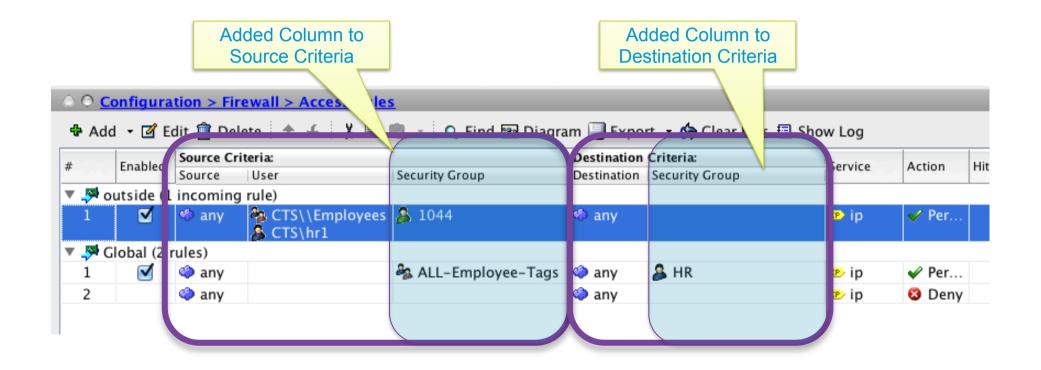
Secure Group Access

Topology Independent Access Control

- Term describing use of:
 - Secure Group TAG (SGT's)
 - Secure Group ACL's (SGACL's)
 - When a user log's in they are assigned a TAG (SGT) that identifies their role
 - The TAG is carried throughout the Network
- Server Switch applies SGACL's based on a "Matrix" (see below).

SGT	Public	Private
Staff	Permit	Permit
Guest	Permit	Deny

Using the SGT's in the FW Policy





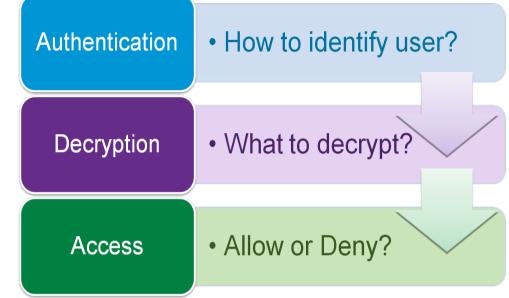
Next Generation Firewall



© 2010 Cisco and/or its affiliates. All rights reserved.

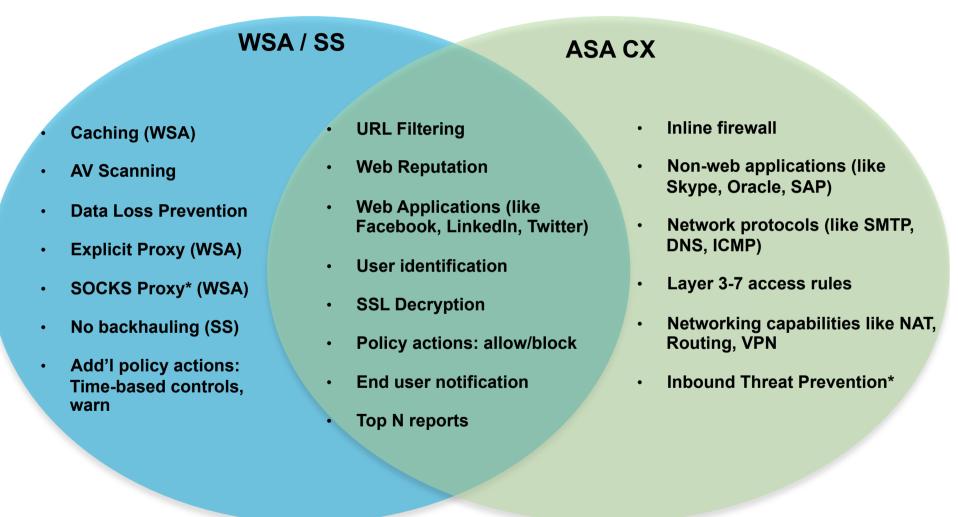
ASA-CX

- Context-Aware Firewall
- Active/Passive Authentication
- Application Visibility and Control
- Reputation Filtering
- URL Filtering
- SSL Decryption
- Secure Mobility
- Reports





ASA CX & WSA/SS: Feature Overlap & Differences



ASA-CX Demo





TechWiseTV 115: Firewall Reinvention with the New ASA CX

http://www.youtube.com/watch?v=JG12_pidHr8



Cisco ASA CX Context-Aware - Video Data Sheet

http://www.youtube.com/watch?v=rTAkEw41RB8

ıılıılı cısco