



**Unified Access Control**

## **Deployment Scenarios Guide**

*Release 3.1*

**Juniper Networks, Inc.**  
1194 North Mathilda Avenue  
Sunnyvale, CA 94089  
USA  
408-745-2000  
**[www.juniper.net](http://www.juniper.net)**

This product includes the Envoy SNMP Engine, developed by Epilogue Technology, an Integrated Systems Company. Copyright © 1986–1997, Epilogue Technology Corporation. All rights reserved. This program and its documentation were developed at private expense, and no part of them is in the public domain.

This product includes memory allocation software developed by Mark Moraes, copyright © 1988, 1989, 1993, University of Toronto.

This product includes FreeBSD software developed by the University of California, Berkeley, and its contributors. All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite Releases is copyrighted by The Regents of the University of California. Copyright © 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994. The Regents of the University of California. All rights reserved.

GateD software copyright © 1995, The Regents of the University. All rights reserved. Gate Daemon was originated and developed through release 3.0 by Cornell University and its collaborators. Gated is based on Kirton's EGP, UC Berkeley's routing daemon (routed), and DCN's HELLO routing protocol. Development of Gated has been supported in part by the National Science Foundation. Portions of the GateD software copyright © 1988, Regents of the University of California. All rights reserved. Portions of the GateD software copyright © 1991, D. L. S. Associates.

Juniper Networks, the Juniper Networks logo, NetScreen, NetScreen Technologies, the NetScreen logo, NetScreen-Global Pro, ScreenOS, and GigaScreen are registered trademarks of Juniper Networks, Inc. in the United States and other countries.

The following are trademarks of Juniper Networks, Inc.: ERX, E-series, ESP, Instant Virtual Extranet, Internet Processor, J2300, J4300, J6300, J-Protect, J-series, J-Web, JUNOS, JUNOScope, JUNOScript, JUNOSe, M5, M7i, M10, M10i, M20, M40, M40e, M160, M320, M-series, MMD, NetScreen-5GT, NetScreen-5XP, NetScreen-5XT, NetScreen-25, NetScreen-50, NetScreen-204, NetScreen-208, NetScreen-500, NetScreen-5200, NetScreen-5400, NetScreen-IDP 10, NetScreen-IDP 100, NetScreen-IDP 500, NetScreen-Remote Security Client, NetScreen-Remote VPN Client, NetScreen-SA 1000 Series, NetScreen-SA 3000 Series, NetScreen-SA 5000 Series, NetScreen-SA Central Manager, NetScreen Secure Access, NetScreen-SM 3000, NetScreen-Security Manager, NMC-RX, SDX, Stateful Signature, T320, T640, T-series, and TX Matrix. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners. All specifications are subject to change without notice.

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.

Copyright © 2006–2009, Juniper Networks, Inc.  
All rights reserved. Printed in USA.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

#### Software License

The terms and conditions for using this software are described in the software license contained in the acknowledgment to your purchase order or, to the extent applicable, to any reseller agreement or end-user purchase agreement executed between you and Juniper Networks. By using this software, you indicate that you understand and agree to be bound by those terms and conditions.

Generally speaking, the software license restricts the manner in which you are permitted to use the software and may contain prohibitions against certain uses. The software license may state conditions under which the license is automatically terminated. You should consult the license for further details.

For complete product documentation, please see the Juniper Networks Web site at [www.juniper.net/techpubs](http://www.juniper.net/techpubs).

#### End User License Agreement

**READ THIS END USER LICENSE AGREEMENT ("AGREEMENT") BEFORE DOWNLOADING, INSTALLING, OR USING THE SOFTWARE.** BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE OR OTHERWISE EXPRESSING YOUR AGREEMENT TO THE TERMS CONTAINED HEREIN, YOU (AS CUSTOMER OR IF YOU ARE NOT THE CUSTOMER, AS A REPRESENTATIVE/AGENT AUTHORIZED TO BIND THE CUSTOMER) CONSENT TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT OR CANNOT AGREE TO THE TERMS CONTAINED HEREIN, THEN (A) DO NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND (B) YOU MAY CONTACT JUNIPER NETWORKS REGARDING LICENSE TERMS.

**1. The Parties.** The parties to this Agreement are Juniper Networks, Inc. and its subsidiaries (collectively "Juniper"), and the person or organization that originally purchased from Juniper or an authorized Juniper reseller the applicable license(s) for use of the Software ("Customer") (collectively, the "Parties").

**2. The Software.** In this Agreement, "Software" means the program modules and features of the Juniper or Juniper-supplied software, and updates and releases of such software, for which Customer has paid the applicable license or support fees to Juniper or an authorized Juniper reseller.

**3. License Grant.** Subject to payment of the applicable fees and the limitations and restrictions set forth herein, Juniper grants to Customer a non-exclusive and non-transferable license, without right to sublicense, to use the Software, in executable form only, subject to the following use restrictions:

- Customer shall use the Software solely as embedded in, and for execution on, Juniper equipment originally purchased by Customer from Juniper or an authorized Juniper reseller, unless the applicable Juniper documentation expressly permits installation on non-Juniper equipment.
- Customer shall use the Software on a single hardware chassis having a single processing unit, or as many chassis or processing units for which Customer has paid the applicable license fees.
- Product purchase documents, paper or electronic user documentation, and/or the particular licenses purchased by Customer may specify limits to Customer's use of the Software. Such limits may restrict use to a maximum number of seats, registered endpoints, concurrent users, sessions, calls, connections, subscribers, clusters, nodes, or transactions, or require the purchase of separate licenses to use particular features, functionalities, services, applications, operations, or capabilities, or provide throughput, performance, configuration, bandwidth, interface, processing, temporal, or geographical limits. Customer's use of the Software shall be subject to all such limitations and purchase of all applicable licenses.

The foregoing license is not transferable or assignable by Customer. No license is granted herein to any user who did not originally purchase the applicable license(s) for the Software from Juniper or an authorized Juniper reseller.

**4. Use Prohibitions.** Notwithstanding the foregoing, the license provided herein does not permit the Customer to, and Customer agrees not to and shall not: (a) modify, unbundle, reverse engineer, or create derivative works based on the Software; (b) make unauthorized copies of the Software (except as necessary for backup purposes); (c) rent, sell, transfer, or grant any rights in and to any copy of the Software, in any form, to any third party; (d) remove any proprietary notices, labels, or marks on or in any copy of the Software or any product in which the Software is embedded; (e) distribute any copy of the Software to any third party, including as may be embedded in Juniper equipment sold in the secondhand market; (f) use any "locked" or key-restricted feature, function, service, application, operation, or capability without first purchasing the applicable license(s) and obtaining a valid key from Juniper, even

if such feature, function, service, application, operation, or capability is enabled without a key; (g) distribute any key for the Software provided by Juniper to any third party; (h) use the Software in any manner that extends or is broader than the uses purchased by Customer from Juniper or an authorized Juniper reseller; (i) use the Software on non-Juniper equipment where the Juniper documentation does not expressly permit installation on non-Juniper equipment; (j) use the Software (or make it available for use) on Juniper equipment that the Customer did not originally purchase from Juniper or an authorized Juniper reseller; or (k) use the Software in any manner other than as expressly provided herein.

**5. Audit.** Customer shall maintain accurate records as necessary to verify compliance with this Agreement. Upon request by Juniper, Customer shall furnish such records to Juniper and certify its compliance with this Agreement.

**6. Confidentiality.** The Parties agree that aspects of the Software and associated documentation are the confidential property of Juniper. As such, Customer shall exercise all reasonable commercial efforts to maintain the Software and associated documentation in confidence, which at a minimum includes restricting access to the Software to Customer employees and contractors having a need to use the Software for Customer's internal business purposes.

**7. Ownership.** Juniper and Juniper's licensors, respectively, retain ownership of all right, title, and interest (including copyright) in and to the Software, associated documentation, and all copies of the Software. Nothing in this Agreement constitutes a transfer or conveyance of any right, title, or interest in the Software or associated documentation, or a sale of the Software, associated documentation, or copies of the Software.

**8. Warranty, Limitation of Liability, Disclaimer of Warranty.** The warranty applicable to the Software shall be as set forth in the warranty statement that accompanies the Software (the "Warranty Statement"). Nothing in this Agreement shall give rise to any obligation to support the Software. Support services may be purchased separately. Any such support shall be governed by a separate, written support services agreement. TO THE MAXIMUM EXTENT PERMITTED BY LAW, JUNIPER SHALL NOT BE LIABLE FOR ANY LOST PROFITS, LOSS OF DATA, OR COSTS OR PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR FOR ANY SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THIS AGREEMENT, THE SOFTWARE, OR ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. IN NO EVENT SHALL JUNIPER BE LIABLE FOR DAMAGES ARISING FROM UNAUTHORIZED OR IMPROPER USE OF ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. EXCEPT AS EXPRESSLY PROVIDED IN THE WARRANTY STATEMENT TO THE EXTENT PERMITTED BY LAW, JUNIPER DISCLAIMS ANY AND ALL WARRANTIES IN AND TO THE SOFTWARE (WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE), INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT DOES JUNIPER WARRANT THAT THE SOFTWARE, OR ANY EQUIPMENT OR NETWORK RUNNING THE SOFTWARE, WILL OPERATE WITHOUT ERROR OR INTERRUPTION, OR WILL BE FREE OF VULNERABILITY TO INTRUSION OR ATTACK. In no event shall Juniper's or its suppliers' or licensors' liability to Customer, whether in contract, tort (including negligence), breach of warranty, or otherwise, exceed the price paid by Customer for the Software that gave rise to the claim, or if the Software is embedded in another Juniper product, the price paid by Customer for such other product. Customer acknowledges and agrees that Juniper has set its prices and entered into this Agreement in reliance upon the disclaimers of warranty and the limitations of liability set forth herein, that the same reflect an allocation of risk between the Parties (including the risk that a contract remedy may fail of its essential purpose and cause consequential loss), and that the same form an essential basis of the bargain between the Parties.

**9. Termination.** Any breach of this Agreement or failure by Customer to pay any applicable fees due shall result in automatic termination of the license granted herein. Upon such termination, Customer shall destroy or return to Juniper all copies of the Software and related documentation in Customer's possession or control.

**10. Taxes.** All license fees for the Software are exclusive of taxes, withholdings, duties, or levies (collectively "Taxes"). Customer shall be responsible for paying Taxes arising from the purchase of the license, or importation or use of the Software.

**11. Export.** Customer agrees to comply with all applicable export laws and restrictions and regulations of any United States and any applicable foreign agency or authority, and not to export or re-export the Software or any direct product thereof in violation of any such restrictions, laws or regulations, or without all necessary approvals. Customer shall be liable for any such violations. The version of the Software supplied to Customer may contain encryption or other capabilities restricting Customer's ability to export the Software without an export license.

**12. Commercial Computer Software.** The Software is "commercial computer software" and is provided with restricted rights. Use, duplication, or disclosure by the United States government is subject to restrictions set forth in this Agreement and as provided in DFARS 227.7201 through 227.7202-4, FAR 12.212, FAR 27.405(b)(2), FAR 52.227-19, or FAR 52.227-14(ALT III) as applicable.

**13. Interface Information.** To the extent required by applicable law, and at Customer's written request, Juniper shall provide Customer with the interface information needed to achieve interoperability between the Software and another independently created program, on payment of applicable fee, if any. Customer shall observe strict obligations of confidentiality with respect to such information and shall use such information in compliance with any applicable terms and conditions upon which Juniper makes such information available.

**14. Third Party Software.** Any licensor of Juniper whose software is embedded in the Software and any supplier of Juniper whose products or technology are embedded in (or services are accessed by) the Software shall be a third party beneficiary with respect to this Agreement, and such licensor or vendor shall have the right to enforce this Agreement in its own name as if it were Juniper. In addition, certain third party software may be provided with the Software and is subject to the accompanying license(s), if any, of its respective owner(s). To the extent portions of the Software are distributed under and subject to open source licenses obligating Juniper to make the source code for such portions publicly available (such as the GNU General Public License ("GPL") or the GNU Library General Public License ("LGPL")), Juniper will make such source code portions (including Juniper modifications, as appropriate) available upon request for a period of up to three years from the date of distribution. Such request can be made in writing to Juniper Networks, Inc., 1194 N. Mathilda Ave., Sunnyvale, CA 94089, ATTN: General Counsel. You may obtain a copy of the GPL at <http://www.gnu.org/licenses/gpl.html>, and a copy of the LGPL at <http://www.gnu.org/licenses/lgpl.html>.

**15. Miscellaneous.** This Agreement shall be governed by the laws of the State of California without reference to its conflicts of laws principles. The provisions of the U.N. Convention for the International Sale of Goods shall not apply to this Agreement. For any disputes arising under this Agreement, the Parties hereby consent to the personal and exclusive jurisdiction of, and venue in, the state and federal courts within Santa Clara County, California. This Agreement constitutes the entire and sole agreement between Juniper and the Customer with respect to the Software, and supersedes all prior and contemporaneous agreements relating to the Software, whether oral or written (including any inconsistent terms contained in a purchase order), except that the terms of a separate written agreement executed by an authorized Juniper representative and Customer shall govern to the extent such terms are inconsistent or conflict with terms contained herein. No modification to this Agreement nor any waiver of any rights hereunder shall be effective unless expressly assented to in writing by the party to be charged. If any portion of this Agreement is held invalid, the Parties agree that such invalidity shall not affect the validity of the remainder of this Agreement. This Agreement and associated documentation has been written in the English language, and the Parties agree that the English version will govern. (For Canada: Les parties aux présentés confirment leur volonté que cette convention de même que tous les documents y compris tout avis qui s'y rattache, soient rédigés en langue anglaise. (Translation: The parties confirm that this Agreement and all related documentation is and will be in the English language).)



# Table of Contents

	<b>About This Guide</b>	<b>vii</b>
	Audience .....	vii
	Where to Find Additional Information .....	vii
<b>Chapter 1</b>	<b>Introduction</b>	<b>1</b>
	Using Transparent Mode .....	2
	Recommendations for Deploying a Test Setup .....	2
	Important Guidelines that Apply to All Scenarios .....	3
	Deploying the Appropriate Firewall.....	4
	IPsec and Source IP Guide for the ScreenOS Enforcer .....	5
<b>Chapter 2</b>	<b>Server Front End Deployment Scenario</b>	<b>7</b>
	Overview of Server Front End Deployment Scenario .....	7
	Overview of Customer Business Problem .....	7
	Overview of the Solution for a Server Front End Scenario .....	7
	Deploying the Unified Access Control Solution in a Server Front End Scenario ..	8
<b>Chapter 3</b>	<b>WAN Gateway Deployment Scenario</b>	<b>11</b>
	Overview of Example WAN Gateway Deployment Scenario.....	11
	Overview of Customer Business Problem .....	11
	Overview of the Solution for a WAN Gateway Scenario .....	11
	Deploying the Unified Access Control solution in a WAN Gateway Scenario ..	11
<b>Chapter 4</b>	<b>MAC Address Authentication</b>	<b>15</b>
	Overview of MAC Address Authentication for Unmanagable Devices.....	15
	Overview of Customer Business Problem .....	15
	Overview of the Solution for MAC Address Authentication .....	15
	Deploying Unified Access Control with MAC Address Authentication .....	15
<b>Chapter 5</b>	<b>802.1X Deployment Scenario</b>	<b>19</b>
	Overview of 802.1X Deployment Scenario using a Remediation VLAN.....	19
	Overview of Customer Business Problem .....	19
	Overview of the 802.1X Solution .....	19
	Basic Setup .....	20
	Deploying an 802.1X Network with a Quarantine VLAN .....	20
	Adding the Infranet Enforcer for Additional Protection.....	22
<b>Chapter 6</b>	<b>Intrusion Detection and Prevention (IDP) Deployment Scenario</b>	<b>25</b>
	Deploying IDP in an 802.1X Network .....	25
	Overview of Customer Business Problem .....	25
	Overview of the Solution with IDP.....	25
	Deploying the Unified Access Control Solution with IDP in an 802.1X Environment .....	26



# About This Guide

This guide contains information and recommendations for deploying five example scenarios of the unified access control solution. You can adapt the information to apply to your specific deployment.

---

## Audience

This guide is for the evaluator or system administrator responsible for configuring the following products for the unified access control solution:

- Infranet Controller
- Infranet Enforcer

---

## Where to Find Additional Information

This guide contains general information to help you understand how to deploy the Infranet Enforcer and Infranet Controller in five different example scenarios. This guide does not contain installation information, feature overviews, or detailed configuration instructions. Those types of information are available in the following guides:

- For information on how to Infranet Enforcer/Infranet Controller, see the *Unified Access Control Installation Guide* that is included with the Infranet Controller.
- For detailed instructions on how to configure the Infranet Enforcer and Infranet Controller for the server front-end scenario, see the *Unified Access Control Quick Start Guide*. The guide is available as a PDF on the Juniper Networks support site.
- For comprehensive overview, configuration instructions, and troubleshooting information, see the *Unified Access Control Administration Guide*. This guide is available as online Help in the administrator's Web console for the Infranet Controller. To open the online Help after completing the Task Guide instructions, click the **Help** link at the top of the Web console. This guide is also available as a PDF on the Juniper Networks support site.
- For more information about configuring the Infranet Enforcer firewall, see the *NetScreen Concepts & Examples ScreenOS Reference Guide*, which you can download from [www.juniper.net/techpubs/](http://www.juniper.net/techpubs/).



## Chapter 1

# Introduction

One of the challenges in securing a network is that it can consist of many different components that are deployed in various scenarios, each of which have different potential vulnerabilities. In an extended enterprise, remote and mobile users need access to the enterprise network, typically by using a remote access VPN. SSL VPNs that support sophisticated client endpoint assessments and policy enforcement capabilities can solve the vulnerability problems of extended enterprises.

However, other areas of the enterprise network can also be vulnerable and each poses unique security challenges:

- **Server front end**—Data centers are often protected by a firewall that has no information about the users or the client endpoints using the applications behind the firewall. To solve this problem, the protection point is located in front of a data center. For more information, see “Server Front End Deployment Scenario” on page 7.
- **WAN gateway**—The WAN gateway is a key source of risk. Unsecured client endpoints can inadvertently transfer threats to the network. To solve this problem, the protection point is located in front of the Internet access gateway. For more information, see “WAN Gateway Deployment Scenario” on page 11.
- **MAC Address Authentication**—There are potentially many different entities on the network in addition to end users. Phones, printers, and other devices that are not user-controlled should be permitted to authenticate to the network. See “MAC Address Authentication” on page 15.
- **802.1X enforcement**—You can control user access to resources by using 802.1X enforcement and VLANs. For more information, see “802.1X Deployment Scenario” on page 19.
- **802.1X Enforcement using IDP**—You can use Juniper Networks Intrusion Detection and Protection (IDP) with the Unified Access Control solution to add real-time attack protection and enforcement to the network.



**NOTE:** If you want to deploy two or more of these scenarios in combination, contact your Juniper Networks representative for assistance with configuration.

---

---

## Using Transparent Mode

The Juniper Networks Infranet Enforcer firewall supports a configuration mode called Transparent Mode. An Infranet Enforcer in Transparent mode does not participate in IP routing (layer 3), but instead forwards layer 2 packets.

By using Transparent mode, you can quickly install the Infranet Enforcer into an existing network infrastructure without doing any network renumbering:

- No need to reconfigure the IP settings of routers or protected servers
- No need to create Mapped or Virtual IP addresses for incoming traffic to reach protected servers



**NOTE:** You can use Transparent mode for all of the example deployment scenarios shown in this guide except the distributed enterprise scenario.

---

For more information about how to set up routing on the Infranet Enforcer, see the “Routing” volume of the *NetScreen Concepts & Examples ScreenOS Reference Guide*, which you can download from [www.juniper.net/techpubs/](http://www.juniper.net/techpubs/). For more information about Transparent or Route mode, see the “Fundamentals” volume of the *NetScreen Concepts & Examples ScreenOS Reference Guide*.

---

## Recommendations for Deploying a Test Setup

There are many ways to configure the Infranet Enforcer and Infranet Controller depending on the requirements of your environment. Some of the main tasks are to define the resources you want to protect, define the group of users who need to access the protected resources, and then create the necessary policies.

But, if you are doing an evaluation, you should consider using a simple deployment scenario such as a server front end. You can use the following recommendations as guidelines for deploying a test setup. Note that these recommendations describe one of many approaches and your particular deployment may require different or additional steps.

1. Identify the first network resource you want to protect. It’s a good idea to start testing the configuration of your deployment with one resource.
2. Install the Infranet Enforcer in front of the protected resource or upgrade your existing Infranet Enforcer. You can set up the Infranet Enforcer in Transparent mode, which is easier to configure because you can avoid renumbering your network for the test deployment.
3. Configure the Infranet Enforcer to allow all traffic to the protected resource to test that users can access the resource. At this point, all users should be able to access the resource without any need to sign into the Infranet Controller.
4. Install the Infranet Controller.

5. Configure the Infranet Enforcer to connect with the Infranet Controller.
6. If you want to allow trusted users to access a protected resource without signing into the Infranet Controller, set up a static policy in the Infranet Enforcer to permit traffic from those users' source IP addresses to the resource.
7. Define an address group that contains a set of IP addresses from which your initial test users will access the protected network resource.
  - If you are using source IP enforcement, configure a “permit infranet-auth” policy that uses the address group as the source for the policy. The infranet-auth policy must appear above the “permit” policy configured in step 3.
  - If you are using IPsec enforcement, configure a “deny” policy instead of a “permit infranet-auth” policy on the Infranet Enforcer, and then configure an IPsec routing policy at the top.
8. As your testing is successful, gradually add more users and enable other features you want to test such as the Host Enforcer.

---

## Important Guidelines that Apply to All Scenarios

Keep the following important guidelines in mind when configuring all of the scenarios in this guide:

- If you want to use Network Address Translation (NAT) devices in the Unified Access Control solution, the endpoints must be located on one side of the NAT devices, and the Infranet Controller and Infranet Enforcer must *both* be located on the other side of the devices.

Also note the following if you are using NAT:

- NAT is not supported between the Infranet Controller and Infranet Enforcer.
- If there is a NAT device between the endpoint and the Infranet Controller, but not between the endpoint and the Infranet Enforcer, source IP enforcement does not work. This is also true if there is a NAT device between the endpoint and the Infranet Enforcer, but not between the endpoint and the Infranet Controller.
- Before deploying the solution, you will need to know the network addresses of your Infranet Enforcer, Infranet Controller, 802.1X switches or 802.1X wireless access points, your solution users, and the network resources you want to protect. You will also need to know the approximate number of concurrent user tunnels so that you can deploy the appropriate Infranet Enforcer and Infranet Controller. For more information, see “Deploying the Appropriate Firewall” on page 4 and the table of recommended Infranet Enforcers included in the description for each scenario.
- If the Infranet Enforcer is between the Infranet Controller and an authentication server, be sure to create a static policy on the Infranet Enforcer to allow traffic from the Infranet Controller to the authentication server.

- If there are any other resources (such as a DNS server) that users need to access before authenticating to the Infranet Controller, be sure to configure the Infranet Enforcer with static policies that allow traffic from the users to those resources.
- If you are using remediation and the resources users need to bring their computer into compliance (such as current anti-virus definitions) are behind the Infranet Enforcer, you must create a static policy on the Infranet Enforcer to allow traffic to that resource. Otherwise, if you are using Host Enforcer to block TCP traffic, you must create a Host Enforcer policy on the Infranet Controller to allow traffic to that resource.
- If you create an IPsec routing policy on the Infranet Controller, be sure to include a range of exceptions for traffic to certain resources that you do not want to flow through the Infranet Enforcer. Do not use IPsec for the Infranet Controller, the Infranet Enforcer, DNS servers, and networks where your endpoints are located. For example, if you create an IPsec routing policy that uses IPsec on an entire network range (such as 0.0.0.0/0) for your protected resources, be sure to also specify exceptions in the same policy for the IP addresses assigned to Infranet Controller, Infranet Enforcer, and the endpoints.
- IP pool policies are required if one of the following applies to your situation:
  - You are using IPsec in a NAT environment.
  - You selected the **Always use a virtual adapter** option in an IPsec routing policy to enable interoperability with other third-party IPsec clients running simultaneously on the endpoint, such as Juniper Network Connect or Microsoft IPsec.

For more information about configuring IP pool policies and IPsec routing policies, see the *Unified Access Control Administration Guide*.

- If you import a different server certificate into the Infranet Controller and CA certificate into the Infranet Enforcer, you may need to initiate a new connection to use them by restarting the Infranet Controller services on the **Maintenance > System > Platform** page. For more troubleshooting information, see the *Unified Access Control Administration Guide*.

---

## Deploying the Appropriate Firewall

You can use the ScreenOS Enforcer or the JUNOS Enforcer as the policy enforcement point in your Unified Access Control deployment.

The following table provides guidance to allow you to choose the correct Infranet Enforcer for your network. Use these guidelines for deploying the right firewall for your network:

**Table 1: Firewall Selection Guide**

Juniper Networks Firewalls				
Product	SSG 5	SSG 140	ISG 1000	SRX 5600
	SSG 20	SSG 320M	ISG 2000	SRX 5800
		SSG 350M	ISG with IDP	
		SSG 520/520M	Netscreen 5200	
		SSG 550/550M	Netscreen 5400	
Designed For	Small branch and remote offices, retail outlets, and fixed telecommuters.	Medium to large branch offices and stand-alone medium enterprises.	Medium to large enterprise sites, carrier networks, data centers.	Large enterprise data center, carrier networks, content provider networks.

**IPsec and Source IP Guide for the ScreenOS Enforcer**

Table 2 lists the maximum number of concurrent IPsec tunnels and source IP users for each ScreenOS Enforcer model and license. One IPsec tunnel or source IP user is required for each user that will be simultaneously accessing resources protected by the ScreenOS Enforcer. Note that if dynamic discovery is not used, one IPsec tunnel or source IP user is required each time a user signs into the ScreenOS Enforcer.

Use the information in this table to deploy the appropriate Infranet Enforcer model based on the number of concurrent IPsec tunnels and source IP users you need to support. Note that you must also include any existing policies, tunnels, and routes configured on the Infranet Enforcer in the total number.

**Table 2: Maximum Concurrent IPsec Tunnels and Source IP Users on each ScreenOS Enforcer Model and License**

Mode	HSC	5XT <sup>a</sup>	25 <sup>b</sup>	50 <sup>c</sup>	SSG5	SSG20	500	ISG 1000	ISG 2000	5200	5400
IPsec tunnels	5	10	125	500	500	500	1000	1,000	1,000	12,000	12,000
					(Base)	(Base)	(Base)	(Base)	(Base)		
					1,000	1,000	8,192	2,000	10,000		
					(Adv.)	(Adv.)	(Adv.)	(Adv.)	(Adv.)		
Source IP users	4,096	4,096	4,096	4,096	4,096	4,096	8,192	8,192	12,288	12,000	12,000

- a.Base and Elite licenses
- b.Base and Advanced licenses

c. Base and Advanced licenses

Note that NS 204 and 208 are End of Life (EOL) on 9/30/2008 and 5GT is EOL on 12/30/2008.

IPsec is not supported on the JUNOS Enforcer.

For the most current information matrix of Juniper Networks products interoperability, see the *Unified Access Control Supported Platforms Guide*. for the most current.

## Chapter 2

# Server Front End Deployment Scenario

---

## Overview of Server Front End Deployment Scenario

### **Overview of Customer Business Problem**

You have a large data center and must protect it from users on the LAN by making sure that only compliant and authenticated users are granted access to data center resources. The solution to this problem should not significantly affect network access performance, and it should not trade off security for performance.

Further, you want to be able to grant access to specific protected resources based on a user's job function or security level.

### **Overview of the Solution for a Server Front End Scenario**

Together, the Infranet Enforcer and Infranet Controller can dynamically enforce network security policies and protect data center resources from unauthorized users and non-compliant endpoints.

To secure the data center, the unified access control solution supports comprehensive endpoint assessment capabilities with the Infranet Controllers Host Checker capabilities for health state compliance measurement, and performs an assessment both prior to user sign in and during the entire user session.

By denying access to endpoints that are unauthorized or not compliant with network security policies, Juniper's UAC solution provides security without replacing infrastructure. By assigning policies based on an individual user's role, you can segregate the network by organizational needs. Individual users can access only those resources that you specify.

---

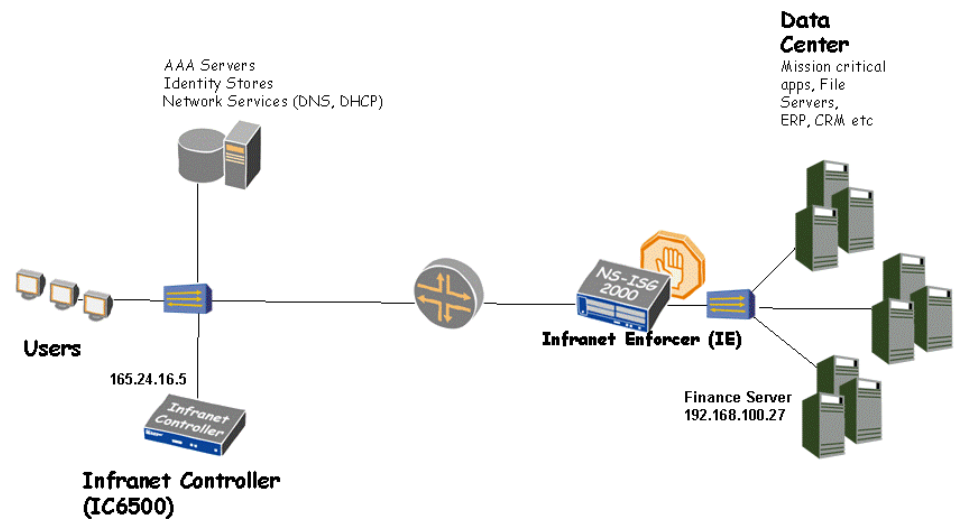
## Deploying the Unified Access Control Solution in a Server Front End Scenario

To deploy the Infranet Controller in a server front end scenario:

1. Deploy the Infranet Enforcer in front of the data center resources you want to protect as shown in Figure 1. Assign each group of protected resources a different internal IP address to segregate different internal assets. For example, the Finance Server assets have an IP address of 192.168.100.27 in this example.
2. Configure captive portal on the ScreenOS Enforcer to re-direct users to the Infranet Controller with the ScreenOS Enforcer to allow users to sign in by accessing protected resources. Captive portal is not supported with the JUNOS Enforcer. Users will sign-in directly to the URI of the Infranet Controller.
3. Deploy the Infranet Controller in the network so that users can access the device. Use the internal port on the Infranet Controller to connect users, the firewall, and authentication servers.
4. Set up security zones and interfaces on the firewall device. End users should always be in a different security zone than protected resources. For example, protected resources in the data center should be in a trusted zone, users should be in an untrusted zone.
5. Add individual users to either an external authentication server, or the local authentication server.
6. Set up roles and realms for individual users. You can provision access to protected resources based on your network security needs. For example, you can protect individual resources using different resource access policies, and then assign roles to the policies based on the resources individuals need to access. To restrict the Finance group to accessing only finance resources, configure a Finance role. Then, configure a resource access policy to Allow access for the Finance role for resources at 192.168.100.27.
7. Create sign-in policies and sign-in pages for individuals to access the Infranet Controller using Odyssey Access Client on Windows endpoints, or agentless access or the Java agent on Solaris, Macintosh and Linux platforms.
8. Set up IPsec for encrypted traffic or source IP policies for clear-text traffic on the ScreenOS Enforcer. IPsec is not supported on the JUNOS Enforcer, users can only connect using source IP.
9. Configure Host Checker policies on the Infranet Controller to ensure endpoint compliance with your network security policies. For example, you can require user endpoints to run the most current version of a particular antivirus application. You can configure a default remediation role that allows users limited access if they do not meet the requirements.
10. Configure logging and network troubleshooting features on the Infranet Controller to help you correctly diagnose any difficulties that end users experience signing in.

11. Instruct end users how to access the Infranet Controller. If you have configured captive portal (on the ScreenOS Enforcer only) users can attempt to directly access the protected resources and they will be automatically redirected to the Infranet Controller. If you have not configured captive portal, users can connect to the Infranet Controller by directing their browser to the Infranet Controller URI that you specify. For example, if you have configured captive portal on the ScreenOS Enforcer, users in Finance can login to 192.168.100.27. Without captive portal, users access the Infranet Controller at 165.24.16.5.

**Figure 1: Server Front End Scenario**



**NOTE:**

- For detailed instructions on how to configure the Infranet Enforcer and Infranet Controller for this server front-end scenario, see the *Unified Access Control Quick Start Guide*. The guide is available as a PDF on the Juniper Networks support site.



## Chapter 3

# WAN Gateway Deployment Scenario

---

## Overview of Example WAN Gateway Deployment Scenario

### **Overview of Customer Business Problem**

You want to ensure that user access to the WAN is enabled only for authorized users and compliant endpoints. If the endpoint is not compliant, the solution must restrict the endpoint's WAN access and use remediation actions to force the user to bring the endpoint into compliance before restoring WAN access.

If a user or endpoint can't pass the health checks required for WAN access, you still want to allow the user access to some resources on the network so that productivity is not lost.

### **Overview of the Solution for a WAN Gateway Scenario**

Together, the Infranet Enforcer and Infranet Controller can dynamically enforce network security policies to make sure that only authenticated users and compliant endpoints can access the WAN.

To secure the WAN gateway, the unified access control solution supports comprehensive endpoint assessment capabilities with the Infranet Controllers Host Checker capabilities for health state compliance measurement, and performs an assessment both prior to user sign in and during the entire user session.

---

## Deploying the Unified Access Control solution in a WAN Gateway Scenario

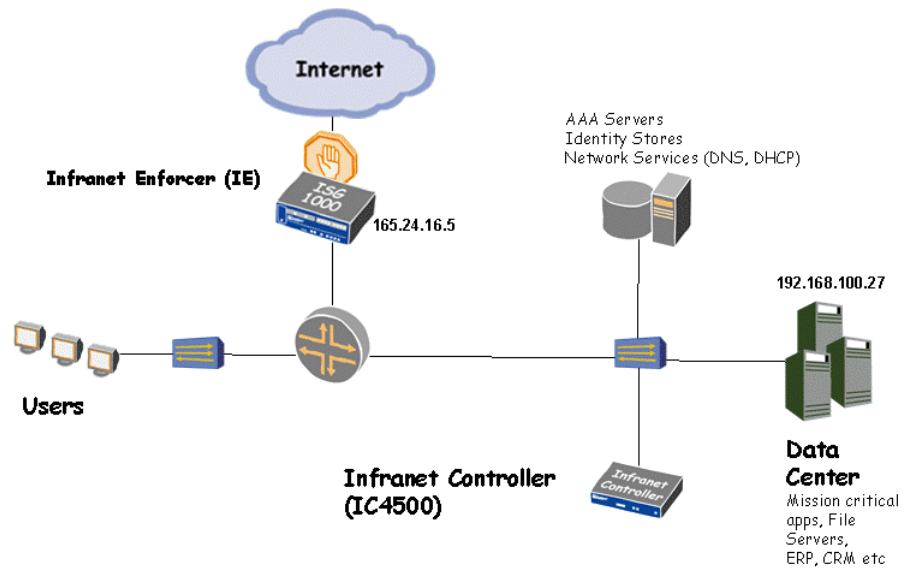
To deploy a unified access control solution in a WAN gateway scenario:

1. Deploy the Infranet Enforcer in the DMZ as shown in Figure 2.
2. Configure captive portal on the ScreenOS Enforcer to re-direct users to the Infranet Controller with the ScreenOS Enforcer to allow users to sign in by accessing protected resources. Captive portal is not supported with the JUNOS Enforcer. Users will sign-in directly to the URI of the Infranet Controller.

3. Deploy the Infranet Controller in the network so that users can access the device. Use the internal port on the Infranet Controller to connect users, the firewall, and authentication servers.
4. Set up security zones and interfaces on the firewall device. End users should always be in a different security zone than protected resources. For example, protected resources in the data center should be in a trusted zone, users should be in an untrusted zone.
5. Add individual users to either an external authentication server, or the local authentication server.
6. Set up roles and realms for individual users. You can provision access to resources based on your network security needs. In this example, create two roles: a WAN\_Access role and an Employee role.
7. Use role mapping to assign both roles to the Company authentication realm.
8. You can protect individual resources using different resource access policies, and then assign roles to the policies based on compliance. Set up one resource access policy that allows the WAN\_Access role to access the WAN gateway at 165.24.16.5. Set up a second resource access policy that allows the Employee role to access the data center at 192.168.100.27.
9. Configure two Host Checker policies: a Firewall policy that requires endpoints to run a particular version of a desktop firewall and an Internal Access policy that does not require the firewall.
10. Assign the Firewall Host Checker policy to the WAN\_Access role, and assign the Internal\_Access Host Checker policy to the Employee role.
11. Create sign-in policies and sign-in pages for individuals to access the Infranet Controller using Odyssey Access Client on Windows endpoints, or agentless access or the Java agent on Solaris, Macintosh and Linux platforms.
12. Set up IPsec for encrypted traffic or source IP policies for clear-text traffic on the ScreenOS Enforcer. IPsec is not supported on the JUNOS Enforcer, users can only connect using source IP.
13. Configure logging and network troubleshooting features on the Infranet Controller to help you correctly diagnose any difficulties that end users experience signing in.
14. Instruct end users how to access the Infranet Controller. If you have configured captive portal (on the ScreenOS Enforcer only) users can attempt to directly access the protected resources and they will be automatically redirected to the Infranet Controller. If you have not configured captive portal, users can connect to the Infranet Controller by directing their browser to the Infranet Controller URI that you specify.

When a user authenticates to the Company realm, they are eligible for the WAN\_Access role and the Employee role. If the user has the specified desktop firewall version running, they can access the WAN with the WAN\_Access role. If the user does not have the firewall, they cannot access the WAN gateway, but they can access internal resources with the Employee role.

Figure 2: WAN Gateway Scenario



**NOTE:** When deploying the WAN gateway scenario, keep these guidelines in mind:

- If you create an IPsec routing policy on the Infranet Controller, be sure to include a range of exceptions for traffic to certain resources that you do not want to flow through the Infranet Enforcer. Do not use IPsec for the Infranet Controller, the Infranet Enforcer, and networks where your endpoints are located. For example, if you create an IPsec routing policy that uses IPsec on an entire network range (such as 0.0.0.0/0) for your protected resources, be sure to also specify exceptions in the same policy for the IP addresses assigned to Infranet Controller, Infranet Enforcer, and the endpoints.



## Chapter 4

# MAC Address Authentication

---

## Overview of MAC Address Authentication for Unmanageable Devices

### **Overview of Customer Business Problem**

You have a number of non-802.1X IP phones and printers that you would like to add to the network. Because these devices cannot authenticate themselves, you need a way to verify their authenticity before permitting them on the network.

### **Overview of the Solution for MAC Address Authentication**

Unmanageable devices each have a unique MAC address. With MAC-based authentication the MAC address serves as both the username and the password.

MAC address authentication is deployed at the edge of the network to provide port-based security. MAC address authentication uses RADIUS as the method for information exchange.

When a device connects to a switch, the switch forwards the MAC address to the IVE as the login credential. The IVE RADIUS server consults the authentication server, either a local database or an external LDAP server, and allows or denies access to the device based on whether there is a matching entry.

After you direct unmanaged devices to a default VLAN, other resources in the VLAN can access the device. For example, if a printer that is plugged into a UAC-integrated switch is registered as a print server on the default VLAN, hosts that can access that VLAN on the network can access the printer.

You can add MAC addresses manually, you can provision MAC address authentication server from an external LDAP server, or you can utilize a third-party device that can profile endpoints and detect MAC addresses on the network.

---

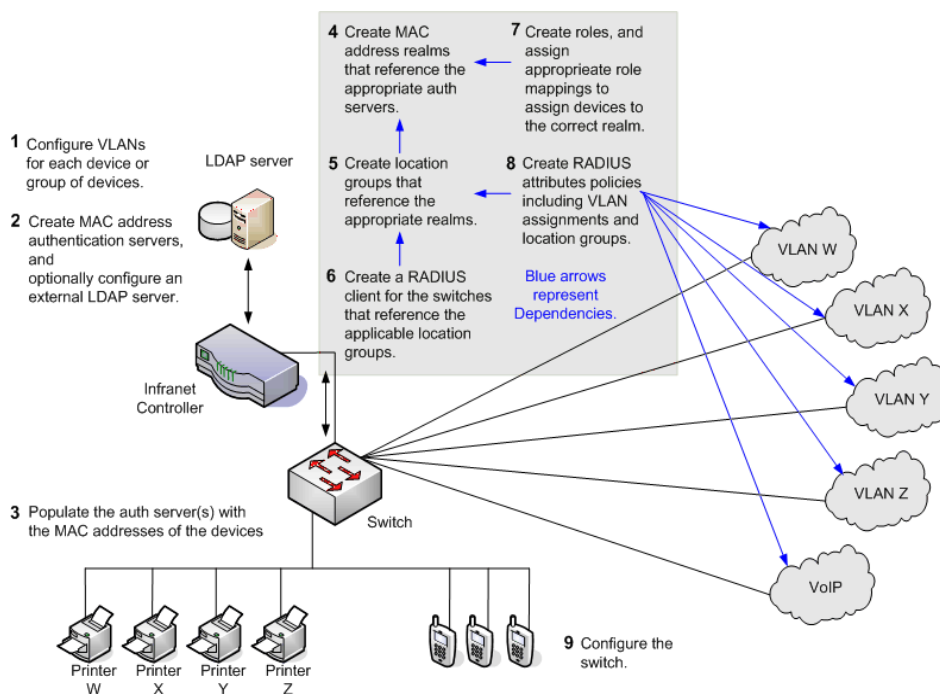
## Deploying Unified Access Control with MAC Address Authentication

To allow access for unmanaged devices, you must perform these basic tasks:

1. Configure the necessary VLANs on your internal network to accommodate the different devices that you want to allow. On the IVE, you assign devices to VLANs through the location groups that are added to RADIUS attributes policies.

In Figure 3 an example network is configured with different phones and printers, an external LDAP server and separate VLANs for different devices. MAC address authentication on the IVE is extremely flexible, and you can configure your network using any or all of these components.

**Figure 3: Example MAC Authentication Configuration**



2. Create MAC address authentication server(s), and populate the server(s) with MAC addresses and wildcards from the **Authentication > Auth. Servers** page. Use the MAC address for both the user name and the password.

**NOTE:**

- The IVE supports several formats for MAC address credentials including no-delimiter 003048436665, single dash 003048-436665, multi-dash 00-30-48-43-66-65, and multi-colon 00:30:48:43:66:65. In the user log, entries appear in the multi-colon format.
- Optionally, you can configure an external LDAP server or a third-party appliance to monitor and classify devices on the network.

3. Create MAC address realms that reference the authentication server(s) or LDAP server(s) from the **UAC > MAC Address Realms** page.
4. Create location groups that reference the realms from the **UAC > Network Access > Location Groups** page.
5. Create RADIUS client policies for the switches that reference the applicable location groups from the **UAC > Network Access > RADIUS Client** page.

6. Create roles from the **Users > Roles** page, and give the authentication server role mappings through the realm as required. You must configure a session length for the role that is appropriate for the re-authentication interval of the switch.



**NOTE:** Do not configure any role restrictions, otherwise roles cannot get assigned to devices, and do not apply any Host Checker policies at the role or realm level.

---

7. Configure RADIUS attributes, to include the applicable VLAN assignments from the **UAC > Network Access > RADIUS Attributes** page.
8. Configure the switch to communicate with the IVE for MAC address authentication. The IVE supports HP Procurve, Cisco Catalyst, and Nortel Secure Network Access switches. You will need to configure the following options on the switch:
  - Configure the desired ports to use the appropriate VLAN for unauthenticated traffic
  - Configure the ports to perform MAC-based RADIUS authentication
  - Specify the IVE as the RADIUS server, with the appropriate shared secret and IP address.

The HP and Cisco switches can use CHAP and EAP-MD5-Challenge protocols for MAC address authentication with the user name (the MAC address) as the clear text password. By default, the Nortel switch uses PAP, with a password in the format . < MAC address > .. Juniper Networks recommends using PAP with the Nortel switch.



## Chapter 5

# 802.1X Deployment Scenario

---

## Overview of 802.1X Deployment Scenario using a Remediation VLAN

### **Overview of Customer Business Problem**

You've been having a problem with host machines on the internal network getting infected from users accessing inappropriate or unsecure sites. You install a personal firewall application on each individual host machine, but users have found a way to uninstall or bypass the firewall application.

You need a way to prevent users from accessing the corporate network if they do not have the firewall installed and running. Setting up a remediation VLAN allows users to access a limited area where they can install the firewall and remediate their machines.

### **Overview of the 802.1X Solution**

In this 802.1X deployment scenario there are two VLANs used to control user access to resources:

- Trusted VLAN: 1
- Quarantine / Remediation VLAN: 31

The interface of the Infranet Controller is trunked to the switch and there is an Infranet Controller virtual interface in every VLAN. All users can access the Infranet Controller from all subnets using the different IP addresses. Users with proper credentials whose endpoints are compliant with company security policies can access the Corporate network. Users whose endpoints are not compliant are placed on the Quarantine VLAN.

In this scenario, an additional layer of security is added by using the Infranet Enforcer to control access to the protected resource, which is a Finance server in the Trusted VLAN.

This document assumes that you are familiar with basic configuration of the Infranet Controller and your Network Access Device (NAD) and 802.1X. See the *Unified Access Control Administrator's Guide* for detailed configuration instructions.

## Basic Setup

In this scenario 802.1X with VLANs that are not routed is used, and there is no default IP address for endpoints. The user must provide valid sign-in credentials to obtain an IP address from an internal DHCP server on the network.

This scenario assumes that endpoints will connect using Odyssey Access Client as the 802.1X supplicant. Users who are accessing the Infranet Controller for the first time will have no way of obtaining the client. You can download the UAC Agent Installer and pre-install the client for initial use.

### Resources

In this scenario, you control access to these three resources:

- Finance Server: 10.0.1.16
- Corp Server: 10.0.0.16
- Remediation Server: 172.16.0.16

### Access Control Rules

To define access control policies, define who the user is and which resources they are allowed to access, if any. In this scenario, the user has to provide valid sign-in credentials to obtain an IP address on the network.

**Table 3: Network Access**

Trusted Network	Quarantined Network	No Network Access
All authenticated users with endpoints that comply with security policies	All authenticated users with endpoints that do not comply with security policies	All unauthenticated users

To access the Corporate server, a user must have a compliant endpoint and valid sign-in credentials. To access the Finance Server, the user must have a compliant endpoint and be a member of the Finance role or group. All other users with un-compliant endpoints can access the Remediation server only.

**Table 4: Resource Access**

Corporate Server	Finance Server	Remediation Server
All users that are using a compliant endpoint	All users that are a member of finance and are using a compliant endpoint	All users that are using a non-compliant endpoint

## Deploying an 802.1X Network with a Quarantine VLAN

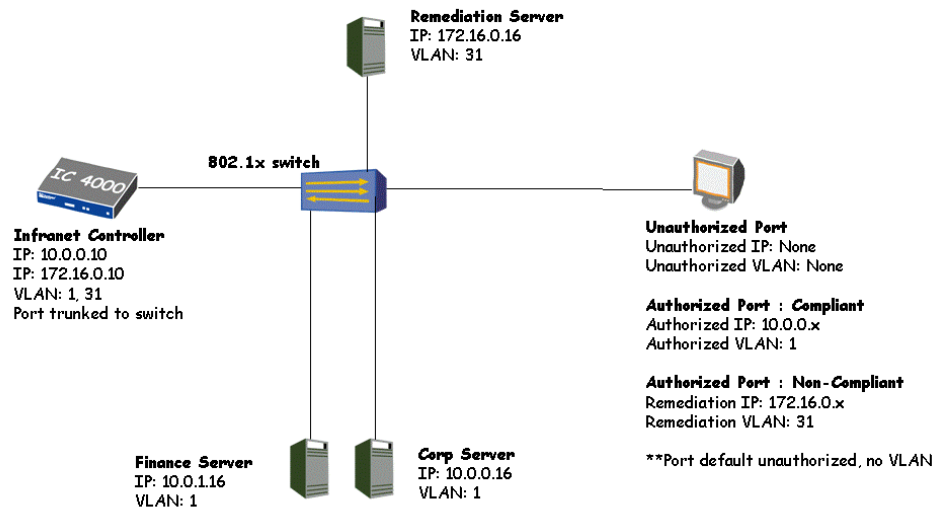
To configure an 802.1X network with a quarantine VLAN:

1. Deploy the Infranet Controller in the network with the internal port connected to the trunk port of an 802.1X-compliant Network Access Device (NAD). Ensure that the ports on the NAD are enabled for 802.1X and the device supports Dynamic VLAN assignment.

2. Configure two VLANs on the NAD: VLAN 31 for Quarantine and VLAN 1 for regular employee access.
3. Add individual users to either an external authentication server or the local authentication server.
4. Set up roles and realms for individual users. You can provision access to resources based on your network security needs. In this example, create two roles: an Employee role and a Quarantine role.
5. Use role mapping to assign both roles to the Company authentication realm.
6. Configure the Infranet Controller RADIUS server for 802.1X, adding your NAD as the RADIUS client.
7. Configure two RADIUS attributes policies. One RADIUS attributes policy is applied to the Quarantine role with a VLAN assignment of 1. The second policy is applied to the Employee role with a VLAN assignment of 31.
8. Configure two Host Checker policies: a Firewall policy that requires endpoints to run a particular version of a personal firewall and a Quarantine policy that does not require the firewall.
9. Assign both Host Checker policies to the Employee and Quarantine roles.
10. Create sign-in policies and sign-in pages for individuals to access the Infranet Controller using Odyssey Access Client.
11. Instruct end users how to access the Infranet Controller. Ensure that the Infranet Controller you are using has been added to the users' Odyssey Access Client application.

Authenticated Odyssey Access Client users who have the personal firewall installed will be assigned the Employee role, and the RADIUS return attributes policy will place the user on VLAN 1. Users who do not have the firewall installed will be assigned the Quarantine role, and the RADIUS return attributes policy will place the user on VLAN 31. Users on the Corporate network can access anything outside of the Finance server. "802.1X with an Isolated VLAN" on page 22 illustrates this example.

You can augment the Host Checker policy to provide remediation for the quarantined user. After the user's endpoint is remediated, access to the Corporate network will be permitted.

**Figure 4: 802.1X with an Isolated VLAN**

### Adding the Infranet Enforcer for Additional Protection

You can provide additional protection to sensitive resources within the network by adding the Infranet Enforcer. In this case, you can allow a specified group of users to access the Finance server within the Corporate network.

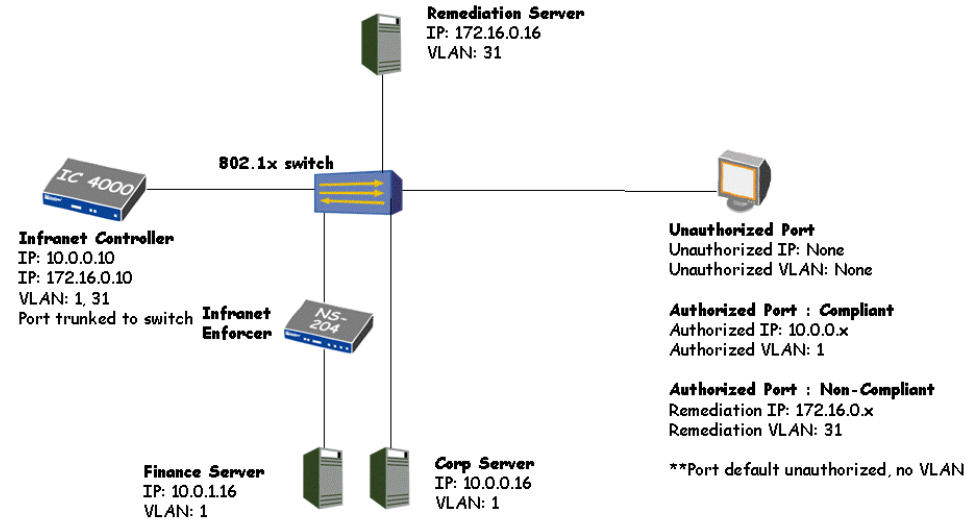
1. Install the Infranet Enforcer within the VLAN 1 trunk port.
2. Assign the the IP address 10.0.1.16 to the Finance server
3. Set up security zones and interfaces on the firewall device. End users should always be in a different security zone than protected resources. For example, protected resources on the Finance server should be in a trusted zone, users should be in an untrusted zone.
4. Create a third role on the Infranet Controller called Finance, and assign the previously configured Host Checker policies to the role.
5. Use additional role-mapping rules to uniquely identify users who should be added to the Finance role through the Company authentication realm.
6. Set up IPsec for encrypted traffic or source IP policies for clear-text traffic on the ScreenOS Enforcer. IPsec is not supported on the JUNOS Enforcer, users can only connect using source IP.
7. Configure a resource access policy on the Infranet Controller that allows the Finance role access to resources at 10.0.1.16.

As in the previous scenario, authenticated Odyssey Access Client users who have the personal firewall installed will be assigned the Employee role, and the RADIUS return attributes policy will place the user on VLAN 1. Users who do not have the firewall installed will be assigned the Quarantine role, and the RADIUS return attributes policy will place the user on VLAN 31.

Additionally, users who meet the role-mapping rules established for the Finance role can access the Finance server that is protected by the Infranet Enforcer.

Figure 5 illustrates this scenario.

**Figure 5: 802.1X with the Infranet Enforcer**



This scenario can be expanded to include any number of VLANs, with different combinations of user access.











