



Unified Access Control

Deployment Scenarios Guide

Release 2.2
July 2008

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089
USA
408-745-2000
www.juniper.net

Part Number: 22D081408D0

Copyright Notice

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.

This product includes software developed by Maker Communications, Inc., copyright © 1996, 1997, Maker Communications, Inc.

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.

Juniper Networks, the Juniper Networks logo, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JUNOS and JUNOSe are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Copyright 2008 Juniper Networks, Inc. All rights reserved.

FCC Statement

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. The equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with the instruction manual, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Consult the dealer or an experienced radio/TV technician for help.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.

Caution: Changes or modifications to this product could void the user's warranty and authority to operate this device and may result in the equipment no longer complying with FCC requirements for Class A or Class B digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

U.S. Government Rights

Commercial software and commercial software documentation: This documentation is commercial computer software documentation and the products (whether hardware or software) covered by this documentation are or contain commercial computer software. Government users are subject to the Juniper Networks, Inc. standard end user license agreement and any applicable provisions of the FAR and its supplements. No further rights are granted.

Products (whether hardware or software) covered by, and information contained in, this documentation are controlled by U.S. Export Control laws and may be subject to the export or import laws in other countries. Nuclear, missile, chemical, biological weapons end uses or end users, whether direct or indirect, are strictly prohibited. Export or re-export to countries subject to U.S. embargo or to entities identified on US export exclusion lists, including, but not limited to, the denied persons and specially designated national lists, is strictly prohibited.

Disclaimer

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR JUNIPER NETWORKS REPRESENTATIVE FOR A COPY.

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. "Embedded Software" means Software which Juniper has embedded in the Juniper equipment.
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:
 - a. Customer shall use the Embedded Software solely as embedded in, and for execution on, Juniper equipment originally purchased by Customer from Juniper or an authorized Juniper reseller.
 - b. 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; provided, however, with respect to the Steel-Belted Radius or Odyssey Access Client software only, Customer shall use such Software on a single computer containing a single physical random access memory space and containing any number of processors. Use of the Steel-Belted Radius software on multiple computers requires multiple licenses, regardless of whether such computers are physically contained on a single chassis.
 - c. 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, realms, devices, links, ports 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. In addition, such limits may restrict the use of the Software to managing certain kinds of networks or require the Software to be used only in conjunction with other specific Software. Customer's use of the Software shall be subject to all such limitations and purchase of all applicable licenses.
 - d. For any trial copy of the Software, Customer's right to use the Software expires 30 days after download, installation or use of the Software. Customer may operate the Software after the 3D-day trial period only if Customer pays for a license to do so. Customer may not extend or create an additional trial period by re-installing the Software after the 3D-day trial period.
 - e. The Global Enterprise Edition of the Steel-Belted Radius software may be used by Customer only to manage access to Customer's enterprise network. Specifically, service provider customers are expressly prohibited from using the Global Enterprise Edition of the Steel-Belted Radius software to support any commercial network access services. 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 Embedded Software 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; (k) disclose the results of testing or benchmarking of the Software to any third party without the prior written consent of Juniper; or (l) 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 présentes 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 are and will be in the English language)).

Table of Contents

	About This Guide	ix
	Audience.....	ix
	Where to find additional information.....	ix
Chapter 1	Introduction	1
	Using Transparent mode.....	2
	Recommendations for deploying a test setup	2
	Important guidelines that apply to all scenarios	3
	Deploying the appropriate firewall based on number of concurrent IPsec tunnels and source IP users	5
Chapter 2	Server Front End Deployment Scenario	7
	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 a unified access control solution in a server front end scenario.....	7
Chapter 3	WAN Gateway Deployment Scenario	9
	Overview of example WAN gateway deployment scenario	9
	Overview of customer business problem.....	9
	Overview of the solution for a WAN gateway scenario	9
Chapter 4	Distributed Enterprise Deployment Scenario	11
	Overview of example distributed enterprise deployment scenario.....	11
	Overview of customer business problem.....	11
	Overview of the solution for a distributed enterprise scenario	11
	Deploying a unified access control solution in a distributed enterprise scenario 11	
	Deploying the Infranet Controller in branch and headquarters offices.....	12
	Deploying Infranet Controller in corporate headquarters office only	13
Chapter 5	Campus Wired Deployment Scenario	15
	Overview of example campus wired deployment scenario	15
	Overview of customer business problem.....	15
	Overview of the solution for a campus wired scenario	15
	Deploying a unified access control solution in a campus wired scenario.....	15
Chapter 6	Campus Wireless Deployment Scenario	17
	Overview of example campus wireless deployment scenario.....	17
	About the business problem	17
	About the solution for a campus wireless scenario	17
	Deploying a unified access control solution in a campus wireless scenario	17

Chapter 7	802.1X Deployment Scenarios	19
	802.1X deployment scenarios that use a remediation VLAN	19
	Scenario 1: Using VLANs that are not routed (no default IP address)	19
	Scenario 2: Using VLANs that are not routed (use default Quarantine IP address)	21
	Scenario 3: Using VLANs that are routed (no default IP address)	22
	An 802.1X deployment scenario that does not use a remediation VLAN.....	23
	Scenario 4: Using 802.1X without a remediation VLAN and no default IP address	23

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 EnforcerInfranet 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/.

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 9.
- **Distributed enterprise**—The distributed enterprise consists of remote or branch offices that can inadvertently transfer threats to the network via their site-to-site VPN. To solve this problem, the protection points are located between remote and branch offices. For more information, see “Distributed Enterprise Deployment Scenario” on page 11.
- **Campus wired**—In the distribution layer, a corporate campus user can connect to the wired network and inadvertently transfer threats to the network. To solve this problem, the protection point is located in front of users connecting to the wired network. For more information, see “Campus Wired Deployment Scenario” on page 15.
- **Campus wireless**—In the distribution layer, a corporate campus user can connect to the wireless network and inadvertently transfer threats to the network. To solve this problem, the protection point is located in front of users connecting to the wireless network. For more information, see “Campus Wireless Deployment Scenario” on page 17.

- **802.1X enforcement**—You can control user access to resources by using 802.1X enforcement and VLANs. For more information, see “802.1X Deployment Scenarios” on page 19.



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/. 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 based on number of concurrent IPsec tunnels and source IP users” on page 5 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. Or, 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 inter-operability 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 based on number of concurrent IPsec tunnels and source IP users

Table 1 lists the maximum number of concurrent IPsec tunnels and source IP users for each Infranet 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 Infranet 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 Infranet 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 1: Maximum concurrent IPsec tunnels and source IP users on each Infranet Enforcer model and license

Mode	HSC	5XT ^a	5GT	25 ^c	50 ^d	204	208	500	ISG 1000	ISG 2000	5200	5400
			5GT ADSL 5GT Wireless ^b									
IPsec tunnels	5	10	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	4,096	8,192	8,192	12,288	12,000	12,000

a. Base and Elite licenses

b. Base, Plus, and Extended. licenses

c. Base and Advanced licenses

d. Base and Advanced licenses

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.

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 unmanaged or not compliant, Juniper's UAC solution provides security without replacing any infrastructure.

Deploying a 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. (If you have an existing Juniper Networks firewall that is deployed in the DMZ, you can also upgrade the software to ScreenOS version 6.1.)
2. Deploy an Infranet Controller on the network so that users can access it.
3. Configure Host Checker policies on the Infranet Controller to add endpoint compliance.

Figure 1: Server front end scenario

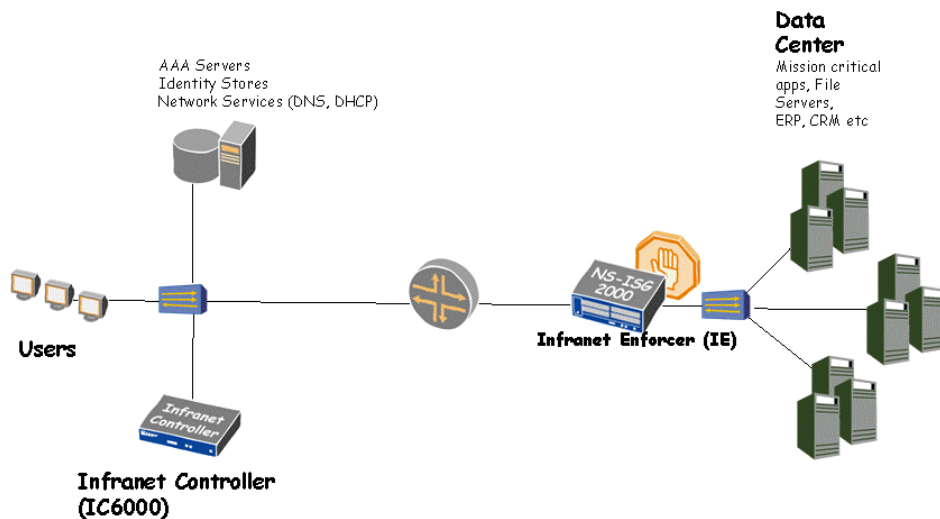


Table 2: Recommended hardware for the server front end deployment scenario

Recommended Infranet Controllers	Recommended Infranet Enforcers
IC 6500	NS5200
	NS5400
	ISG2000



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 to force the user to bring the endpoint into compliance before restoring WAN access.

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 a 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. (If you have an existing Juniper Networks firewall that is deployed in the DMZ, you can also upgrade the software to ScreenOS version 6.1.)
2. Deploy an Infranet Controller on the network so that users can access it.
3. Configure and enforce Host Checker policies to ensure that only compliant endpoints can access the network.

Figure 2: WAN gateway scenario

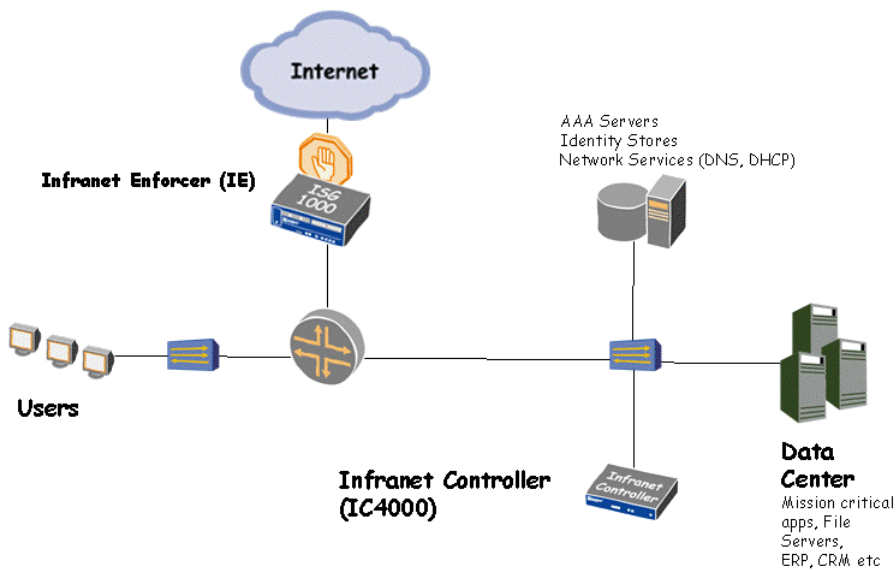


Table 3: Recommended hardware for the WAN gateway deployment scenario

Recommended Infranet Controllers	Recommended Infranet Enforcers
IC 6500	NS204
	NS208
	NS500
	ISG1000

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

Distributed Enterprise Deployment Scenario

Overview of example distributed enterprise deployment scenario

Overview of customer business problem

You have a branch office with a significant portion of the employee base. In addition to securing the corporate headquarters, your company wants to secure the branch office assets. The company also wants to allow access from the branch office to protected resources on the corporate LAN at the corporate headquarters.

The company has two Juniper NetScreen firewalls site-to-site VPN deployments and wants to use them to protect the perimeter and the LAN from malicious users and applications.

Overview of the solution for a distributed enterprise scenario

Typically, users with an unmanaged endpoint connect from an insecure branch network directly to the enterprise LAN via a site-to-site IPsec tunnel. A Juniper NetScreen firewall provides Deep Inspection and antivirus checking to mitigate some of the threat. But deploying an Infranet Enforcer as the branch office firewall provides needed support for policy enforcement.

The unified access control solution checks all endpoints for compliance before allowing access to the enterprise LAN at the corporate headquarters, which eliminates a major source of security problems.

Together, the Infranet Enforcer and Infranet Controller can dynamically enforce network security policies and protect the enterprise LAN at the corporate headquarters from unauthenticated users and non-compliant endpoints.

Deploying a unified access control solution in a distributed enterprise scenario

There are two versions of deploying the distributed enterprise scenario:

- Deploy the Infranet Controller in both the branch and corporate headquarters offices

- Deploy the Infranet Controller in the corporate headquarters office only



NOTE: When deploying either version of the distributed enterprise scenarios, keep these guidelines in mind:

- You *must* use a route-based site to site VPN policy between the Infranet Enforcers at the branch and corporate headquarters offices. Any traffic that is routed to a specific network must pass through the site to site tunnel. A policy-based VPN will not work correctly in the distributed enterprise scenarios.
 - You *cannot* use Transparent mode for the Infranet Enforcers in either version of the distributed enterprise scenario.
-

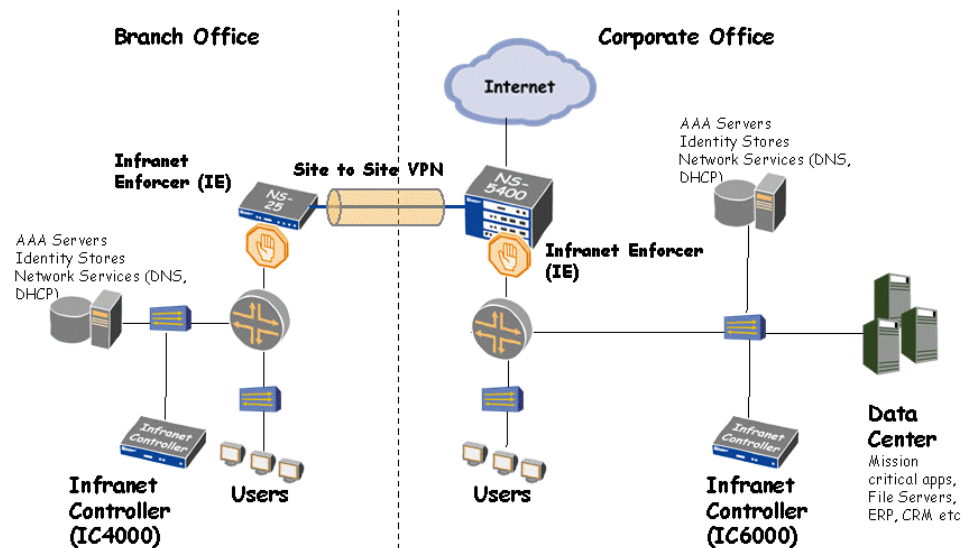
Deploying the Infranet Controller in branch and headquarters offices

In this deployment scenario, you deploy the Infranet Controller in both the branch and headquarters offices. You also deploy the Infranet Enforcer in both the branch and headquarters offices.

The unified access control solution makes sure that only the endpoints that the Infranet Controller has assessed and authenticated can access the resources in corporate headquarters offices.

To deploy Infranet Enforcer and Infranet Controller in branch and headquarters offices:

1. Deploy an Infranet Enforcer in the DMZ of the branch and headquarters offices as shown in Figure 3. (If you have an existing Juniper Networks firewall that is deployed in the office DMZs, you can also upgrade the software to ScreenOS version 5.3.)
2. Deploy an Infranet Controller on the branch and corporate office networks so that users in each location can access them.
3. Configure and enforce Host Checker policies to ensure that endpoints meet your security requirements for accessing the network.

Figure 3: Distributed enterprise with IC in both branch and headquarters offices scenario

Deploying Infranet Controller in corporate headquarters office only

In this deployment scenario, you deploy the Infranet Controller in the corporate headquarters office only. You also deploy the Infranet Enforcer in both the branch and headquarters offices.

The unified access control solution makes sure that an unauthenticated user in the branch office can only gain access to the Infranet Controller and some essential services such as DHCP and DNS. After the user signs in and the Infranet Controller verifies that the user's computer is compliant, the user can access the protected resources on the corporate headquarters network.

To deploy the Infranet Controller in the corporate headquarters office only:

1. Deploy an Infranet Enforcer in the DMZ of the branch and headquarters offices as shown in Figure 4. (If you have an existing Juniper Networks firewall that is deployed in the office DMZs, you can also upgrade the software to ScreenOS version 5.3.)
2. Deploy an Infranet Controller on the corporate headquarters network only so that branch and corporate headquarters users can access it.
3. Configure and enforce Host Checker policies to ensure that endpoints meet your security requirements for accessing the network.

Figure 4: Distributed enterprise with IC in headquarters office only scenario

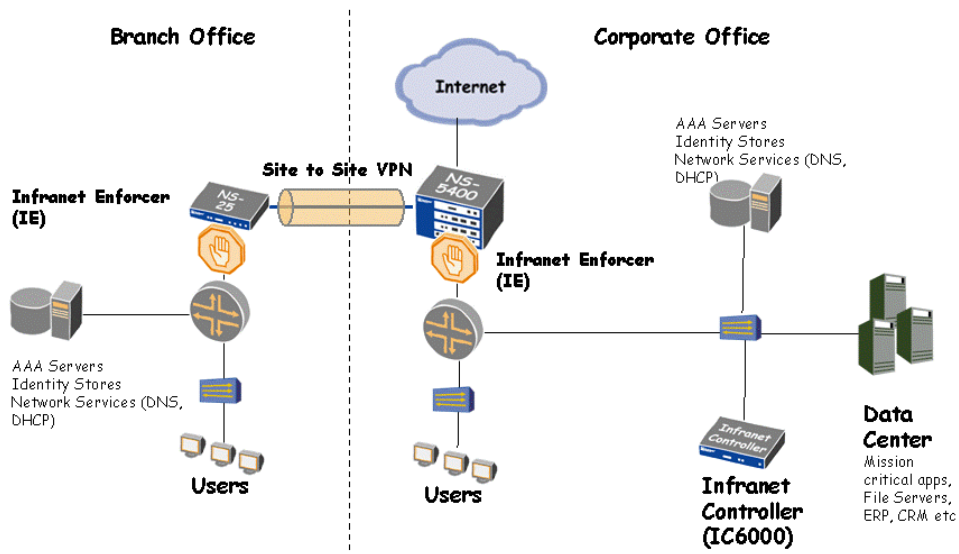


Table 4: Recommended hardware for the distributed enterprise deployment scenario

Recommended Infranet Controllers	Recommended Infranet Enforcers
IC 4500 (branch office)	NS5GT
IC 6500 (corporate HQ)	NS25
	NS50

Chapter 5

Campus Wired Deployment Scenario

Overview of example campus wired deployment scenario

Overview of customer business problem

You are concerned that resources on the wired corporate LAN are not adequately protected. Users can connect their computers to the corporate LAN and obtain complete access to the network resources without assessment or authentication.

Because of the cost and complexity, the company does not want to replace or upgrade the network infrastructure devices such as switches and routers.

Overview of the solution for a campus wired scenario

While it is typical for users in the extended enterprise to sign in to an SSL VPN and be authenticated and verified as secure, users on the campus LAN are usually not required to do so.

The unified access control solution changes this approach by requiring users to sign into the Infranet Controller, which authenticates them and verifies the compliance of their computers before allowing them access to protected resources.

The solution does not require an upgrade of the network infrastructure. You can deploy an Infranet Enforcer at the distribution layer or in front of mission critical applications that need protection.

Together, the Infranet Enforcer and Infranet Controller can dynamically enforce network security policies to make sure that only compliant endpoints can access resources on the campus wired LAN.

Deploying a unified access control solution in a campus wired scenario

To deploy a unified access control solution in a campus wired scenario:

1. Deploy the Infranet Enforcer in front of the data center resources you want to protect or in the distribution layer behind a switch as shown in Figure 5. (If you have an existing Juniper Networks firewall that is deployed in the DMZ, you can also upgrade the software to ScreenOS version 5.3.)

2. Deploy an Infranet Controller on the network so that users can access it.
3. Configure and enforce Host Checker policies to ensure that endpoints meet your security requirements for accessing the network.

Figure 5: Campus wired scenario

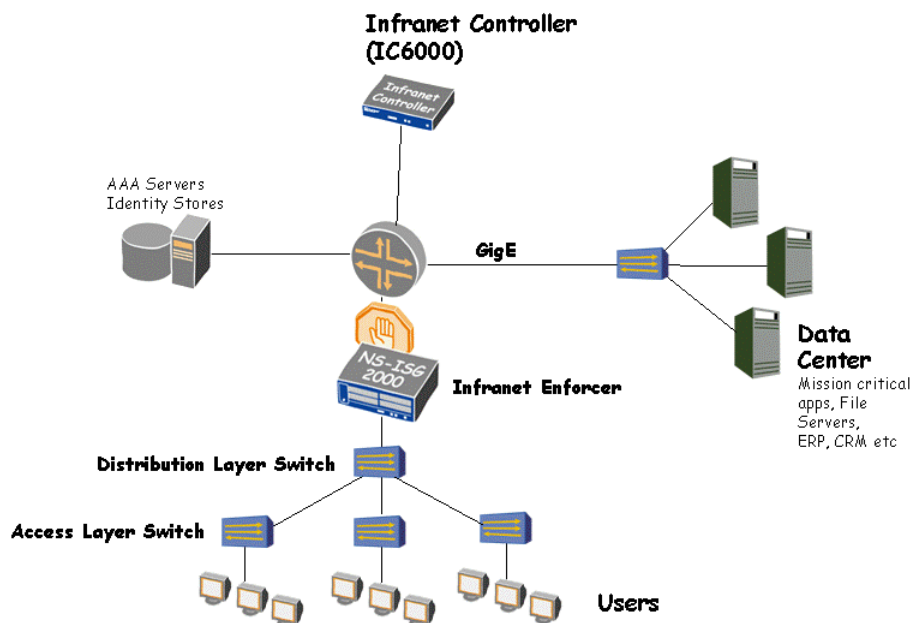


Table 5: Recommended hardware for the campus wired deployment scenario

Recommended Infranet Controller	Recommended Infranet Enforcers
IC 6500	NS5200
	NS5400
	ISG2000

NOTE: When deploying the campus wired scenario, keep these guidelines in mind:

- If there is a firewall between your users and your authentication server, be sure to configure the firewall with static policies that allow traffic from the users to the authentication server.
- If there are any other resources that users need before authenticating to the Infranet Controller, be sure to configure the firewall with static policies that allow traffic from the users to those resources.

Chapter 6

Campus Wireless Deployment Scenario

Overview of example campus wireless deployment scenario

About the business problem

You are concerned that resources on the wireless corporate LAN are not adequately protected. The company is aware of the security issues with 802.11 and wants additional security for your wireless deployments.

About the solution for a campus wireless scenario

The unified access control solution requires wireless users to sign into the Infranet Controller, which authenticates them and verifies the compliance of their computers before allowing them to use the wireless network to access protected resources on the network.

The solution does not require an upgrade of the wireless network infrastructure. You can either deploy an Infranet Enforcer network enforcement point behind a wireless access point, or you can deploy an Infranet Enforcer that includes a built-in wireless access point.

Together, the Infranet Enforcer and Infranet Controller can dynamically enforce network security policies to make sure that only compliant wireless endpoints can access campus-wide resources via the wireless network.

Deploying a unified access control solution in a campus wireless scenario

To deploy a unified access control solution in a campus wireless scenario:

1. Do either of the following as shown in Figure 6:

- Deploy the Infranet Enforcer behind a wireless access point.
- Deploy an Infranet Enforcer that is also a wireless access point.

If you have an existing Juniper Networks firewall that is deployed in the DMZ, you can also upgrade the software to ScreenOS version 5.3.

2. Deploy an Infranet Controller on the network so that users can access it.
3. Configure and enforce Host Checker policies to ensure that endpoints meet your security requirements for accessing the network.

Figure 6: Campus wireless scenario

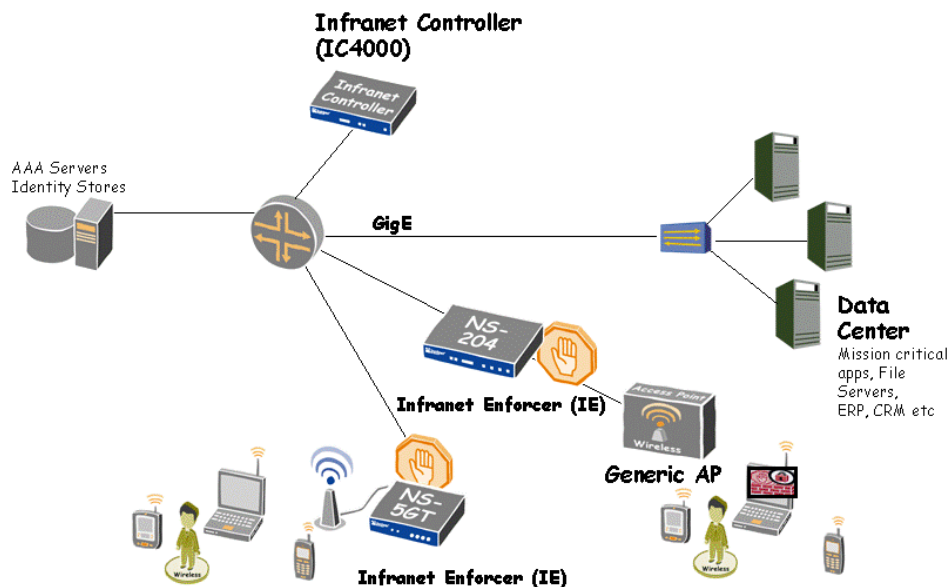


Table 6: Recommended hardware for the campus wireless deployment scenario

Recommended Infranet Controller	Recommended Infranet Enforcers
IC 4500	NS5GT
	NS25
	NS50
	NS204
	NS208



NOTE: When deploying the campus wireless scenario, keep these guidelines in mind:

- If there is a firewall between your wireless access point and your authentication server, be sure to configure the firewall to allow traffic from the access point to the authentication server.
- If there are any other resources that users need before authenticating to the Infranet Controller, be sure to configure the firewall with static policies that allow traffic from the wireless access point to those resources.

Chapter 7

802.1X Deployment Scenarios

This chapter contains the following deployment scenarios for using 802.1X enforcement with the Unified Access Control solution:

- “Scenario 1: Using VLANs that are not routed (no default IP address)” on page 19
- “Scenario 2: Using VLANs that are not routed (use default Quarantine IP address)” on page 21
- “Scenario 3: Using VLANs that are routed (no default IP address)” on page 22
- “Scenario 4: Using 802.1X without a remediation VLAN and no default IP address” on page 23

802.1X deployment scenarios that use a remediation VLAN

In the three 802.1X deployment scenarios described in this section, there are two VLANs that are used to control user access to resources:

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

In all three scenarios in this section, 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. In these scenarios, an Infranet Enforcer controls access to the protected resource, which is a Finance server in the Trusted VLAN.

Scenario 1: Using VLANs that are not routed (no default IP address)

Scenario 1 uses 802.1X with VLANs that are not routed and there is no default IP address for the endpoint. That is, the user must provide valid sign-in credentials to obtain an IP address on the network.

Resources

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

- Finance Server: 10.0.0.16
- Corp Server: 10.0.0.17
- 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 7: 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

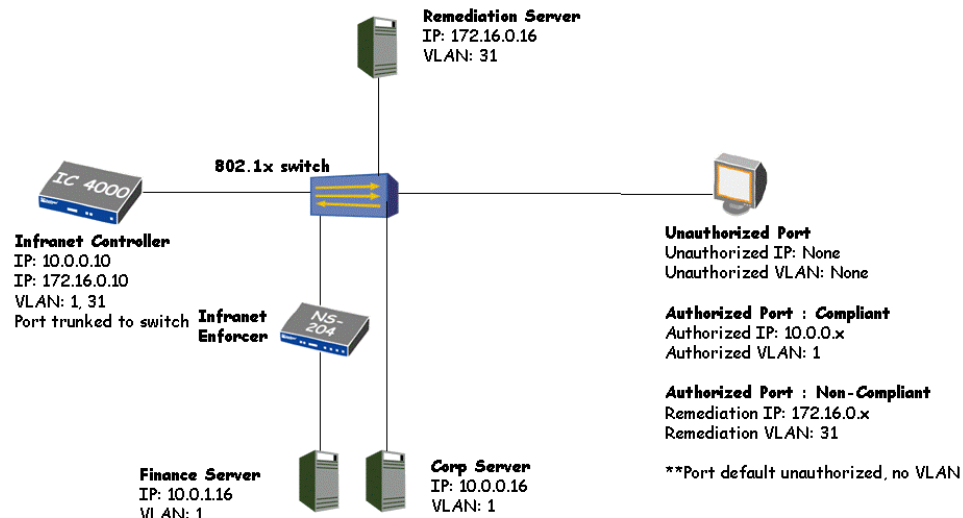
To access the Corp server, a user must have a compliant endpoint and valid sign-in credentials. To access the Finance Server, the user must have a compliant endpoint and be a member of the finance role or group. All other users with un-compliant endpoints can access the Remediation server only.

Table 8: Resource Access

Corp 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

Figure 7 illustrates this scenario.

Figure 7: 802.1X with VLANs not routed (no default IP address) scenario



Scenario 2: Using VLANs that are not routed (use default Quarantine IP address)

Similar to scenario 1, scenario 2 uses 802.1X with VLANs that are not routed. The difference in scenario 2 is that it uses a default Quarantine IP address for the endpoint instead of no default IP address. That is, the endpoint is assigned an IP address on the Quarantine VLAN before the user provides valid sign-in credentials.

Resources

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

- Finance Server: 10.0.0.16
- Corp Server: 10.0.0.17
- 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 does not have to provide valid sign-in credentials and does not need to use a compliant endpoint to obtain an IP address on the Quarantined network.

Table 9: Network Access

Trusted Network	Quarantined Network
All authenticated users with endpoints that comply with security policies	All users

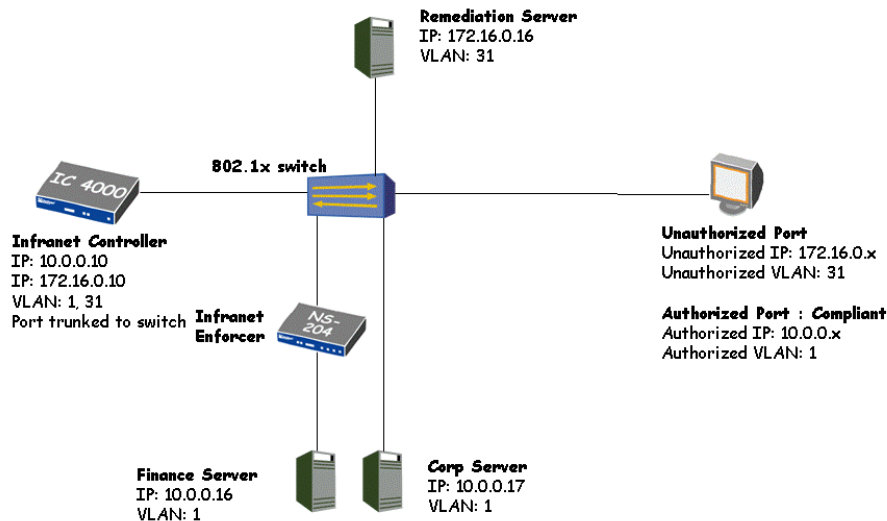
To access the Corp server, a user must have a compliant endpoint and valid sign-in credentials. To access the Finance Server, the user must have a compliant endpoint and be a member of the finance role or group. All other users with un-compliant endpoints can access the Remediation server only.

Table 10: Resource Access

Corp 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

Figure 8 illustrates this scenario.

Figure 8: 802.1X with VLANs not routed (default Quarantine IP address) scenario



Scenario 3: Using VLANs that are routed (no default IP address)

Scenario 3 uses 802.1X with VLANs that are routed and does not use a default IP address for the endpoint. That is, the user must provide valid sign-in credentials to obtain an IP address on the network.

The difference in scenario 3 is that it uses a router or firewall that provides routing between the two VLANs. The router or firewall also has access control rules that only allow the Infranet Controller to be accessible across VLANs.

Resources

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

- Finance Server: 10.0.0.16
- Corp Server: 10.0.0.17
- 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 11: 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

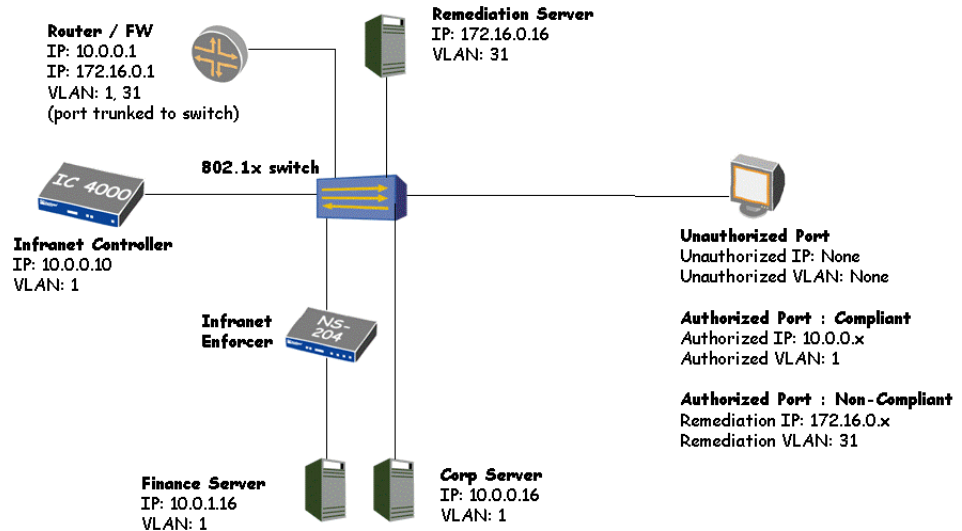
To access the Corp server, a user must have a compliant endpoint and valid sign-in credentials. To access the Finance Server, the user must have a compliant endpoint and be a member of the finance role or group. All other users with un-compliant endpoints can access the Remediation server only.

Table 12: Resource Access

Corp 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

Figure 9 illustrates this scenario.

Figure 9: 802.1X with VLANs routed (no default IP address) scenario



An 802.1X deployment scenario that does not use a remediation VLAN

The 802.1X deployment scenario described in this section does not use a remediation VLAN. 802.1X is used to authenticate the port on the endpoint, which starts in an unauthorized state and does not provide access. The user has to authenticate using 802.1x to get an IP address on the network.

Scenario 4: Using 802.1X without a remediation VLAN and no default IP address

In this scenario, an Infranet Enforcer in Transparent mode controls access to two protected resources, which are a Finance server and a Corporate server in the Trusted VLAN.

Resources

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

- Finance Server: 10.0.0.16
- Corp Server: 10.0.0.17
- Remediation Server: 10.0.0.15

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 13: Network Access

Trusted Network	No Network Access
All authenticated users with endpoints that comply with security policies	All unauthenticated users

To access the Corp 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 14: Resource Access

Corp 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

Figure 10 illustrates this scenario.

Figure 10: 802.1X without remediation VLANs (no default IP address) scenario

