# Unified Access Control

Juniper™ NETWORKS

# Agenda

- Enterprise Trends
- Enterprise Pain Points
- Juniper's Unified Access Control Solution
  - Infranet Controller
  - Infranet Agent
  - Agentless Mode
  - Infranet Enforcers
- How UAC works
- Use Cases
- Juniper's Layer 2 Access Offerings
  - Odyssey Access Client
  - Steel-Belted Radius
- The next phase in access control

# Enterprise Trends

## Access Increases

Business critical network assets

Mobile devices transiting the LAN perimeter

Unmanaged or ill managed endpoints

Widely diverse users

## Secure & Resilient Network Experience Decreases

Explosive growth of vulnerabilities

Patch-to-outbreak time getting shorter

New breed of threats can come in with "permitted" users and traffic

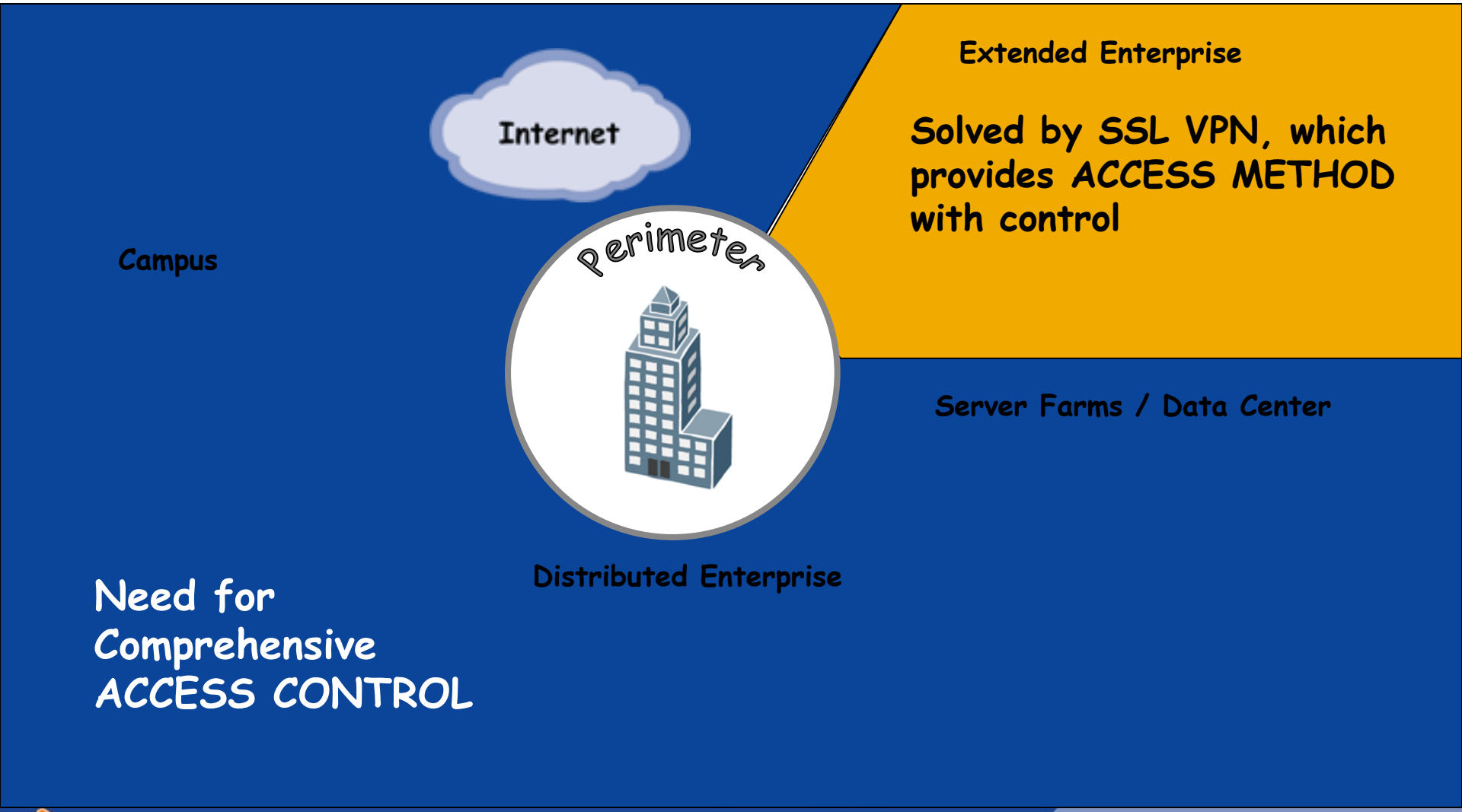
INCREASED THREAT VOLUME

FASTER OUTBREAKS

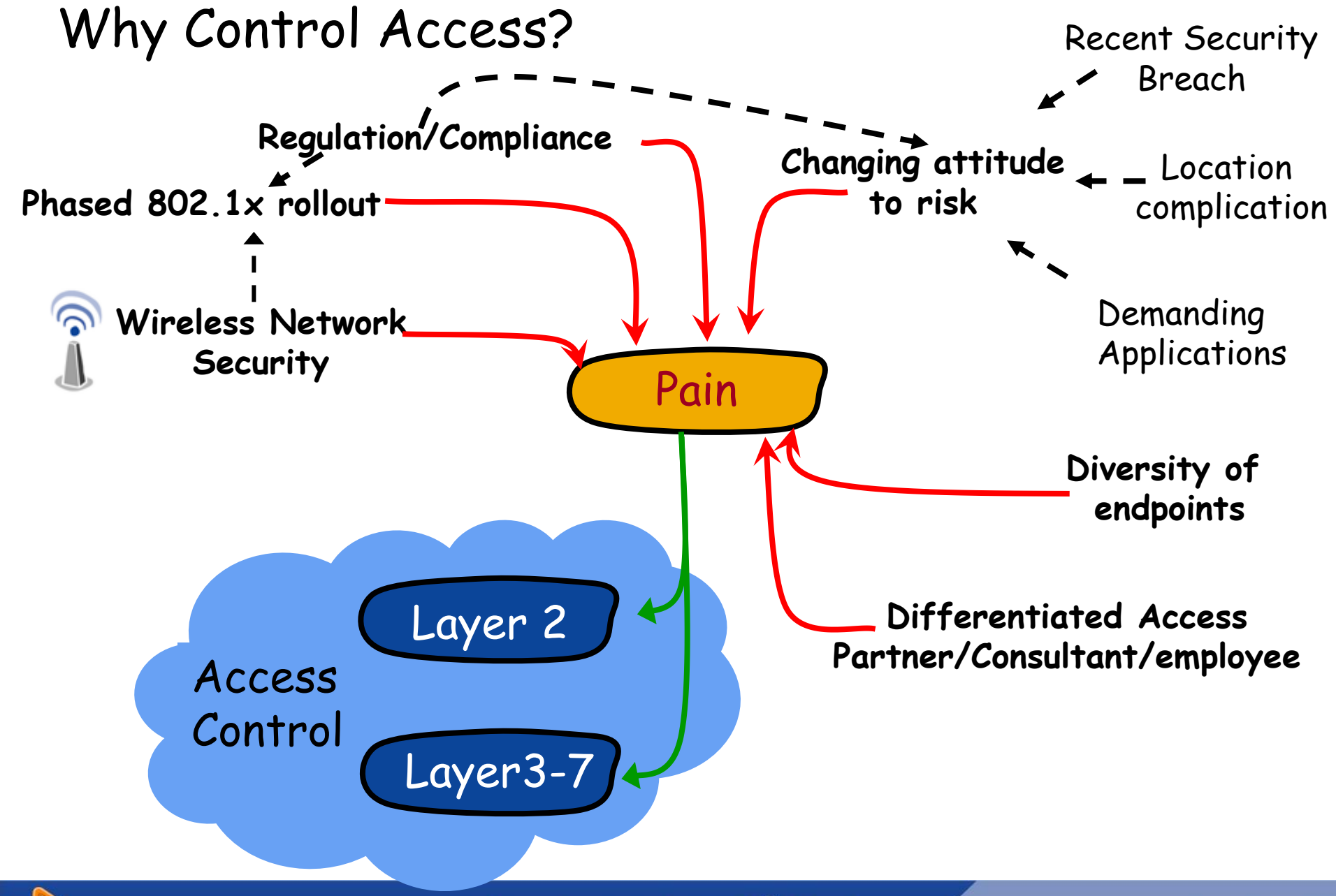
MORE TARGETS

# Enterprise Results

Skyrocketing security costs; loss of productivity with downtime



# Why Control Access?



# Why is this technology so important??

- Dynamic Network Boundaries – Location Complication
  - Mobile Workforce
  - Wireless Networks
  - Contractors
  - Partners
  - Diversity of endpoints

- Sophisticated Attacks
  - Zero-Day Exploits
  - Rapid Infection Speed
  - Targeted Attacks (crimeware)
  - Rootkits, Botnets, Zombies and Back Doors

- Harder to control/More demanding Applications
  - IM/VoIP/VoD
  - Unenforceable policy
- The Grey Network
  - The Network you don't know you own!
- The Usual Suspects
  - Bad People
    - More Money for Attackers
    - Extortion, Identity Theft, Bank Fraud, Corporate Espionage,…

  - Careless People
    - Accidental agents of catastrophe

# This market is exploding!!

But don't believe us…

**" Nearly 40% of all large enterprises are looking to implement a solution for LAN access control in the next 12-18 months"**

*Forrester Research*

**"Once companies finish building out security for the edge of the network, they will turn their attention inward, and NAC is the obvious place to invest."**

*Infonetics – Jan 2006 Enforcing Network Access Control: Market Outlook and Worldwide Forecast*

**"…we predict that, by 2007, 80 percent of enterprises will have implemented NAC (0.8 probability). This figure includes wireless and remote access virtual private network (VPN)-based NAC, as well as LAN-based NAC."**

*Gartner, Jan 2006 - Pitfalls Lurk Where IP Telephony Meets Network Access Control*

# Problems Facing Access Control Adoption

- Must tie user identity, device state and network info to access
  - Including managed, unmanaged, and unmanageable 3rd party devices
  - Enable granular access control
- Must enable true security, throughout the session
  - Must check security posture initially and throughout the session
  - Should use your choice of security apps
  - Should give users the opportunity to remediate
  - With encryption where you need it
- Need to enable security TODAY
  - Without rearchitecting my entire network
  - Without having to touch every single endpoint
  - In a phased manner
- Need it to "just work" – for the enterprise and the users
  - With cross platform endpoints
  - With field-tested components that you can trust

# The Solution:
## Unified Access Control

### Infranet Controller (IC)
- Access control decision point
- Automatically provisions Infranet Agent (if required)
- Dynamically provisions enforcement policy
- Integrated remediation support

**AAA Servers Identity Stores**

*Comprehensive enterprise integration*



*Unified policy enforcement based on identity, endpoint assessment, and network*

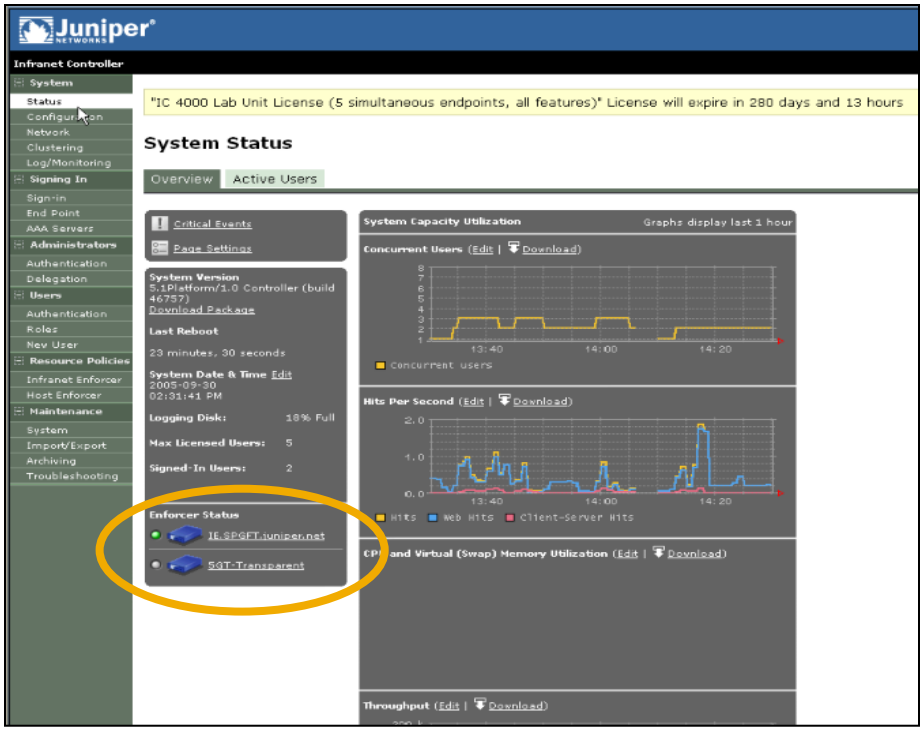
### Infranet Agent (IA)
- Host Checker (J.E.D.I)
- Host Enforcer (with firewall policy or optional dynamic MS IPSec enforcement)
- MS Windows Single SignOn
- Agentless enforcement for Windows, Mac and Linux
- IA protects authenticated endpoints from malicious/non-compliant endpoints

### Phase 1 Enforcers
- Enforcers – ScreenOS 5.4 capable
- NetScreen 5GT – NetScreen 5000
- From 90 Mbps to 30 Gbps

# Infranet Controller Overview


IC 4000

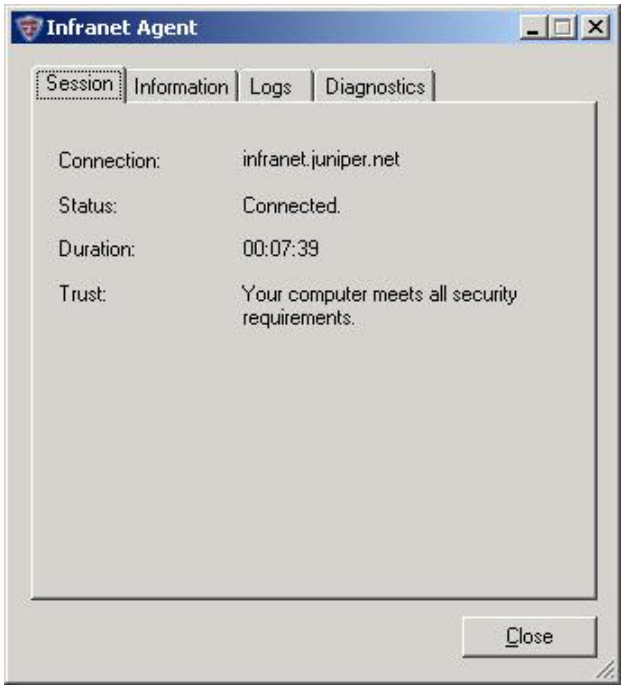
IC 6000




- Easy out-of-the-box deployment
- Centralized Policy Management
  - Endpoint, User, Access Policy configured in 1 box
  - Changes in policy dynamically propagated across network
  - Leverage existing AAA/identity stores for policy management
- Reliable Operation
  - Delegated Administration
  - High Availability across LAN and WAN
- Cross Platform support with two types of delivery
  - The Infranet Agent
  - Agentless Mode
  - Both enable Host Checking for ongoing real-time checks of endpoint security state

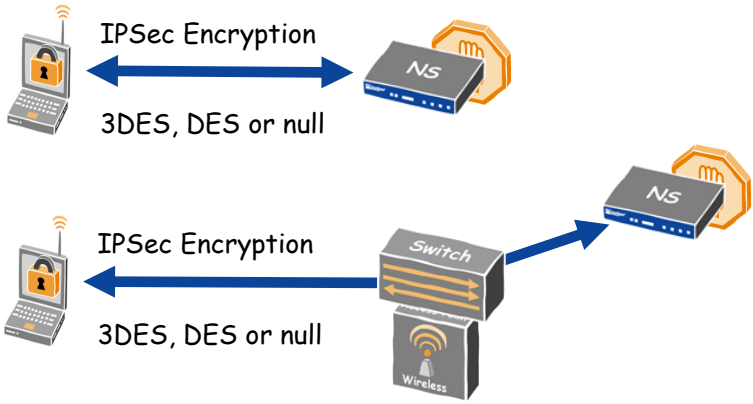
# Infranet Agent

- Lightweight client downloaded automatically to Windows endpoints
- Several easy installation options
  - Dynamic via ActiveX or Java
  - Juniper Installer Service
  - Pre-installed
- Provides:
  - Windows Single SignOn
  - Source IP based access, or
  - Authenticated Transport (IPSec)
  - Troubleshooting tools
  - Host Checker and Remediation
  - Host Enforcer (Endpoint firewall)

# Infranet Agent Benefits

- Windows Single Sign-On
  - Used with Active Directory or Windows NT Domain authentication on IC
  - Agent will use Windows credentials to automatically sign into the IC
  - Eliminates user intervention when signing into the Infranet
- IPSec Transport
  - Leverages the Microsoft Windows native capability
  - Detects and disables (not uninstalls) IPSec client if another is installed
- Provides authenticated and potentially encrypted transport
  - DES/3DES
  - Null encryption



# Infranet Agentless

- Web based clientless access
- Provides:
  - Access from machine without admin privileges
  - Agentless access
  - Cross-platform support
    - Mac
    - Linux
    - Windows
  - Source IP based access onto network
    - Enough for many networks
  - Host Checking and Remediation
  - Replacement / enhancement to complex departmental firewall deployment and management
- All browsers/platforms with JavaScript support

# Phase One Infranet Enforcers

NetScreen 25 & 50

NetScreen 500

HSC

NetScreen 5 Series

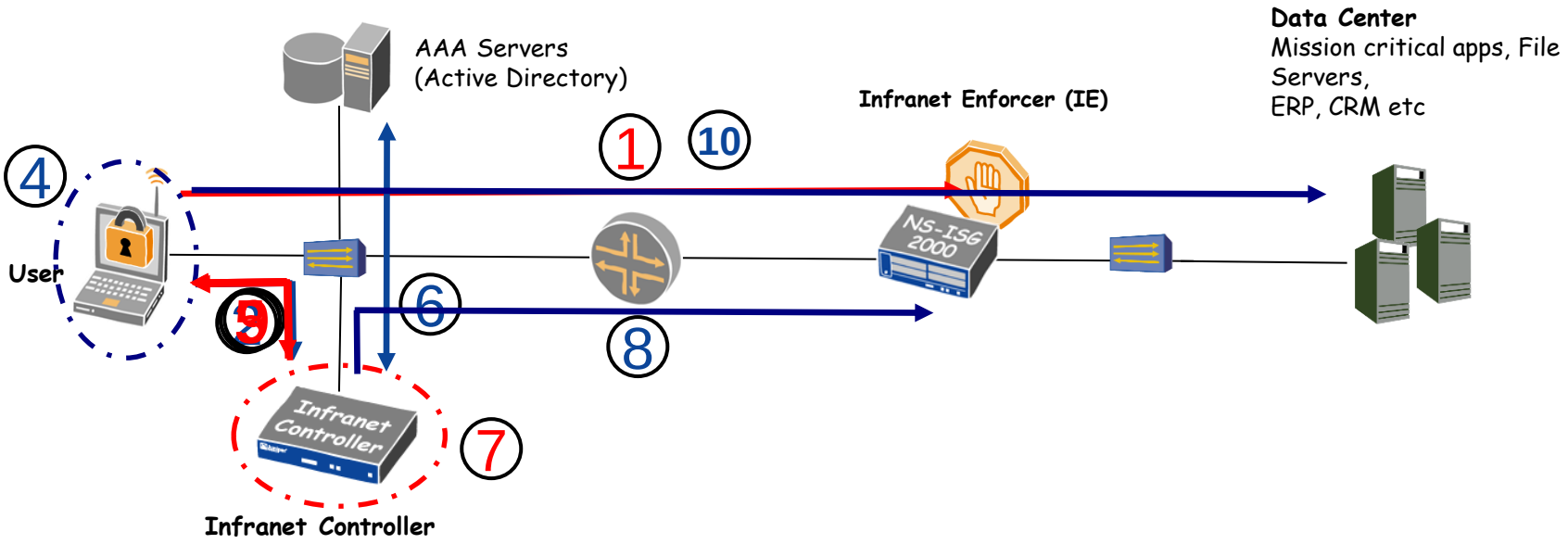
ISG Series

NetScreen 5200 & 5400

NetScreen 204 & 208

- Phase 1 incorporates Juniper FW/VPN platforms
- Screen OS 5.3 Software upgrade required
- 75Mbps to 30Gbps for wire speed policy enforcement in LAN
- Network security policy enforcement
  - DOS Protection
  - Deep Packet Inspection
  - Anti Virus Capabilities
  - Content Management

# How it works... User connection (Agent)




1. User tries to access resource - user is unable to get to resource. Traffic is blocked by the Infranet Enforcer].
2. User is redirected to the Infranet Controller or to a remediation site.
3. Infranet Controller deploys Infranet Agent to the endpoint over SSL.
4. Infranet Agent profiles the endpoint.
5. User authenticates to the Infranet Controller using the Infranet Agent.
6. Infranet Controller authenticates user against AAA servers. (AD, LDAP, etc.)
7. Infranet Controller determines users access policy.
8. Infranet Controller provisions user access on the Infranet Enforcer over SSL and SSH.
9. Infranet Controller provisions connection policies on the Infranet Agent over SSL.
10. User accesses the resource directly through the enforcer.

# Problem:

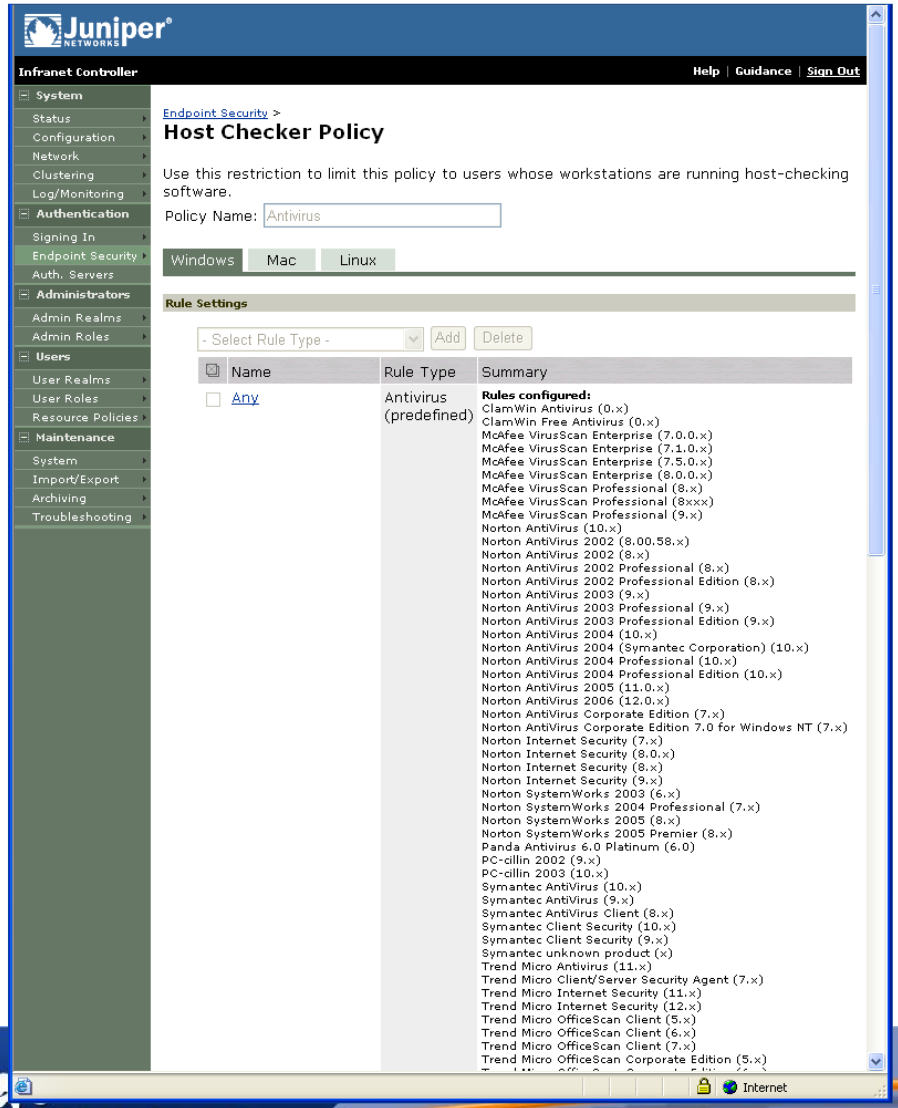
Need to tie user identity, device state and network info to access

- Juniper's Unified Access Control solution
  - Handles all use cases
    - Managed, unmanaged, and unmanageable devices
    - Employees, contractors, partners and guests
    - Agent or agentless mode available
  - Granular access control
    - Concept from Juniper's Secure Access SSL VPN engine
    - Combines data for dynamic access privileges
      - Network information
      - Endpoint security state
        - » Checked throughout session
      - AAA information
        - » Works with virtually all AAA schemes

# Problem:

## Must enable true security, throughout the session

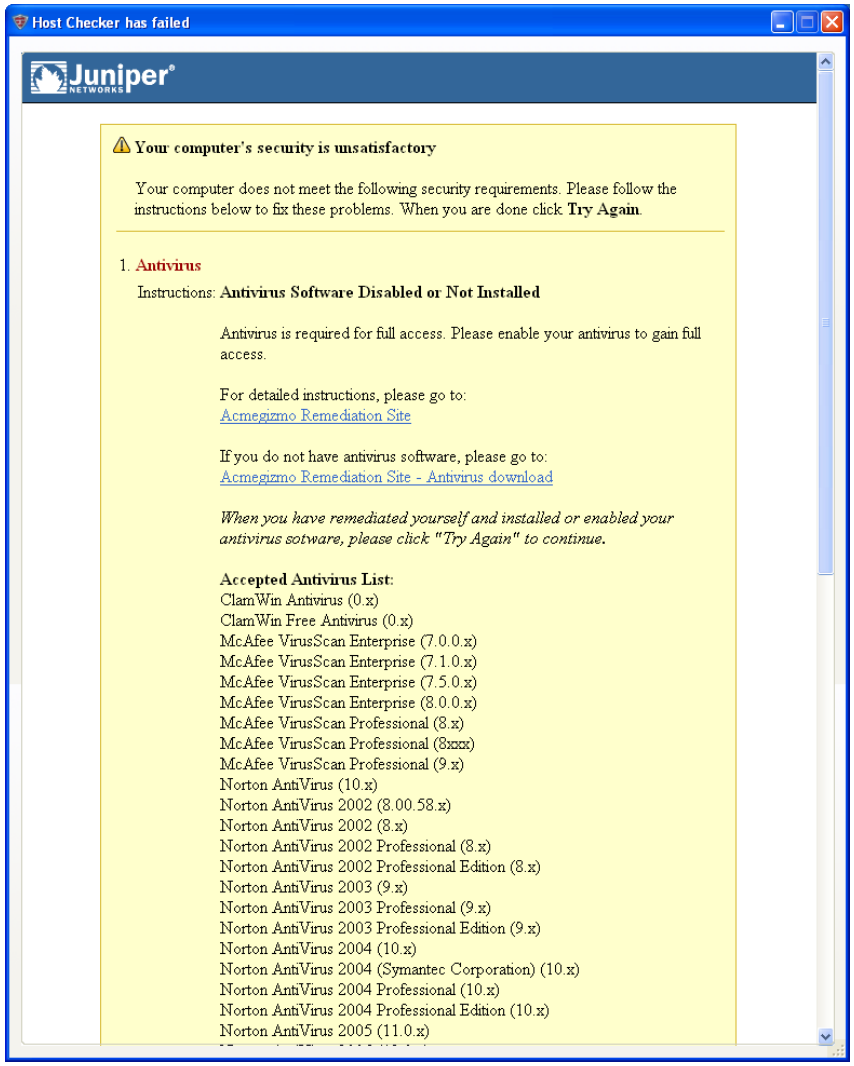
- Comprehensive endpoint Host Checks
  - Check the endpoint security state
  - Host Checks run in both agent and agentless modes
  - Works with your choice of security applications
  - Host Checks can run at admin configurable times throughout the session
- Predefined Host Checker for AV, FW, and Spyware
  - Pre-Defined Endpoint Assessment Checks simplify deployment
    - Query the application found, including Product type, Product version, Engine version, signatures, and last scan time.
    - Validate authenticity of app.
    - Tie remediation actions to specific Infranet Controller access policies



# Problem:

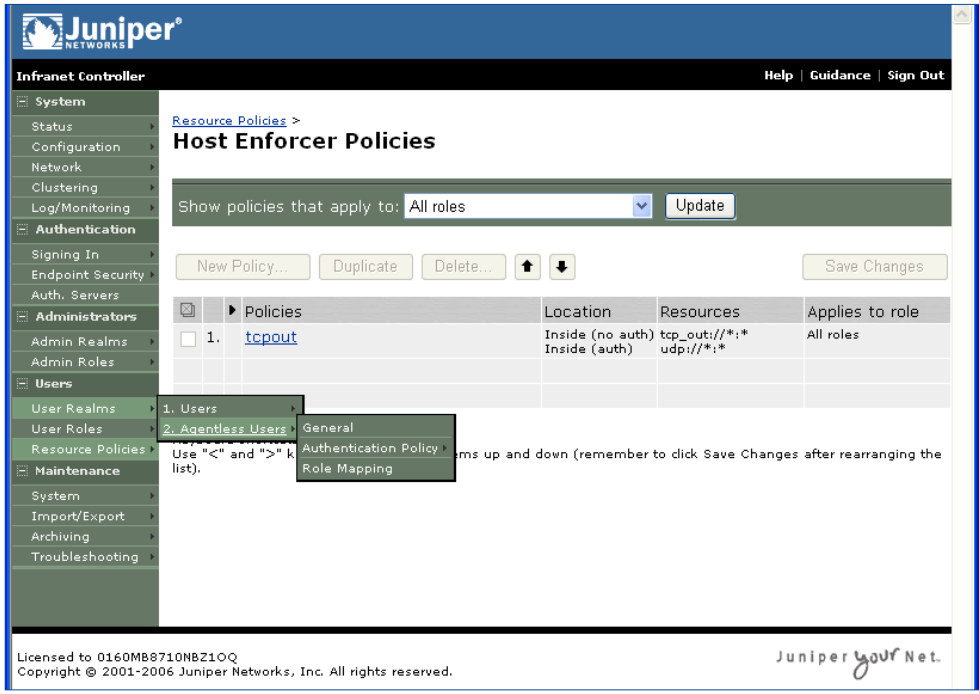
## Must enable true security, throughout the session

- Remediation site makes it easy for users to comply with policy
- Encryption to the desktop
- Automatic Monitoring of AV signature files
  - Virus signature version monitoring
    - Used in conjunction with pre-defined host checks
    - IC contacts Juniper download site at periodic intervals to obtain latest virus signature versions
    - IA checks currently installed version on PC against list to see if host check passes



# Problem:
## Need to enable security TODAY

- Unified Access Control solution
  - Enables phased deployment
    - Can protect the network at critical choke points today
    - Roll out enterprise-wide deployments or switch-based enforcement on your timeline
  - Leverage what you have
  - Can be easily dropped into your network with no changes
  - Dynamic agent download or agentless deployment
    - No pre-installation required



# Problem:

Need it to "just work" – for the enterprise and the users

- The solution is cross platform
  - Windows
  - Mac
  - Linux
- Captive Portal functionality on enforcers redirects new users automatically - the IC is transparent to the end user
- Agent software is dynamically downloaded if required
  - No pre-installation required
- Field Tested components
  - Controller policy engine from Juniper's #1 SSL VPN
  - Dynamic delivery also from Secure Access SSL VPN
  - Enforcers bring years of NetScreen experience

# Competitive Positioning

## You *KNOW* we don't like Cisco…so don't listen to us

Network Computing

Juniper's approach to the NNV conundrum can be summed up in two words: ***Simple and straightforward.***

Out of the box it took us ***less than 30 minutes*** to get the [Juniper] IE and IC up and running"

"Juniper's node-validation components are ***more comprehensive*** than the base Cisco NAC offerings."

"This simplicity is what allows Juniper Infranet to deliver ***a lot of functionality from the get-go***."

"A full Cisco NAC implementation is a ***complicated, intrusive process***"

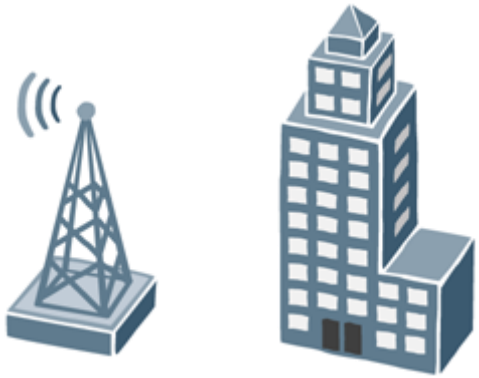
"For starters, Cisco has developed a gallon of alphabet soup's worth of ***new protocols*** to allow communication among devices…

…At the same time, ***protocols that haven't gone through IETF or IEEE*** standards processes tend to make IT people nervous"

"The alerting and troubleshooting interface in [Cisco's] Secure ACS is ***abysmal***…"

"The ACS user interface, however, is ***confusing***."

# UAC Use Cases



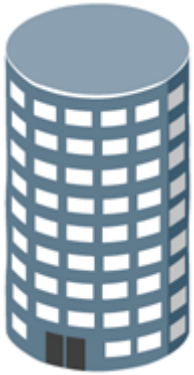
**Enterprise Wired & Wireless**

- Distributed Juniper firewall deployment (Branch office, DMZ, wireless)
- Flexible enforcement options
- Support for employees, partners, guests with agent/agentless modes
- Cross platform support (Windows, Mac and Linux)
- WAN/LAN clustering of policy servers
- Policy Specific Remediation for self administering platform
- Active Directory Integration

**Data Center**

- Deployed for dynamic access control to datacenter resources
- Part of enterprise wide zoning/firewalling strategy at a lot of enterprises
- Layer dynamic policy on a per user basis, by binding user, network and endpoint integrity information
- Ease of deployment key
- High Availability critical (Both Policy server and enforcement points)
- Firewalls in transparent mode for bump in the wire enforcement

# UAC Use Cases



**Finance**

- Flat network with no zoning
- Rollout of 802.1x planned over a 2-3 year period
- Segregated network for traders, partners, employees
- IPsec service for strong security (encrypting data/ authenticating endpoints)
- High Availability critical (DOS Protection etc)
- Distributed Architecture support
- Leverage existing investments (SEM, endpoint, switch/routing infrastructure)

**Retail**

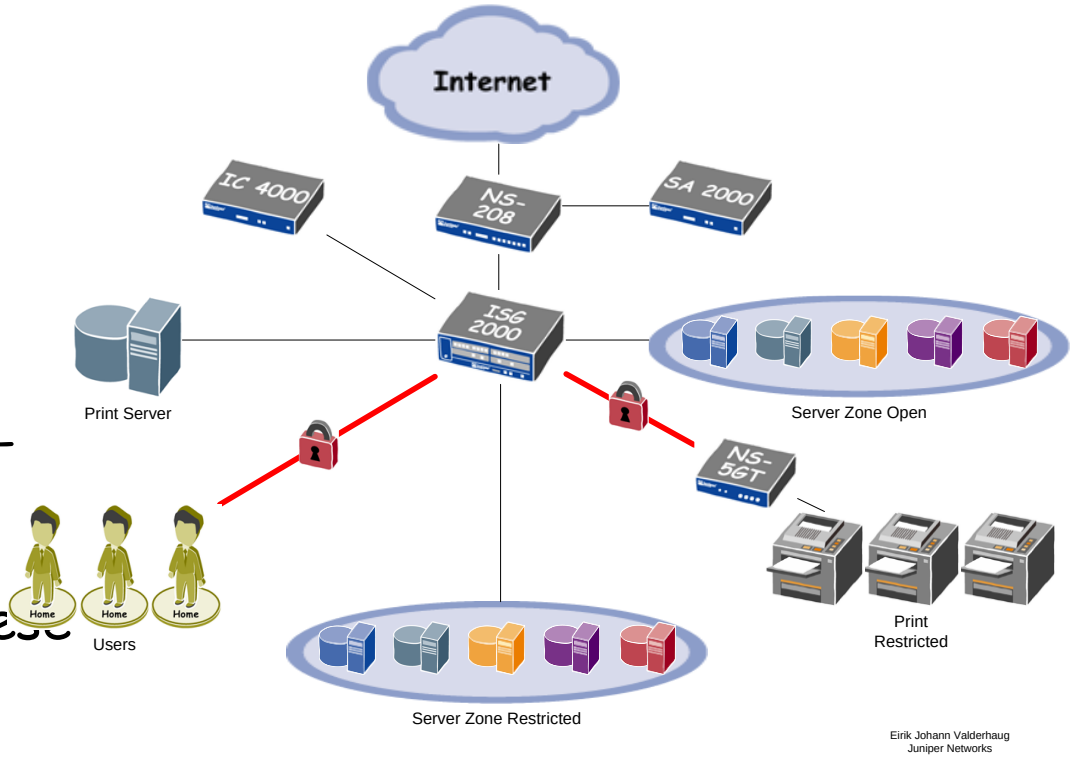
- Vendor access from unmanaged endpoints needs to be controlled
- Machines with admin rights/ guest privileges
- On demand delivery of agent preferred
- Dynamic access easily enforced in branch office firewalls
- Pre-populated list of endpoint security policies

**High Tech**

- Partners/guest access to network from conference rooms
- Mixed Hardware: Plenty of Mac, Linux, Solaris machines
- Regulatory Compliance requirements (Access to financials etc)
- Delegated administration for granular control over policy control
- Granular access control (HR, Accounting, finance, marketing, engg)
- Single Sign on preferable

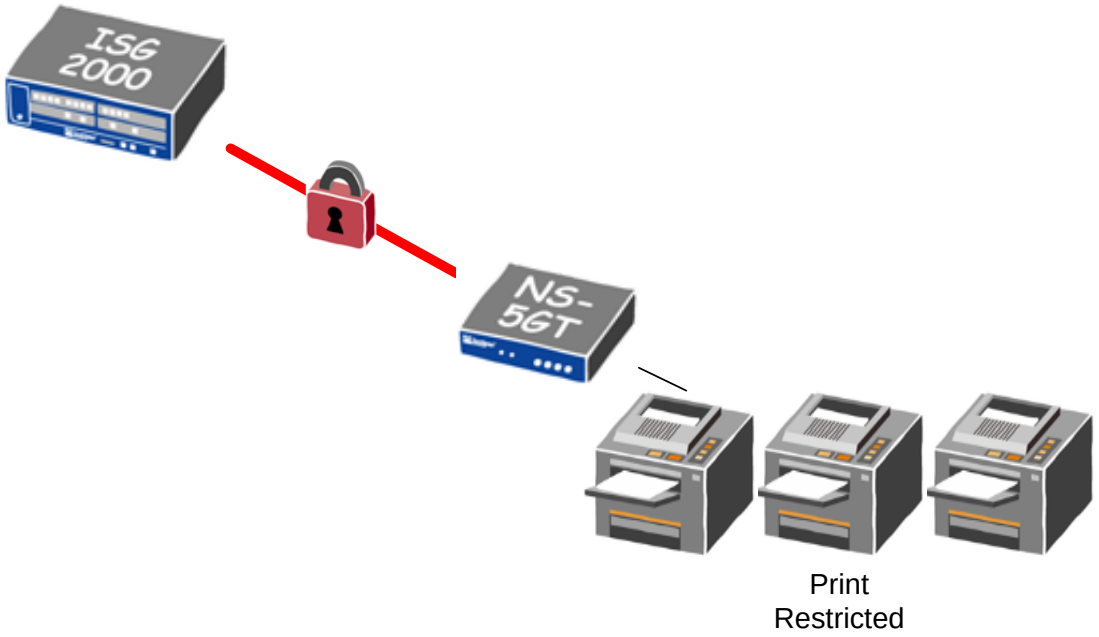
# EMEA Case Study

- Regional government
- Why they bought
  - Thin client computing to enforce access in a highly regulated environment
  - Significant proportion of endpoints unable to run thin-client due to technical constraints
  - UAC rolled out to secure these endpoints – led to additional secure printing application
  - No client install required
- What was sold
  - IC4000, ISG2000 and NS 5GT enforcement points



# EMEA Case Study

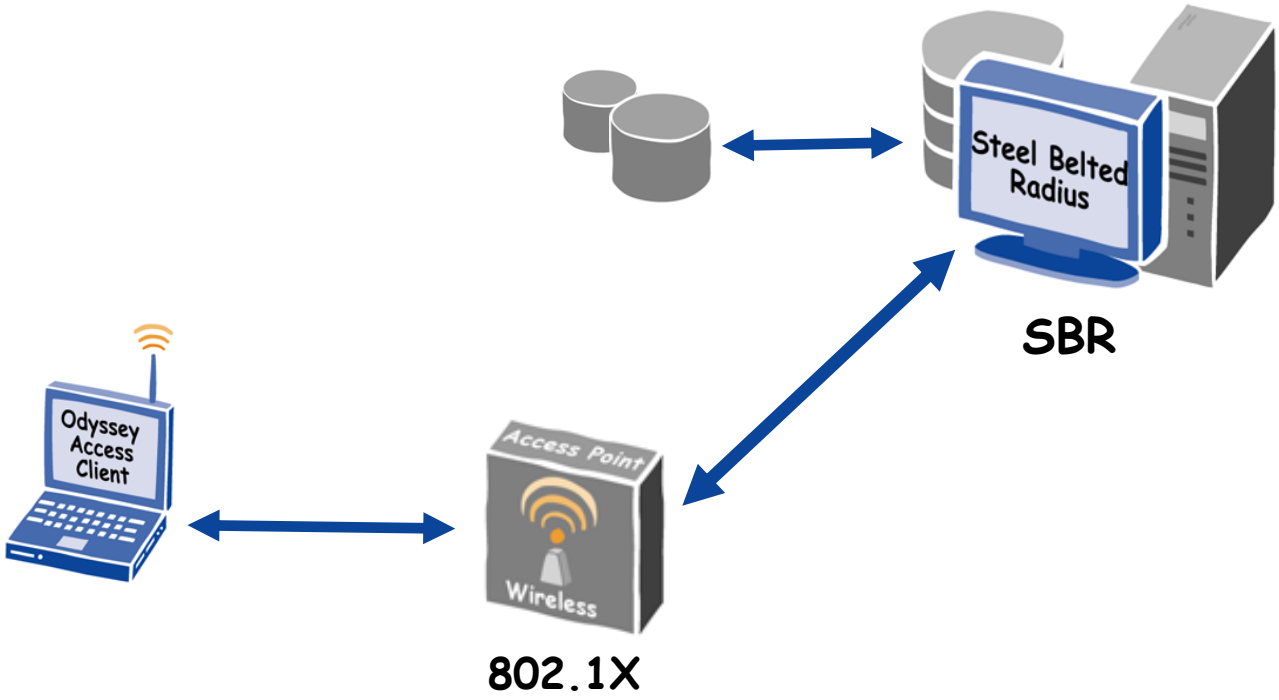
- Secure Printing
- Compliance concerns over print jobs traveling in the clear over the network
- Solution
  - Place a 5GT as an enforcement point in front of the print-farm
  - Infranet policy to encrypt traffic between client machine and enforcement point



# Consider UAC 1.x when

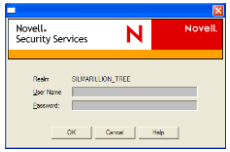
- You are interested in LAN access control with 802.1x, but
  - Haven't rolled your switching infrastructure
  - Need to secure a segment of your LAN immediately
- You are an existing Juniper firewall customer
  - Plenty of options to enforce policy in an overlay manner
- You are an existing SSL VPN customer who understands Juniper's policy control engine and
  - Has plenty of users with managed/unmanaged devices
  - Cares about plug n' play policy server that works with diverse AAA servers/ endpoint solutions

# Layer 2 Access Control Offerings
## Odyssey Access Client & Steel-Belted Radius



# Value Proposition for Odyssey (OAC)
## 802.1x Supplicant

- Ideal for large scale enterprise-wide deployments
  - Standardize on one security solution across organization
  - Uses a common tool to administer clients  across all platforms
  - Same client supports wired and wireless simultaneously
  - Supports a huge range of OS, platforms and device types
- Supports complex authentication schemes
- FIPS-compliant since Fall 2005
  - Compatible with DOD CAC card
- Current with all security standards
- Supports all major EAP methods

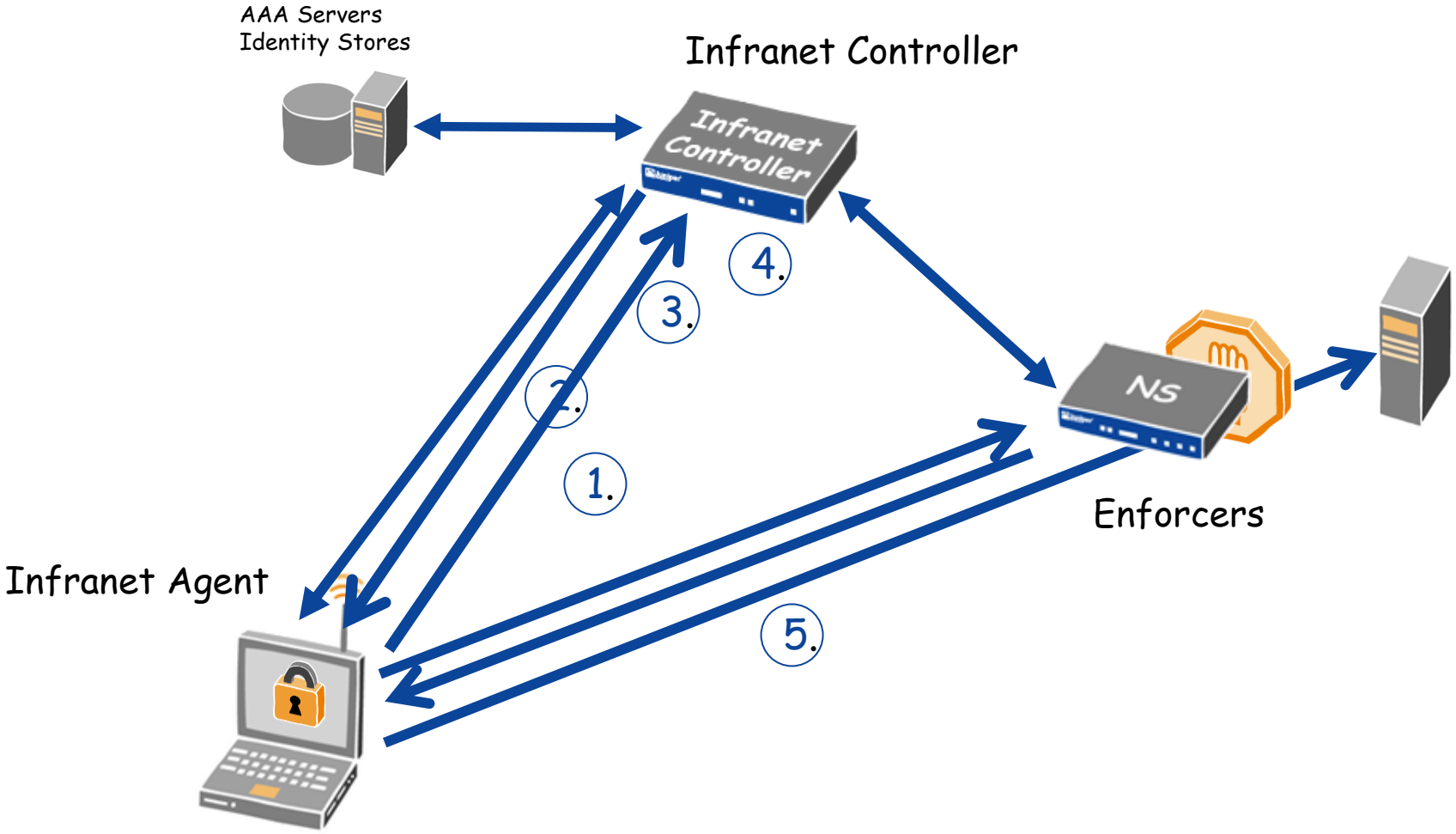




# Value Proposition for Steel Belted Radius

- Most flexible, reliable RADIUS server
- Performance – can handle more authentication transactions/second than Microsoft or Cisco
- All Steel Belted Radius servers fully support AAA functions
- Comprehensive feature set, designed for compatibility in heterogeneous environment
  - Multi-platform
  - Multi-vendor
- Broadest line of RADIUS servers for every network architecture:
  - Enterprise Edition (EE): Mid-Large Enterprises & Branch
  - Global Enterprise Edition (GEE): Fortune 500 and Gov't
  - Appliance – both EE & GEE available on hardened form factor for easy deployment

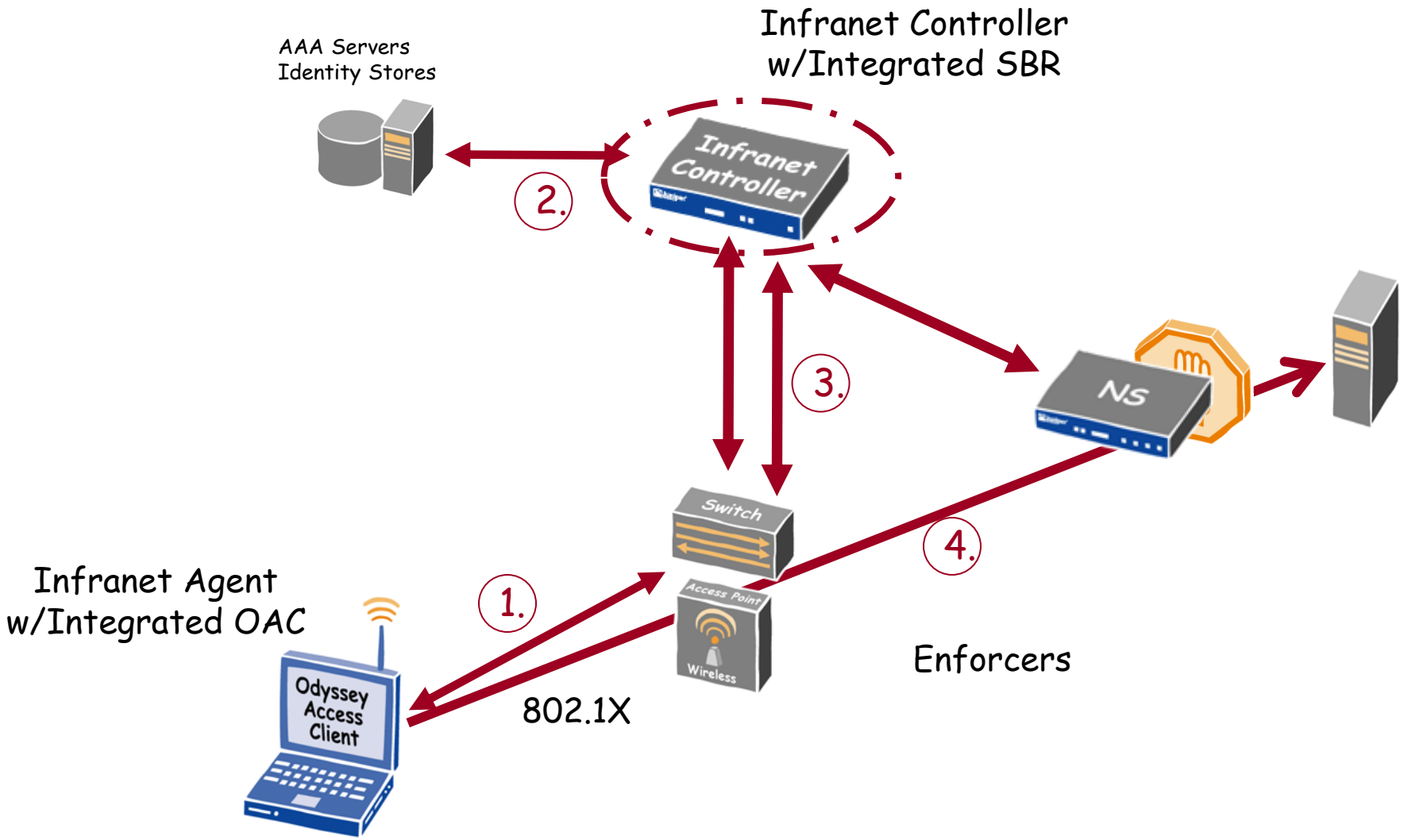
# UAC 1.X

## Review of how it works today

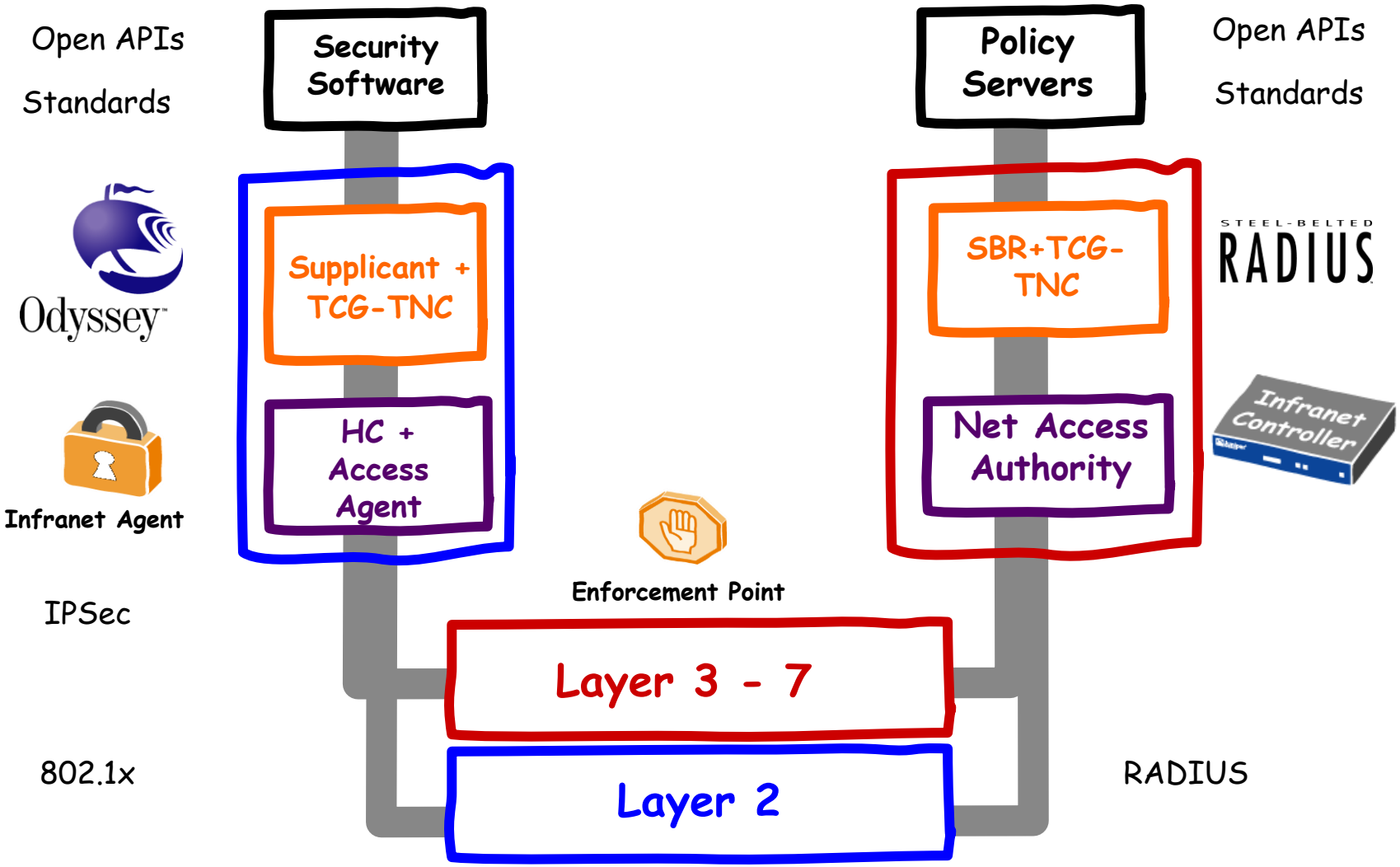


# UAC 2.0: Layer 2 + Layer 3

## The future of Unified Access Control



# UAC 2.0: Comprehensive Control



# Benefits of UAC with L2 Access Control

- Standards Based Solution
  - Support for enforcement on vendor agnostic switch infrastructure (TNC IF-PEP Compliant)
  - Support for TNC standards on endpoint vendor interoperability
- Comprehensive Security
  - Secure at edge, in the network or both
  - Protect network assets (L2-L7)
- Ease of Deployment
  - Flexible support for evolving networks
  - On demand agent and agentless modes for diverse user/endpoint scenarios (partners, guests, non 802.1x, Linux, Mac)

# Summary - Juniper's UAC Solution Delivers

- LAN Access Control today without requiring an 802.1x rollout
  - Granular secure access to your LAN for employees, contractors, partners with cross platform support
- Layer 3-7 Access control via dynamic IPSec VPN or Source-based IP policy
- A clear route to Layer 2 port based access control
- Leverage of your existing Juniper firewall investment
- Proven technology from the SSL VPN portfolio
- Support for users with managed/unmanaged devices
- A plug n' play policy server that works with diverse AAA servers/ endpoint solutions
- Security without compromising performance